Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

The White House Office of Science and Technology Policy published a Request for Information (RFI) in the Federal Register on public and private sector uses of biometric technologies. The purpose of this RFI was to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation. Input was requested on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states. The RFI comment period opened on October 8, 2021, with responses requested by January 15, 2022. This RFI generated 130 responses.

The responses received through the RFI by January 26, 2022, are posted below. In accordance with the instructions provided in the RFI, only approximately 10 pages of content are posted. Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government.

Table of Contents

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Accenture

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022
Office of Science and Technology Policy
Washington, DC 20502

Re: Request for Information on Public and Private Sector Uses of Biometric Technologies [Docket Number 2021-21975]

To Whom it May Concern:

Accenture is pleased to provide comments in response to the Office of Science and Technology Policy (OSTP) on its request for information (RFI) regarding public and private sector uses of biometric technologies.

As a leading global professional services and technology company, Accenture provides a broad range of services and solutions in strategy and consulting, technology, interactive, and operations, that span all industries.

Accenture has deep experience helping organizations use biometric technologies safely, securely, and effectively to provide enormous benefits. From collaborating with the World Economic Forum's Known Traveller Digital Identity (KTDI) initiative on a biometric-enabled digital identity pilot to enhance security and efficiency in cross-border travel[1] to delivering a Biometric Identity Management System for the United Nations High Commissioner for Refugees to register and verify the identities of persons around the world,[2] Accenture is at the forefront of not just promoting the responsible use of biometrics but actually designing and using biometric technologies responsibly and effectively.

We believe the United States government can and should establish and enforce guardrails that promote innovation while preventing harmful use-cases. We look forward to further engaging with OSTP on its evaluation of biometric technologies and its broader effort to create a Bill of Rights for an Automated Society.

Sincerely,

David Treat
Senior Managing Director – Blockchain and Multiparty Systems Global Lead
Accenture

[1] The Known Traveller Digital Identity (KTDI) initiative is available here: https://ktdi.org/
[2] More information of Accenture's work with the United Nations High Commissioner for Refugees is available here: https://newsroom.accenture.com/industries/systems-integration-technology/united-nations-high-commissioner-for-refugees-and-accenture-deliver-global-biometric-identity-management-system-to-aid-displaced-persons.htm

Introduction

While biometric techniques have been used for almost one hundred years, in the last twenty years we have seen rapid growth in personal, commercial, and governmental use-cases of biometric authentication and identification. Today, biometric recognition, or automated recognition technology, has been widely adopted and used in the private, public, and humanitarian sectors.

Since 2013, millions of biometric systems have been added to the market, spurred by the release of smart phones utilizing biometric technologies like fingerprint and facial recognition to allow users to unlock their phones. The proliferation of biometric-enabled smart phones increased public awareness and trust in these systems, primarily for the usability and security that they bring. Biometric technologies have also been increasingly used to bolster the security of financial transactions, automate border clearance, and increase inclusion of undocumented people[3], among many other examples.

As biometric technologies have become a common part of people's daily lives, there has also been increased government, media, and public attention to the potential risks of this technology, including legitimate concerns about accuracy and potential discriminatory impacts. Some jurisdictions have banned biometric systems such as facial recognition, while others have placed indefinite moratoria into effect.

It is critical to recognize that the relative performance of biometric recognition systems is highly use-case dependent. Therefore, to maximize the potential of biometric technology, including enhanced security and user experiences while mitigating risks, we believe the United States needs policies and regulations that are use-case specific that enable various yet disparate beneficial uses and criminalize those deemed harmful, rather than outright bans and indefinite moratoria.

As outlined in the Office of Management and Budget's (OMB) *Guidance for the Regulation of Artificial Intelligence Applications*, policymakers and regulators should collaborate with stakeholders, including designers, developers, and deployers to develop voluntary standards, guidelines, and best practices for private sector testing and certification of biometric technologies.

As the OMB memo outlines, in some cases, after conducting a regulatory impact analysis, proposed regulations should be considered when there is a demonstrated public need. In these cases, regulators should explore risk and impact-based regulatory approaches that account for privacy, security, and interoperability, while ensuring that any regulation of biometric technology is consistent with other regulations of AI-enabled systems.

[3] More information on uses biometric technology to increase inclusion of undocumented people is available here: https://www.unhcr.org/en-us/protection/basic/550c304c9/biometric-identity-management-system.html

We appreciate the opportunity to share our views with OSTP. We have organized our comments below into four sections: terminology, responsible use and regulation, testing and certification, and a conclusion.

Terminology

Regulators, Congress, and other stakeholders need a consistent way of communicating what biometric systems are and how they work in their many and varied applications. They should also understand what technologies, like inference of cognitive and/or emotion state, are not generally categorized as biometric technologies. To that end, Accenture suggests the following amendments to OSTP's biometrics terminology as expressed in the RFI:

- *Biometric Information:* Accenture agrees with OSTP's use of "biometric information" to refer to any measurements or derived data of an individual's physical or behavioral characteristics.
- *Biometric Technology:* Accenture believes that OSTP's definition of "biometric technology" as a "system that uses biometric information for recognition or inference" is too broad because it includes multiple industries that must be regulated separately.
- *Biometric Recognition:* The International Organization for Standardization (ISO) defines Biometric Recognition as the "automated recognition of individuals based on their biological and behavioral characteristics[4]." Further, Biometric Recognition relies on the commonly accepted characteristics of biometric factors as outlined by the National Academy of Sciences: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention[5].
- *Inference of cognitive and/or emotional state:* This should not be categorized as "biometric technology" because cognitive or emotional state is charactered by none of the commonly accepted National Academy of Sciences characteristics of biometric factors outlined above. Despite relying on an individual's physical and behavior characteristics, inference of cognitive and/or emotional state is typically classified as Emotion Detection or Sentiment Analysis and is in the domain of text, audio, and video analytics technology(ies), not biometric technology.

Responsible Use and Regulation of Biometrics

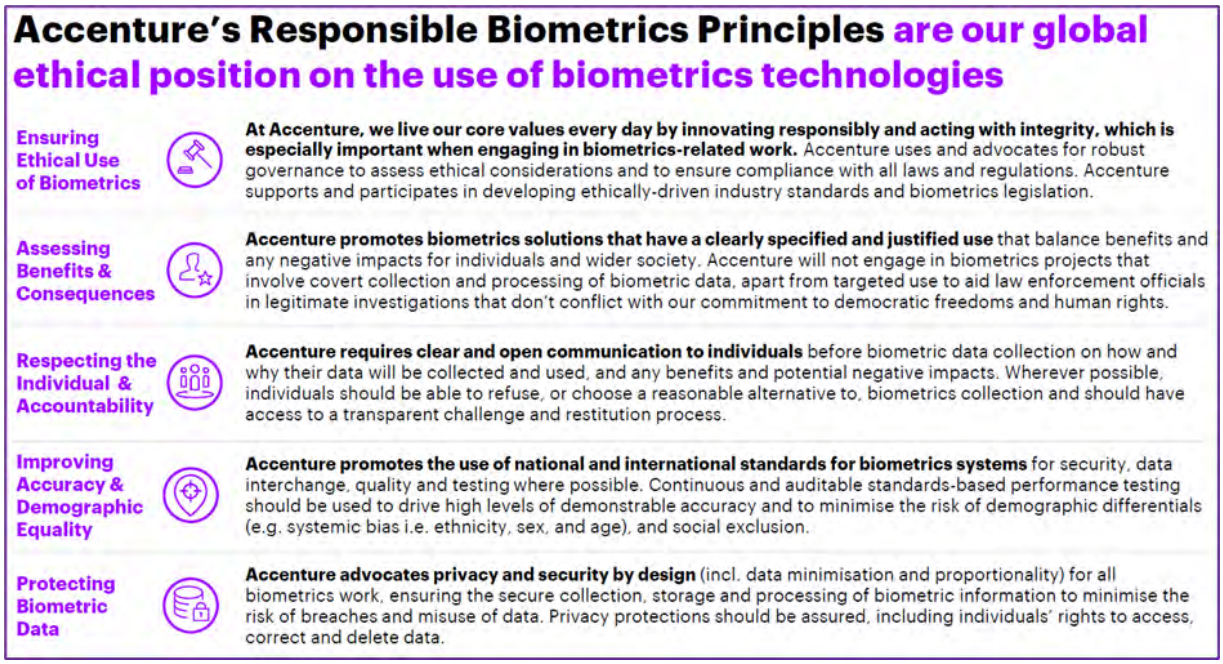
Accenture is committed to ethics, human rights, and strong corporate governance. These principles are a key driver of our business strategy and a foundation for technological innovation in areas including biometrics.

For both corporate governance and government regulation, responsible use of biometrics should begin with the understanding that all biometric systems have Type I (false non-match) and Type II (false match) errors; that is, they are probabilistic not deterministic.

[4] ISO's biometrics definition is available here: https://www.iso.org/standard/66693.html
[5] The National Academy of Sciences' characteristic of biometric factors is available here: https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities

Additionally, the many and varied use-cases for the application of biometric technologies have differing error rates. For example, covert, uncooperative, unconstrained surveillance applications of biometric technologies (e.g., surveillance) often yield much higher error rates than overt, cooperative, constrained, opt-in applications (e.g., Automated Border Clearance). Responsible use is highly dependent on the specified use-case. Each target use-case must consider factors such as inclusion, exclusion, and differential treatment.

Accenture has outlined five Responsible Biometrics Principles that serve as our global ethical position on the use of biometric technologies:



In response to increased scrutiny on biometric systems, some jurisdictions have banned the technology outright and others have put moratoria in effect with no clear path to effective regulation. It is difficult to understand the practical benefits of outright bans that do not delineate factors such as:

- Is the system overt or covert?
- Is the system performing authentication or identification?
- Does the system require informed consent of the data subject?
- Under which privacy regulations does the system operate?
- Under which performance requirements does the system operate?
- To which security requirements does the system conform?

Instead of bans and moratoria that stop all innovation in its tracks, regulators should create policies and regulations that drive responsible innovation and use of biometrics that helps to keep communities secure from fraudsters and those empowered by a lack of reliable authentication. This might require system owners to document answers to the above questions according to specific intended use-cases. If a biometric solution is insufficiently

accurate for the intended use-case or its performance is impacted by demographic differentials, specific performance requirements and regulations that require certification to specified conformance criteria for its intended use-cases are a better option than outright bans and moratoria. Some examples of potential regulations include:

- Requiring documentation of the system, its failure states, and its intended use-case;
- Requiring that implementors of biometric systems evaluate use-case specific performance using operational data, from the operational environment on a continuing basis;
- Requiring that implementors of biometric systems publish their performance metrics for the specified use-case(s);
- Requiring that biometric systems operate with the allowable limits of demographic differentials for the specified use-case(s);
- Requiring that there be a manual alternative to the biometric system for the intended use-case(s);
- Requiring defined mechanisms and governance for recourse and redress;
- Requiring that automated decisions can be human adjudicated for the intended use-case(s);
- Requiring that automated decisions are human adjudicated or reviewable for any use-case where the results are not in favor of the individual; and
- Requiring an analysis that illustrates how human rights may be upheld or enhanced with the introduction of the solution in its intended implementation and how human rights may be diminished if the solution or the use-case is intentionally altered.

We expect regulators to define the responsible use of biometrics to include traditional privacy protections around Personally Identifiable Information (PII) – where policy such as the European Union's General Data Protection Regulation (GDPR) defines both the guidance for protection and the penalties for failures, while recognizing that biometric information is sensitive personal data because it is not private, linkable, and non-changeable. The sharing, retaining, and protecting of personal data, including biometric information, are all fundamental privacy provisions, as are portability, accuracy, redress, and breach alerts that should have corresponding regulation. To this end, as stated by our CEO, it is imperative that the U.S. establish a national privacy law and we would welcome an opportunity to discuss this with OSTP.

Additionally, OSTP should align its biometrics work and broader efforts to develop a Bill of Rights for an Automated Society with other government initiatives, including the National Institute of Standards and Technology's (NIST) upcoming AI Risk Management Framework and their on-going AI User Trust Project, and OMB's *Guidance for the Regulation of Artificial Intelligence Applications.* It would also be beneficial to have the work feed into the National AI Advisory Committee so that stakeholders have a single place to discuss and make recommendations for policymaking.

Testing and Certification

Regulators should work with relevant stakeholders, including developers, designers, and deployers of biometric systems to define certain use-cases that should be subject to a process similar to the FDA's 12-step approval process for drugs to be considered safe and effective. Before any drug can be released to the market for a specific, on-label use, it must go through a process that includes rigorous testing, with independent review, to demonstrate safety and efficacy, as well as post-approval monitoring. There are currently no such certifications to consider biometric technologies, as implemented, are "safe and effective." We recommend that OSTP refer to OMB's *Guidance for the Regulation of Artificial Intelligence Applications* when considering the overall approach to regulation as well as testing and certification best practices for biometric technologies.

NIST performs many in-depth evaluations of various biometric technologies using their data in their laboratory environment, which is informative but ultimately limited. NIST asserts that "…it is incumbent upon the system owner to know their algorithm…" and to "…measure accuracy of the operational algorithm on the operational image data…"[6] While NIST's work is certainly helpful, it is not sufficient to ensure responsible and safe use of biometrics.

For certain use-cases, regulators should consider mandating that biometric system owners define the intended use-case(s), seek approval for each based on transparent, reviewed, publicly available data, and continuously monitor effectiveness.

Conclusion

Congress and regulators should continue to seek to understand how biometric systems work in their many varied applications and regulate accordingly as they have in the past with health information, food safety, and other important topics. This RFI is an important step toward effective biometric governance and should constitute a key part of OSTP's work toward developing a Bill of Rights for an Automated Society. A cohesive approach that brings together OSTP's AI Bill of Rights, OMB's regulatory guidance, NIST's ongoing activity, and the Department of Commerce's National AI Advisory Committee would benefit all stakeholders in supporting and advancing America's leadership and protection of Americans' values.

In conclusion, Accenture believes that biometric techniques, if properly regulated and responsibly deployed can continue to facilitate and secure our lives, while preserving our privacy and human dignity – for the next twenty years and beyond.

[6] More information on NIST's evaluations of biometric technologies can be found here: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Access Now

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

Dr. Eric S. Lander
Director, White House Office of Science andTechnology Policy
Executive Office of the President

Dr. Lynne Parker
Director, National Artificial Intelligence Initiative Office
Executive Office of the President

Dr. Alondra Nelson
Deputy Director, White House Office of Science and Technology Policy
Executive Office of the President

Via electronic filing

Re: Request for Information on the on Public and Private Sector Uses of Biometric Technologies

Access Now appreciates the opportunity to submit comments to the White House's Office of Science and Technology Policy (OSTP) Request for Information (RFI)on Public and Private Sector Uses of Biometric Technologies.[1]

Access Now provides thought leadership and policy recommendations to the public and private sectors by offering a digital rights perspective to ensure the internet's continued openness and the protection of human rights.[2] We have special consultative status at the United Nations. Access Now also leads the **Ban Biometric Surveillance** campaign, which calls for a prohibition on uses of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance, and which has been signed by 193 civil society organisations from 63 countries around the world.[3] In Europe, Access Now is part of the **Reclaim Your Face** campaign which launched a formal petition to ban biometric mass surveillance in the European Union.[4] We also launched a campaign with All Out, a global LGBT+ organization to expose the threat of

1 https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.
2 https://www.accessnow.org/.
3 https://www.accessnow.org/ban-biometric-surveillance/.
4 https://reclaimyourface.eu/.

automated gender "recognition" and the use of AI systems to predict sexual orientation. In addition, we facilitate the **#WhyID** community to ensure that digital identity programs respect the rights of people around the world.[5]

With the rising investments in and expansion of automated technologies, the global biometric industry is projected to grow around USD84.27 billion by 2026.[6] The United States must therefore enforce and develop the highest human rights compliance standards for biometric technologies designed, developed, or deployed in the United States. While strong regulation and safeguards can mitigate certain harms, certain biometric technologies are incompatible with the protection of human rights. Accordingly, we believe that these uses of biometric technology deserve greater scrutiny.

Introduction

The Request for Information (RFI) seeks answers on a variety of questions. These comments focus on the use of biometrics to infer emotion, gender and other attributes as well as the use of biometric recognition in mandatory digital ID programs and biometric mass surveillance. This submission provides information in response to question four of the RFI (the exhibited and potential harms of a particular biometric technology), namely (I) what emotion recognition technology is (II) the unreliability and discriminatory nature of emotion recognition technology, (III) how emotion recognition undermines the rights to freedom of thought and privacy, (IV) how mandatory digital identity programs using biometric recognition leads to exclusionary outcomes, (V) how biometric recognition is predicated on mass surveillance, and (VI) our recommendations to the OSTP.

I. What is Emotion Recognition Technology ?

The term 'emotion recognition' covers a range of technologies that claim to infer someone's emotional state from data collected about that person.[7] Emotion recognition systems can be used in job interviews claiming to tell how enthusiastic or honest you are.[8] Airport security systems use emotion

[5] https://www.accessnow.org/whyid/.
[6] Global $84.27 *Ban Biometrics Markets, Competition, Forecast & Opportunities*, Yahoo News (Nov. 22, 2021) https://www.yahoo.com/now/global-84-27-bn-biometrics-163200622.html.
[7] Jay Stanley, Experts Say 'Emotion Recognition' Lacks Scientific Foundation, ACLU (July 18, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/experts-say-emotion-recognition-lacks-scientific.
[8] Angela Chen and Karen Hao, *Emotion AI researchers say overblown claims give their work a bad nam*e, MIT Technology Review (Feb. 14, 2020), https://www.technologyreview.com/2020/02/14/844765/ai-emotion-recognition-affective-computing-hirevue-regulation-ethics/.

recognition to analyze your facial expressions for bad intent,[9] and if you are a defendant on trial, policing programs claim to detect deception.[10]

Many 'face-based' emotion recognition applications rely on the assumption that everyone expresses emotion in the same way, relying on Paul Eckman's controversial 'basic emotions' theory, which posits 'universal categories' of human emotion and claims to describe how these can be read from facial expressions.[11] Furthermore, these systems often have the implicit or express intention of manipulating our thoughts by tailoring content to our emotional state.[12]

II. Emotion Recognition is Unreliable and Racially Biased

A prominent study by researchers in the science of emotion concluded that despite "[t]echnology companies [...] investing tremendous resources to figure out how to objectively "read" emotions in people by detecting their presumed facial expressions [...] **the science of emotion is ill-equipped to support any of these initiatives**".[13] Further, devastating criticism of the entire project of emotion recognition has been voiced from numerous quarters, with even Paul Eckman, whose theories underlie the majority of face-based emotion recognition systems, stating that "**[m]ost of what I was seeing was what I would call pseudoscience**" in emotion recognition technology.[14]

The relationship between facial expressions and a person's emotional state is a lot more complex than it may appear because **people express their emotions considerably differently across cultures, ethnicities, and circumstances**. This is corroborated by researchers from the University of Glasgow, which found that culture shapes the perception of emotions.[15] Facial expressions are filtered through

---

[9] Emotion recognition at the airport, Felena, https://felenasoft.com/xeoma/en/articles/emotion_recognition_in_airport/.
[10] Sebastien Krier, *Facing Affect Recognition*, (Sept. 18, 2020)https://asiasociety.org/sites/default/files/inline-files/Affect%20Final.pdf; https://emojify.info/ ;
[11] *Id*; see also Oscar Schwartz, *Don't look now: why you should be worried about machines reading your emotions*, The Guardian (Mar. 6, 2019), https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science.
[12] See, for example, this case taken by the Brazilian consumer organisation, IDEC, where such a system was used in a metro line in São Paulo. Access Now intervened, submitting an expert opinion, and the judge ultimately ruled in favour of IDEC: https://www.accessnow.org/sao-paulo-court-bans-facial-recognition-cameras-in-metro/
[13] Lisa Feldman Barrett, et al, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, Psychological Science in the Public Interest, vol. 20, no. 1, July 2019, pp. 1–68, https://journals.sagepub.com/doi/10.1177/1529100619832930.
[14] Madhumita Murgia, *Emotion recognition: can AI detect human feelings from a face?* The Financial Times (May 12, 2021),https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452; see also Luke Stark and Jevan Hutson, *Physiognomic Artificial Intelligence* (September 20, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927300.
[15] Chaona Chen et al., *Distinct Facial Expressions Represent Pain and Pleasure Across Cultures*, Proceedings of the National Academy of Sciences of the United States of America, vol. 115, no. 43, 2018, pp. E10013–E10021, https://www.pnas.org/content/115/43/E10013.

culture to gain meaning and our culture and societal attitudes fundamentally shape our emotions.[16] In addition, facial expressions do not always reflect our inner emotions because people often mask or suppress their emotions.[17]

Researchers from the University of Cambridge who designed a game that attempt to identify emotions from facial expressions concluded "that **the software's readings are far from accurate, often interpreting even exaggerated expressions as 'neutral.'**"[18] The game, emojify.info, challenges you to produce six emotions (happiness, sadness, fear, surprise, disgust, and anger), which the system will "read" by your computer via your webcam and attempt to identify.[19] This study demonstrates that **"the basic premise underlying much emotion recognition tech: that facial movements are intrinsically linked to changes in feeling, is flawed."**[20]

Emotion recognition technology is also racially biased. Research shows that some **emotion recognition technology has trouble identifying the emotions of darker-skinned faces**. In one study, emotion recognition systems assigned more negative emotions to black men's faces when compared to white men's faces. These systems **read the faces of black men as angrier than the faces of white men**, no matter their expression.[21]

The use of emotion recognition systems in hiring interviews,[22] schools,[23] and other settings have also caused great concern.[24] In China, emotion recognition has been used by teachers to monitor students' emotions as they study at home and gauge how they respond to classwork.[25] As they study, the system

[16] Michael Price, *Facial Expressions – Including Fear – May Not Be As Universal As We Thought*, Science (Oct. 17, 2016),https://www.science.org/content/article/facial-expressions-including-fear-may-not-be-universal-we-thought ; see also Carlos Crivelli et al., *The Fear Gasping Face as a Thread Display in a Melanesian Society*, Proceedings of the National Academy of Sciences of the United States of America (Oct. 17, 2016) ,https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5098662/.
[17] Miho Iwasaki and Yasuki Noguchi, *Hiding true emotions: Micro-expressions in eyes retrospectively concealed by mouth movements*, Scientific Reports. 2016, https://www.nature.com/articles/srep22049.
[18] James Vincent, *Discover the stupidity of AI emotion recognition with this little browser game*, The Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; see alo Emojify, https://emojify.info/
[19] *Id.*
[20] James Vincent, *Discover the stupidity of AI emotion recognition with this little browser game*.
[21] Lauren Rhue, *Emotion-reading tech fails the racial bias test*, The Conversation (Jan 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.
[22] Sheridan Wallar and Schellmann, *We tested AI interview tools. Here's what we found*, MIT Technology Review (July 7, 2021), https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/.
[23] Milly Chan, *This AI reads children's emotions as they learn*, CNN Business (Feb. 17, 2021), https://www.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html ; https://restofworld.org/2021/chinas-emotion-recognition-tech/.
[24] Cheryl Teh, *'Every smile you fake' — an AI emotion-recognition system can assess how 'happy' China's workers are in the office*, Insider (Jun. 15, 2021), https://www.insider.com/ai-emotion-recognition-system-tracks-how-happy-chinas-workers-are-2021-6.
[25] Chan, *This AI reads children's emotions as they learn.*

collects specific biometric information (like the muscle points on their faces) through the camera on their computer or tablet.[26] The system then attempts to identify emotions such as happiness, sadness, anger, surprise and fear.[27]

This technology presents real harms to marginalized communities.[28] The use of **emotion recognition systems in education could further exacerbate existing oppressive dynamics**. For instance, it is common knowledge that black students experience more suspensions and other disciplinary actions than white students, often for the same behavior.[29] Another study exploring racialized perception of emotions and bias among prospective teachers concluded that the **teachers are more likely to interpret the facial expressions of black boys and girls as being angry**, even when they are not.[30] If racially biased emotion recognition technology is deployed in these already problematic situations, existing inequalities and oppression could be magnified.

III. Emotion Recognition undermines the Right to Privacy, Freedom of Thought and Expression

Inferences about our emotional state represents an unacceptable intrusion into our private mental life, and erodes our right to privacy and freedom of thought.[31] The right to freedom of thought includes the right to keep our thoughts and opinions private, the right not to have our thoughts and opinions manipulated, and the right not to be penalized for our thoughts and opinions.[32]

As Article 19 pointed out, emotion recognition applications are a highly invasive form of surveillance that tracks, monitors, and profiles individuals through overt collection of sensitive personal data [33] In

---

[26] *Id.*
[27] *Id.*
[28] Abeba Birhane, *The Impossibility of Automating Ambiguity,* Artificial Life (June 11, 2021) https://direct.mit.edu/artl/article-abstract/27/1/44/101872/The-Impossibility-of-Automating-Ambiguity?redirectedFrom=fulltext.
[29] Travis Riddle and Stacey Sinclair, *Racial disparities in school-based disciplinary actions are associated with county-level rates of racial bias*, Princeton University (Apr. 2, 2019), https://www.pnas.org/content/116/17/8255.
[30] Amy G. Halberstadt et al., *Racialized Emotion Recognition Accuracy and Anger Bias of Children's Faces*, American Psychological Association (2020), https://www.apa.org/pubs/journals/releases/emo-emo0000756.pdf; see also Amy Halberstadt and Matt Shipman, *Future Teachers More Likely to View Black Children as Angry, Even When They Are Not*, NC State University (July 6, 2020), https://news.ncsu.edu/2020/07/race-anger-bias-kids/
[31] Access Now submission to the UN Special Rapporteur on Freedom of Religion or Belief Call for Inputs: Report to the UN General Assembly 76th Session on Respecting, Protecting and Fulfilling the Right to Freedom of Thought (Jun. 30, 2021), https://www.accessnow.org/cms/assets/uploads/2021/11/UN-Special-Rapporteur-on-Freedom-of-Religion-or-Belief_-Consultation-on-freedom-of-thought-technology.pdf.
[32] Susie Alegre, *Protecting Freedom of Thought in the Digital Age*, Centre for International Governance Innovation (May 2021), https://www.cigionline.org/static/documents/PB_no.165.pdf.
[33] *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, Article 19 (Jan. 2021), https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

her 2021 annual report on *The Right to Privacy in the Digital Age*, the UN High Commissioner for Human Rights notes that the "the use of emotion recognition systems by public authorities, for instance for singling out individuals for police stops or arrests or to assess the veracity of statements during interrogations, **risks undermining human rights, such as the rights to privacy, to liberty and to a fair trial**" and that a "risk-proportionate approach to legislation and regulation will require the prohibition of certain AI technologies, applications or use cases, where they would create potential or actual impacts that are not justified under international human rights law, including those that fail the necessity and proportionality tests."[34]

Similarly, in their Joint Opinion on the European Union's Artificial Intelligence Act, the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) state that the "use of AI to infer emotions of a natural person is highly undesirable and should be prohibited."[35] While the EDPB-EDPS statement further notes that exceptions should be made for "certain well-specified use-cases, namely for health or research purposes," **the fact that these systems are based on flawed scientific premises suggests that they should not be allowed in sensitive domains such as health**.[36]

A particularly acute risk to human rights occurs if emotion recognition systems are used to detect potentially dangerous or aggressive protests, leading to the arrest of these people before they have committed any aggressive act.[37] In such a case it wouldn't matter whether the inference was unreliable or not; the consequences of being arrested are real and would undermine our rights to freedom of expression and freedom of assembly.

IV. Automated Recognition of Gender and Sexual Orientation is a threat to LGBT+ people

Automatic Gender Recognition (AGR) aims to infer the gender of individuals from data collected about them. AGR uses information, like a legal name or the bone structure of your face, to infer your gender identity, often reducing it to a simplistic binary.[38]

Studies have shown that **women of color, particularly black and trans people are at a higher risk of misgendering.**[39] Furthermore, inferring gender on a binary scale erases the existence of non-binary

---

[34]UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/48/31, UN Human Rights Council, 48th Session (Sept. 13, 2021), https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx.
[35] Natasha Lomas, *EU's data protection adviser latest to call for ban on tracking ads*, TechCrunch (Nov. 19, 2021), https://techcrunch.com/2021/11/19/edpb-call-to-ban-tracking-ads/.
[36] *Id.*
[37] Thomas Macaulay, *British police to trial facial recognition system that detects your mood,* TNW News (Aug. 17, 2020) https://thenextweb.com/news/british-police-to-trial-facial-recognition-system-that-detects-your-mood
[38] OS Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, Proceedings of the ACM on Human-Computer Interaction (Nov. 2018), https://ironholds.org/resources/papers/agr_paper.pdf.
[39] http://gendershades.org.

people and has real world consequences. AGR not only fails to reflect any objective or scientific understanding of gender but it **indirectly symbolizes a form of erasure for people who are trans or non-binary**. Simply put: when you and your community are systematically misrepresented, your ability to advocate effectively for your human rights and freedoms are crippled.[40]

In 2021, hundreds of human rights groups, recording artists, and academics penned an open letter to Spotify, requesting that the company not use their recently patented technology to listen to users' conversations and recommend content based on their perceived emotions.[41] Spotify's speech-recognition patent[42] claims to be able to detect,[43] among other things, "emotional state, gender, age, or accent" to better recommend music. In other words, Spotify's technology uses emotion recognition and gender recognition to make inferences about what emotion a person is experiencing and what gender they are in order to recommend a song. According to the patent, the device would stay on all the time, constantly monitoring, processing voice data, and likely collecting sensitive information.[44] It would even be able to detect the number of people in a room.

Automated recognition of gender and sexual orientation can cause several harms to LGBT+ people. You could be interrogated at the airport if the system determines you don't match the gender marker in your passport. A trans person could be prohibited from access to gender-specific spaces like bathrooms and locker rooms. Authorities in repressive countries could analyze security camera footage or social media profiles to track down individuals they believe to be LGBT+ and arrest them.[45]

When biometric technology is used to infer gender it limits the ability of a person to self-identity[46] and puts companies in a dangerous position of power in relation to people using the service.[47] Spotify, for example, has an incentive to manipulate a person's emotions in a way that encourages them to

---

[40] Daniel Leufer, *Computers are binary, people are not: how AI systems undermine LGBTQ identity*, Access Now (Apr. 6, 2021), https://www.accessnow.org/how-ai-systems-undermine-lgbtq-identity/.
[41] Todd Feathers, *Artists Are Telling Spotify To Never Use 'Emotion Recognition,'* VICE News (May 5, 2021), https://www.vice.com/en/article/7kvvka/artists-are-telling-spotify-to-never-use-emotion-recognition.
[42] *Identification of taste attributes from an audio signal*, Justia (Feb. 21, 2018), https://patents.justia.com/patent/10891948.
[43] Mark Savage,*Spotify wants to suggest songs based on your emotions*, BBC News (Jan. 28, 2021) https://www.bbc.com/news/entertainment-arts-55839655.
[44] *Identification of taste attributes from an audio signal*, Justia (Feb. 21, 2018), https://patents.justia.com/patent/10891948.
[45] https://campaigns.allout.org/ban-AGSR.
[46] Veronica Arroyo and Daniel Leufer, *Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazi*l, Access Now (June 29, 2020), *https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil/*; see also Petition to Ban Automated Recognition of Gender and Sexual Orientation, Access Now, *https://act.accessnow.org/page/79916/action/1*.
[47] *Dear Spotify: don't manipulate our emotions*, Access Now (Apr. 15, 2021) https://www.accessnow.org/spotify-tech-emotion-manipulation/.

continue listening to content on its platform — which could look like playing on a person's depression to keep them depressed.[48]

V. Mandatory Digital Identity Programs using Biometric Recognition lead to Exclusionary Outcomes

Governments and companies around the world are leveraging biometric technologies to identify and authenticate ill-considered, badly designed, and poorly implemented digital identity programs.[49] Often, these digital identity programs are mandatory.[50] Most of these enrollment systems capture personal information along with biometrics. The introduction of such a program jeopardizes human rights, particularly for political and religious minorities, and exposes them to threats from third parties.[51] In many places, populations including refugees, transgender people, and those affected by HIV are forced to register in digital identity programs as a pre-condition to receiving aid.[52]

There are also many privacy concerns related to these digital identity programs. For example, a few months ago the Intercept[53] reported that **an Afghanistan Automated Biometric Identification System[54] maintained by the Afghan Ministry of the Interior *with* support from the U.S. government was seized by the Taliban**. The devices, known as HIIDE, for Handheld Interagency Identity Detection Equipment, collected sensitive biometric data (such as iris scans, fingerprints, and other biographical information) on Afghan criminals, terrorists and those who assisted the U.S. (or worked with the military).

---

[48] *Id*.

[49] https://www.accessnow.org/whyid/; see also Veronica Arroyo and Donna Wentworth, *We need to talk about digital ID: why the World Bank must recognize the harm in Afghanistan and beyond*, Access Now (Oct. 14, 2021), https://www.accessnow.org/digital-id-world-bank/

[50] *National Digital Identity Programmes: What's Next?*, Access Now (May 2018), https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf.; see also *Mandatory National IDs and Biometric Databases*, Electronic Frontier Foundation, https://www.eff.org/issues/national-ids.

[51] *Busting The Dangerous Myths Of Big Id Programs:Cautionary Lessons from India*, Access Now (Oct. 2021), https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf; see Carolyn Tackett and Naman M. Aggarwal, *Government responses to COVID-19 reinforce the need to ask — #WhyID?,* Access Now (Apr. 29, 2020) https://www.accessnow.org/government-responses-to-covid-19-reinforce-the-need-to-ask-whyid/; see also *Civil society organizations call for a full integration of human rights in the deployment of digital identification systems,* Access Now (Dec. 17, 2020), https://www.accessnow.org/civil-society-call-for-human-rights-in-digital-identification-systems/; *#WhyID: Digital health certificates are not immune from violating users' rights*, Access Now (July 22, 2020), https://www.accessnow.org/whyid-digital-health-certificates-are-not-immune-from-violating-users-rights/.

[52] *Iris scanning of refugees is disproportionate and dangerous — What's happening behind IrisGuard's closed doors?* Access Now (Apr. 12, 2021), https://www.accessnow.org/irisguard-refugees-jordan/.

[53] Ken Klippenstein and Sara Sirota,*The Taliban Have Seized U.S. Military Biometrics Devices*, The Intercept (Aug. 17, 2021), https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

[54] Mission Afghanistan: Biometrics, FBI (Apr. 29, 2011), https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.

VI. Biometric Recognition is Predicated on Mass Surveillance

Biometric recognition systems have the capacity to identify, follow, single out, and track people everywhere they go, undermining our human rights and civil liberties — including the rights to privacy and data protection, the right to freedom of expression, the right to free assembly and association (leading to the criminalization of protest and causing a chilling effect), and the rights to equality and non-discrimination..[55]

Still, many governments are eagerly purchasing the dangerous technology and ramping up implementation — even as the movement to ban facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance gains traction worldwide. [56] Biometric recognition technologies have already enabled a litany of human rights abuses including the right to privacy and right to free assembly and association not only in the United States, but China, Russia, England, Kenya, Slovenia, Myanmar, Israel, India, and the United Arab Emirates.[57]

Wrongful arrests, in the United States, as well as in Argentina, and Brazil have undermined people's right to privacy and their rights to due process and freedom of movement. So far, three black men have been wrongfully arrested based on flawed facial recognition in the United States.[58] Similarly, the surveillance of ethnic and religious minorities and other marginalized and oppressed people in China, Thailand, and Italy have violated people's right to privacy and their rights to equality and non-discrimination.[59]

Access Now, along with 193 civil society organisations from 63 countries around the world, call for a ban on the use of these technologies in publicly accessible spaces because even though a moratorium could put a temporary stop to the development and use of these technologies, and buy time to gather evidence and organize democratic discussion, it is already clear that these investigations and discussions will only further demonstrate that the use of these technologies in publicly accessible spaces is incompatible with our human rights and civil liberties and must be banned outright and for good.

---

[55] *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*, Access Now (Jun. 7, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.
[56] *Id*; see also Veronica Arroyo and Gaspar Pisanu, *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*, Access Now (Aug. 8, 2021), https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/.
[57] *See Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*.
[58] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, New York Times (Jan 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
[59] *Id*.; See also *Alibaba facial recognition tech specifically picks out Uighur minority*, Reuters (Dec. 17, 2020) https://www.reuters.com/article/us-alibaba-surveillance-idUKKBN28R0IR; Laura Carrer, Riccardo Coluccini, Philip Di Salvo, *Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale*, WIRED (Sept. 9, 2020), https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/?refresh_ce=.

Facial recognition and remote biometric recognition technologies have significant technical flaws in their current forms, including, for example, facial recognition systems that reflect racial bias and are less accurate for people with darker skin tones. However, technical improvements to these systems will not eliminate the threat they pose to our human rights and civil liberties.

While adding more diverse training data or taking other measures to improve accuracy may address some current issues with these systems, this will ultimately only perfect them as instruments of surveillance and make them more effective at undermining our rights.

Recommendations to the OSTP

Human rights harms are inevitable when we allow companies to sell flawed technology. Without a robust process to validate the claims made by corporations selling these systems, we risk a proliferation of pseudoscientific technologies, damaging consumer confidence and public trust. For all these reasons**, we encourage the White House to use its *full* authority to protect persons against biometric systems**. This includes urging companies to stop the use of these technologies in public spaces, publicly-accessible spaces, and places of public accommodation, where such use could enable mass surveillance or discriminatory targeted surveillance, including but not limited to their use in parks, schools, libraries, workplaces, transport hubs, sports stadiums, and housing developments. **Some biometric technologies must be banned outright, such as automated gender recognition and AI-based "detection" of sexual orientation.** These systems cannot be fixed by simply introducing more diverse training data, increasing accuracy, or applying technical methods to reduce bias; the fundamental aim of these systems is incompatible with human rights.

Respectfully Submitted,

Willmary Escoto
U.S. Policy Analyst
Access Now

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

ACT | The App Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Suresh Venkatasubramanian
Assistant Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, District of Columbia 20504

RE: ACT | The App Association Response to the Request for Information Regarding Public and Private Sector Uses of Biometric Technologies

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit input in response to the Office of Science and Technology Policy's (OSTP) Request for Information (RFI) regarding public and private sector uses of biometric information. The App Association thanks OSTP for soliciting feedback from a broad range of stakeholders on this important issue, as the potential benefits and impacts that flow from the use of biometric information are substantial and will require careful deliberation to be fully understood.

The App Association represents thousands of small business software application development companies and technology firms in the United States and abroad. These companies create technologies that generate internet of things (IoT) use cases across consumer and enterprise contexts and are primary drivers of the global digital economy. Today, the App Association represents an ecosystem valued at approximately $1.7 trillion and that is responsible for 5.9 million American jobs.

Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure, particularly their sensitive biometric data. The small business developer community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and, as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity.

[redacted] [redacted]

The App Association serves as a leading resource in the biometrics and privacy space for thought leadership and education for the global small business technology developer community.[1] We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and useable guidance to ease the burden of compliance.[2]

II. Responses to the Request for Information

OSTP's RFI asks for input regarding two separate, but related, categories of biometric technologies: 1) biometric recognition, which includes *verification* (one-to-one biometric matching) and *identification* (one-to-many queries that match an individual input against a larger database); and 2) biometric inference of cognitive and/or emotional states, such as mood or attentiveness. Below, we include some findings on the two categories.

Biometric Recognition

App Association members currently leverage numerous innovative biometric-assisted technologies, including facial verification, in order to provide services consumers need and demand in the digital economy. Facial verification involves the comparison of a baseline, or "gallery," image against another image, the "comparison" or "probe" image, sometimes provided by the consumer's own device or by a device managed by the entity carrying out the comparison. Facial verification technologies are most often used for security purposes, i.e., to verify whether a person really is who they say they are. To share one key use case, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log-in to apps using a scan of their face from the camera app. An app developer can choose integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.[3]

[1] *See e.g., ACT | The App Association, Innovators Network Foundation Announces Inaugural Privacy Fellows* (September 2019), available at: https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/

[2] *See e.g.*, *What is the California Consumer Privacy Act (January 2020),* available at: https://actonline.org/wp-content/uploads/What-is-CCPA.pdf; *The App Association's Visual Guide to Facial Recognition Use-Cases* (June 2020), available at: https://actonline.org/2020/06/18/the-app-associations-visual-guide-to-facial-recognition-use-cases/; *About-Face: The Year in Facial Recognition and Trends to Watch in 2021* (February 2021), available at: https://actonline.org/2021/02/03/about-face-the-year-in-facial-recognition-and-trends-to-watch-in-2021/

[3] Apple, "About Face ID advanced technology", September 14, 2021, https://support.apple.com/en-us/HT208108

In recent years, academic and media reports have questioned the ethics and efficacy of various facial recognition technologies.[4] Often those reports discuss facial *identification*, the sub-set of facial recognition technologies that match an individual against a much larger database of images and which have struggled with accuracy rates, bias, and questionable deployment strategies.[5] Facial verification programs, by contrast, are much more limited in scope and typically prove highly-reliable in testing. In its most recent Facial Recognition Vendor Test, the National Institute for Standards and Technology (NIST) found that the highest performing facial verification algorithms can achieve accuracy rates as high as 99.97 percent.[6] While those accuracy rates tend to drop when the image collection occurs in less controlled environments (for example, verification via cameras in a crowded airport terminal), collection for a use case like Face ID is typically well-controlled. Notably, many facial identification algorithms also perform increasingly well on recent NIST tests, some showing marked improvements over just the past few years since the negative reports first surfaced. In its latest assessment of facial identification algorithms, NIST concluded that "at least 30 developers' algorithms outperformed the most accurate algorithm from late 2013."[7]

As the underlying technology continues to improve, app developers are likely to implement a greater variety of facial recognition use-cases. Therefore, it will become increasingly important that regulation ensure that appropriate governance and accountability structures attach to each use case commensurate with its risk. For example, in existing risk frameworks created by academics, targeted use of facial verification algorithms on a one-to-one basis typically represents a lower risk deployment, whereas real-time deployment of facial identification in public spaces is among the highest.[8]

[4] *See e.g.,* Joy Buolamwini and Timnit Gebru "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research 81:1–15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", ACLU, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

[5] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[6] NIST Facial Recognition Vendor Test, "N Identification", December 2021, https://pages.nist.gov/frvt/html/frvt1N.html

[7] NIST Facial Recognition Vendor Test, "Part 2: Identification", November 2021, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

[8] Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Risk Framework", Georgetown Center Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/risk-framework

[redacted] [redacted]

The App Association supports legislation to limit particularly risky uses of facial recognition technology and consistently advocates for a federal privacy law that would limit how companies can process consumer data without their consent.[9] Crafting rules that differentiate between targeted, consent-based uses of biometrics versus dragnet applications will be an important task for regulators going forward.

Biometric Inferences of Cognitive or Emotional States

The collection of biometrics, including inputs that relate to or can infer cognitive or emotional states, holds both great promise and risk as one element in broader efforts to improve the quality of patient care in the United States. Through our Connected Health Initiative (CHI), the App Association seeks to advance responsible pro-digital health policies and laws that can harness the great potential of connected healthcare devices and tools, some of which may leverage biometric inputs, to unlock a higher standard of care for patients while minimizing potential harms.

One of the most exciting potential benefits of connected health technology is the ability of wearable devices that capture biometrics to improve equitable outcomes in healthcare. As co-creator of the Health Equity and Access Leadership (HEAL) Coalition, a group comprising about 35 organizations spanning the health ecosystem, CHI recently released a report highlighting how wearable devices, among other innovations, can contribute to reducing the divides in health outcomes across racial lines. As the report points out, access to traditional healthcare facilities, often stratified along income and racial lines, remains one of the major social determinants of health. The remote collection of health data through wearables can help ameliorate some of those disparities in access by allowing personalized diagnostics to occur outside of traditional healthcare institutions. For example, fitness trackers that collect valuable data, such as sleep patterns, activity, and stress levels, can automatically share relevant information with clinicians, therapists, or coaches so that they can use granularized data to create more personalized care routines without requiring an in-person visit.

[9] ACT | The App Association, “Testimony of Morgan Reed, President at ACT | The App Association Before the U.S. Senate Committee on Commerce, Science, and Transportation on Protecting Consumer Privacy”, September 19, 2021, https://actonline.org/wp-content/uploads/Reed-Testimony.pdf

Connected health technologies that make use of biometrics to recommend cognitive or behavioral changes show efficacy in a number of different contexts to date. For example, a trial of a mobile phone application that creates personalized behavioral interventions, including behavioral coaching, to improve for blood glucose control resulted in "substantially reduced glycated hemoglobin levels over 1 year."[10] The WellDoc mobile diabetes management platform also showed statistically significant improvements in A1c, in part due to behavioral recommendations.[11] Some studies have also shown significant mental health improvements among users of certain mental health apps, depending on the level of engagement of the user.[12]

In light of the COIVD-19 pandemic, many have turned to digital health platforms, tools, and services to consult with caregivers in greater numbers as in an effort to avoid the risk of exposing themselves or others to the virus. Wearable ownership and use increased in 2020, with 43 percent of respondents using wearables in 2020, compared to 33 percent in the year prior.[13] Additionally, since the beginning of the COVID-19 pandemic, more than half of all owners and users of wearables reported using them to manage a diagnosed health condition.[14] Sixty-two percent of physicians reported in a recent study that they believe wearable devices would increase the overall quality of care for their patients.[15]

[10] Quinn et al., "Cluster-Randomized Trial of a Mobile Phone Personalized Behavioral Intervention for Blood Glucose Control", Diabetes Care, September 1 2011; 34 (9): 1934–1942, https://doi.org/10.2337/dc11-0366 https://diabetesjournals.org/care/article/34/9/1934/38702/Cluster-Randomized-Trial-of-a-Mobile-Phone

[11] Quinn et al., "WellDoc™ Mobile Diabetes Management Randomized Controlled Trial: Change in Clinical and Behavioral Outcomes and Patient and Physician Satisfaction", *Diabetes Technology & Therapeutics,* Vol. 10, No. 3 May 12, 2018, https://www.liebertpub.com/doi/pdf/10.1089/dia.2008.0283

[12] David Bakker and Nikki Rickard, "Engagement in mobile phone app for self-monitoring of emotional wellbeing predicts changes in mental health: MoodPrism", *Journal of Affective Disorders,* VoL. 227, p. 432-42, February 2018, https://www.sciencedirect.com/science/article/abs/pii/S0165032717316786

[13] Rock Health, "Digital Health Consumer Adoption Report 2020", February 26, 2021, https://rockhealth.com/insights/digital-health-consumer-adoption-report-2020/

[14] Ibid.

[15] Nersi Nazari, "5 Key Attributes For Medical Wearables Seeking Adoption By Hospitals", Vital Connect, October 20, 2017: https://vitalconnect.com/5-key-attributes-medical-wearables-seeking-adoption-hospitals/

[redacted] [redacted]

Clearly, usership of technologies that can pull biometrics and infer cognitive or emotional states will continue to increase, especially as efficacy improves and the benefits become clearer to users. The App Association is keenly aware of the need to create appropriate guardrails to keep up with the growth of the industry and to ensure that mobile health players that collect sensitive biometric data continue to do so responsibly. Aside from advocating federal privacy legislation, as mentioned earlier, the App Association continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of such AI innovations, including by developing Good Machine Learning Practices specifically for AI development and risk management of AI.[16]

III. Conclusion

The App Association strongly supports risk-based guardrails around the use of biometrics that provide consumers and patients with a baseline level of trust and that set a clear set of expectations for the businesses that seek to do good through these services. While the technology offers incredible potential, we understand the risks of misuse are particularly high in this context.

We thank OSTP in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,

[redacted]

Brian Scarpelli
Senior Global Policy Counsel

Matt Schwartz
Policy Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
e: [redacted]

[16] CHI's Good Machine Learning Practices are available at https://bit.ly/3gcar1e.

[redacted] [redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

AHIP

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Guiding Greater Health

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

[redacted]

ahip.org

Matthew Eyles
President & Chief Executive Officer

January 15, 2022

Submitted Via Email: BiometricRFI@ostp.eop.gov

The White House
Office of Science and Technology Policy
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Request for Information (RFI) Response: Biometric Technologies

Dear White House Representative:

Every American deserves the peace of mind of knowing that their personal health information is used appropriately and protected. For years, health insurance providers have supported this commitment, and that is why AHIP appreciates the opportunity to provide comments on the Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.

We provide information in response to the RFI about various health uses of these technologies, including by some health insurance providers. Our comments also address themes from the recently held OSTP Listening Sessions that sought public input on the future development of an Artificial Intelligence (AI) Bill of Rights to help avoid potential harmful consequences to individuals due to the use of biometric data.

AHIP applauds OSTP for taking a proactive approach to advance responsible AI for Americans. We will stay engaged as your office continues to explore the potential development of an AI Bill of Rights.

AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone. With that experience and perspective, AHIP has been collaborating with public and private entities to lead the way in protecting consumers and advancing trustworthy AI. Our work includes:

- Participation with the U.S. Chamber of Commerce to develop AI principles for how American businesses serve consumers.
- Collaboration with the Consumer Technology Association in developing its new Trustworthiness Standard for AI in Health Care.

- Engagement with the National Association of Insurance Commissioners in their work related to the use of AI in insurance, mitigating bias in AI and pending Principles for Data Collection.
- Working closely on an ongoing basis with the Confidentiality Coalition to address AI policies and potential legislation and regulations.

Health Insurance Providers Use AI and Biometrics to Improve Care and Minimize Fraud

Health insurance providers currently use AI and biometric technologies to benefit patients and consumers, improving care and creating efficiencies while minimizing opportunities for fraud. However, we believe the full extent of the benefits of AI applications, including the use of biometric technologies within these models, have yet to be realized.

Some examples of how health insurance providers use AI include:

- ***Clinical models*** to understand health conditions through clinical research programs.
- ***Predictive analytics*** to identify patients who may benefit from improved access to services (based on metrics other than historical spending).
- ***Physician performance*** to identify high-value care for use in consumer choice and network design.
- ***Service models*** to enhance the customer experience.
- ***Market research regarding prospective employer sponsors of health insurance*** to help determine which employers might align with a company's product offerings, value, areas of access, or health care networks.
- ***Actuarial analysis*** to help identify utilization patterns (not individually identifiable) for an employer or other health plan sponsor to understand usage trends both now and for the future.
- ***Claims analysis*** *to* identify potential fraud and abuse.

Additional examples that specifically highlight specific uses of biometric technologies in healthcare and by health insurance providers can include:

- ***Voice biomarkers*** to improve care by identifying patient needs, authenticating users, and detecting emergencies.
- ***Clinical vocal biomarkers*** for health tracking, detection and triage, as a diagnostic aid, risk prediction, to assess discharge readiness, and as a remote patient monitoring tool.
- ***Voice recognition*** to improve human-to-human interaction by capturing notes and supporting care teams (e.g., authorized user dictation). Combined with AI, voice recognition can leverage data from visits to provide care recommendations to providers (e.g., at the point of care in a health setting), as well as potentially expedite claims processing.
- ***Clinical diagnostic data*** with applied- AI can augment the ability to pinpoint diseases, monitor conditions, and establish tailored care paths. For example, this may include genetic testing results in combination with clinical imaging using biomarkers for specific cancer types (i.e., detection and diagnosis) to assist with determining which therapies would be best suited for an individual.

- ***Fingerprint and facial biomarkers*** (i.e., retinal scans or facial recognition) can be appropriately applied to expedite authentication and access. For example, leveraging fingerprint or facial recognition technology, alongside user consent to use and transparency around such applications, to log into phones and devices to access information and programs can enable efficient authentication and access the person requesting access, such as consumers accessing their phone, plan members using a medical device, or provider-partners accessing medical platforms in a secure way particular to the individual.
- ***Personal characteristics*** captured in vision, audio and natural language processing models can aid in identifying conditions. For example, models can assess body language, gait, word choice, pupil dilation and other factors while an individual answers questions for an avatar or performs an action.

Recommendations for Considering an AI Bill of Rights for Americans

- As AI continues to advance, we recognize there may be challenges and new areas to explore. Health insurance providers are seeking ways in which they can allow consumers to direct how their information is used, improve privacy and security, mitigate potential implicit data bias, establish governance best practices, and achieve other shared objectives. We recommend that as OSTP continues to consider the development of an AI Bill of Rights, future discussions should explore:

- **Educating consumers about the uses of the technologies, along with the potential benefits and risks.** Consumers should know what AI is and how it is used in public and private sectors (e.g., how consumers will interact with and utilize AI-powered tools in different or intersecting sectors). **Consumers should also have resources on the benefits** (e.g., privacy and security) **and potential drawbacks that may be associated with some of those uses** (e.g., data breach, data scraping, loss of privacy, secondary uses of data)**.** Americans will be more likely to trust AI-powered services if they can clearly obtain relevant information and benefit from its utility.

- **Preventing harmful intended bias and taking actions to address potential unintended bias**. Depending on the application, understanding and being transparent about potential bias in AI is the first step toward mitigating unintended consequences. Context is crucial in determining how to address potential "bias" in the use of AI. For example, some AI initiatives are designed to benefit specific groups or populations, which might be considered "good bias," even though the approach is deliberate and beneficial. In other words, we need to be able to distinguish between different approaches to ensure that important efforts to avoid harmful bias, do not impede deliberate and beneficial efforts to identify and benefit an underserved group or population. Engaging a diverse set of stakeholders who will be impacted by the AI in the design of the use cases is a good way to better understand AI programs, promote beneficial advancements, and mitigate harmful unintended outcomes as much as possible.

- **Ensuring that governance programs, practices or procedures can be applicable to the context, scope, and data use of a specific use case.** AI efforts exist against an

important backdrop of existing laws. There may well be benefit from voluntary activities among industry participants, such as principles or best practices. Areas for such legal or potential industry guidance include: data privacy and consent, transparency that a biometric technology is being used and for what purpose, and the right for a user to opt out. Governance is essential for engaging public trust, a consistent framework across applications, and appropriate and ethical use of the technologies. Likewise, program design will be a key element for AI, as well as how automated and supported decision-making by AI directly relate to the key governance rules.

- **Focusing on consumer understanding and the effective use of the technology.** Public and private entity uses should be disclosed. Federal agencies, including the National Institute of Standards and Technology (NIST) and others can help inform new regulatory proposals, which should align with the work of OSTP. To date, NIST has been a federal leader in this area and should serve as a resource for individuals and entities as substantive and technical policies are developed and adopted.

- **Making policy makers and the public aware of the AI functions in current systems, and existing measures to ensure fairness and effectiveness throughout use and application.** We must balance benefits from AI against the associated risks and design policies that seek to mitigate those risks in a way that least interferes with beneficial innovation.

- **Staying ahead of foreign actors and governments** that attempt to leverage the technology to outpace the United States from a competitive standpoint or nefarious activities, and **ensuring that foreign actors and governments, and U.S.-based public and private entities do not exploit the privacy and security of individuals.**

The use of AI and biometric technologies hold great promise for improving health care for everyone. We can work together to address the challenges and ensure patients are protected while promoting innovation. Engaging a diverse set of stakeholders is essential to success, and AHIP and our health insurance provider members are eager to work with you and other stakeholders on these important efforts.

Please contact me at [redacted] if you have any questions and for future engagement.

Sincerely,

[redacted]

Matthew Eyles
President & Chief Executive Officer

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Alethicist.org

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Why was your job application rejected? Bias in Recruitment Algorithms

Humans are biased and so can be the algorithms they develop and the data they use, but what does that mean to you as a job applicant coming out of school or looking to move up to the next step in career ladder or considering a change in roles or industry. What does that mean for society?

In the fast-moving world of technology, AI has particularly expanded into many domains of our personal and business life. Whether you are aware of it or not, algorithmic decision-making systems are now prominently used by companies as well as governments to make decisions on credit worthiness, housing, recruitment, immigration, healthcare, criminal justice system, pricing of goods, welfare eligibility, college admissions – just to name a few. Despite the high stakes and high impact of these decisions on an individual (not to mention the society as a whole), the landscape still greatly lags behind in developing oversight, transparency and accountability measures around these algorithmic systems.[1]

Recruitment has always been one of those areas where people always run the risk of being on the receiving end of a biased decision. Given the historical context on discrimination in recruitment, there are a number of legislation actions which provide guidelines and red lines to organizations to make better choices. Title VII of the Civil Rights Act (Civil Rights Act, 1964) for example, prohibits discrimination based on "race, color, religion, sex, or national origin" that would result in disparate treatment or disparate impact. It also puts the liability and legal responsibility on employers to ensure that the tools being used are not creating such results. Moving inside the organizations, in an effort to be more fair, equitable and diverse many companies have taken upon themselves to improve their hiring processes and eliminate as much as possible perceived legacy structural issues through new technology. There is still a long way to go for both the legislation as well as the products and business processes to create more objective and less biased decisions in hiring. Today, companies find AI tools which are used in the full spectrum of hiring process attractive without understanding the potential issues these products might create, or without considering how these results might actually be in complete disagreement with what they want to do with their workforce and future.

[1] Adapted from original article by the author published in Medium, and Montreal AI Ethics Institute blog.

The attractiveness of AI-powered recruitment products come from the fact they help companies reach multiple times more candidates than they could reach with the more traditional ways (corporate career websites, referral programs etc.). On the same token, they also make it extremely easy for prospective candidates to submit their CVs to multiple roles at a time with the click of a button. The result is a mutual technology escalation from both the employers and candidates. Once the net is cast, these products help the companies to efficiently process those candidates through the recruitment funnel. The ability to process hundreds of applications in a matter of minutes with an automated system is not only a great benefit in terms of scalability but it also reduces the time to hire and hence potentially the cost to hire (assuming the choices were right) and gives hiring teams more space to develop strategies rather than constantly trying to stay on top of hiring transactions.

One other way these AI recruitment products are marketed is as an alternative to the biased decisions of hiring managers and recruiters and thus to provide a more standard processing of applications. The big issue with this statement is algorithms are not independent of their creators and their biases, nor are they independent of the historical data used to build its models. Algorithms are created by people, about people, for people. In other words, *"*Algorithms are opinions embedded in code" (Cathy O'Neill, 2017) For long years now, companies have rolled out a number of initiatives to fight the subject and biased decisions involved in hiring decisions. These included training recruiters and hiring managers about unconscious bias so they would be aware of their bias and intentionally and proactively make decisions which are more objective; blinding/hiding certain fields in resumes or applications so hiring managers would not be biased with names, addresses, universities etc; forcing hiring manager and recruiters to have an equal number of male and female candidates in each stage of the recruitment funnel; creating roundtables of hiring committees where candidates are scored against objective criteria and the committee challenges each other on their scores. All these initiatives have some merit in them, but the success varies with the intensity of the effort as well as the culture of the organization trying to make a change. So, when AI systems have potential to reduce bias and reduce cost at the same time, the kneejerk reaction of some companies to jump on wagon without asking too many questions is only too natural.

The AI application in each stage of recruitment may be a recommender system using "collaborative filtering" which makes recommendations based on historic preference of multiple users for items (clicked, liked, rated, etc.), or a "content-based" recommendation by matching for example key

words in your profile or resume. The algorithm might also be a predictive system which uses historical data to find trends or patterns which are then used to predict usually the future, or the likelihood of something happening (for example analyzing the characteristics of applicants who were hired previously and predict your alignment with their success factors, and hence your future success in the job accordingly). It can generate scores or rankings for example for individuals. Alternatively, the AI system might be using a classification algorithm where it maps the input data (in this case candidates) into different categories or clusters. Imagine the recommender systems as Netflix/Pandora where the machine learning algorithm tries to learn your taste and choice by looking at your historical behavior interacting with that app, and it also analyses people whose choices are similar as yours and refines its recommendation; and the predictive systems as your credit scoring.

It is extremely crucial to remember that with AI systems any outcome or prediction is based upon the training data fed into the system. Nature, context and quality of training data for predictive tools can vary, ranging from click patterns, to historical application data, to past hiring decisions, to performance evaluations and productivity measures.

When you add the errors and biased decisions humans made in the past which made up the dataset to the efficiency of the AI systems, you can appreciate how algorithms can magnify the biased decisions. As they are quoting Timothy Wilson (Strangers to Ourselves (2004) in their paper the authors of "Discrimination In The Age Of Algorithms" (Kleinberg & Jens Ludwig & Sendhil Mullainathan & Cass R. Sunstein, 2019) suggest when humans are making decisions, "many choices happen automatically; the influences of choice can be subconscious; and the rationales we produce are constructed after the fact and on the fly". The researchers than suggest "the black-box nature of the human mind also means that we cannot easily simulate counterfactuals. If hiring managers cannot fully understand why they did what they did, how can even a cooperative manager answer a hypothetical about how he would have proceeded if an applicant had been of a different race or gender" (Kleinberg et al, 2019). The historical record does not help the case for objectivity or fairness with regards to the employers either. In their analysis of trends in discrimination by performing a meta-analysis on 24 field experiments performed between 1990-2015, which included data from more than 54,000 applications across more than 25,000 positions, Quillian and etc al found there were no changes in hiring rates over time for black applicants over the last 25 years. *(*Quillian, Pager, Hexel, Midtbøen, 2017). In the words of Meredith Whittaker,

co-founder of the AI Now Institute, “AI is not impartial or neutral. In the case of systems meant to automate candidate search and hiring, we need to ask ourselves: What assumptions about worth, ability and potential do these systems reflect and reproduce? Who was at the table when these assumptions were encoded?” (Rosenbaum, 2018)

The following is a step-by-step review of recruitment funnel activities bias can enter the process and result in unintended outcomes.

TARGETING:

This is the step when a recruiter tries to cast as wide as a net to the active and passive applicants which would be a strong match to the position that he/she is hiring for. In the digital age, this process has moved from advertising open positions and job descriptions in a company’s corporate website and company profile to publishing it in different career platforms, and general and niche job boards. For any candidate, active or passive, it is crucial the person sees the posting and hence is aware of the opportunity. If you are not aware of the opportunity in the first place, your chances of getting the role is close to nil.

The data collected from your overall online activity provides the platforms with a way to create groups of users with shared attributes (or characteristics, preferences, interests, etc). Today employers have access to the same microtargeting tools advertisers long had on these job boards (like LinkedIn, Glassdoor, ZipRecruiter, Upsider to name just a few of the most known ones). They can select a number of targeting criteria like job seniority, age, gender, degree, etc, and advertise the job opening to candidates in the board’s database.

In 2018, Facebook faced a lawsuit which alleged the social media platform’s practice of allowing job advertisers to consciously target online users by gender, race, and zip code constituted evidence of intentional discrimination (Heater, 2019). Notwithstanding the bias of the recruiter in selecting those criteria and their relevance to job success, the machine learning algorithm in these criteria can collect data on users’ search histories or demographics and use algorithms to predict which individuals companies might want to recruit and only show job postings to those candidates. So as an active or passive candidate if your previous job clicks were significantly more in say junior positions, or in a certain department, the chances you will be targeted for the new job opening are smaller for more senior positions or in different departments. The algorithm also learns from the

recruiter's behavior and which previous criteria was clicked and used more in previous postings and suggests those to the recruiter. If you are not intentionally making an effort to go over each criterion and verify it, soon your former behavior becomes a personalized default. "It's part of a cycle: How people perceive things affects the search results, which affect how people perceive things," Cynthia Matuszek, a computer ethics professor at University of Maryland and co-author of a study on gender bias in Google image search results says (Carpenter, 2015).

Facebook also offers a tool called "lookalike audience" where an employer, might provide Facebook data on its current employees. As Pauline Kim describes it, Facebook takes the source audience, analyzes data about them and identifies other users who have similar profiles, and targets ads to this "lookalike" group to help employers predict which users are most likely to apply for their jobs (Kim, 2018)

On top of all these, the digital marketing platforms like Google or Facebook use their own marketing algorithms to decide which ads are more likely to be clicked by which users within each of their user groups. So just because a recruiter selected 'all females in Chicago with 10 years of work experience in consulting' does not mean all those females who fit in that category will see the job posting in their feeds. One experiment by the Carnegie Mellon researchers showed that Google displayed adverts for a career coaching service for "$200k+" executive jobs 1,852 times to the male group and only 318 times to the female group So in other words, these platforms run their own predictions and further narrow the visibility of a job posting (Vincent, 2015)

MATCHING & SOURCING:

If your application made it to the next stage where the candidates are filtered on how much they aligned with the recruiter's choices, the next set of bias arises from how the algorithm is structured in a way that rank-ordered lists and numerical scores may influence recruiters (Bogen and Rieke, 2018). If a recruiter sees a 95% compatibility vs an 85% compatibility to the job posting, he/she might not even bother to compare the two applications and actually read the totality of the resumes. This issue might snowball further if say the results show only the 10 top ranked applicants per page versus more and the recruiter does not even click to see the rest. On a separate note, when predictions, numerical scores, or rankings are presented as precise and objective, recruiters may give them more weight than they truly warrant, or more deference than a vendor intended (Joachims, Granka, Pan, Hembrooke, and Gay, 2005,) The problem of the algorithm learning from

the recruiter's previous use of filters for candidate matching (i.e. location, skill, previous company, within x mile radius) is also present in this stage and make future recommendations accordingly.

SCREENING:

So let's assume your application was one of the ones ranked high in the matching and sourcing platform, and the recruiter clicked your name to process you in to the next stage where you are screened against the company's preferred criteria. Whether it is through hard-coded questions and filters built into the system, or machine learning algorithms which make decisions, the screening process helps to reduce the number of applications as it goes through your CV / resume and picks up the skills and information (degree, GPA, years of experience, fluency in spoken or technical languages, etc). Whatever the software was able to read (or parse) from your CV, the data points are then matched with the desired points for the specific role. The candidates who have matching points may then again be ranked according to the degree or percentage of match. However, the bigger bias issues in this stage have to do with data out of which the algorithm was created and what kind of a model makes the predictions.

One way to create the datasets by the AI vendors is to scrape data online or buy commercially available datasets – which means a lot of the vendors are using the same data sets. Volume does not mean quality, however. In 2016, Microsoft and Boston University researchers revealed that the Word2Vec (publicly available algorithmic model built on millions of words scraped from online Google News articles, which computer scientists commonly use to analyze word associations) model trained itself on gender stereotypes existing in online news sources (Bolukbasi, 2016). The other finding from the study was these biased word associations were overwhelmingly job related. For example, Man Is to Computer Programmer as Woman is to Homemaker. The data used in training might not have a fair representation in the first place and have embedded bias and imbalances in it, or even if it is perfectly clean it might not be representative of the population you are targeting. In other words, the dataset collected in US might not make a sense if you are a recruiter trying to use this algorithm in Southeast Asia.

Another approach to create the dataset and then the criteria upon which the model is based can be used to look at an organization's current and past workforce (and/or applicant pool) and determine the success stories and create a model (baseline criteria) based on what "worked" in the past. This is a customized model for the specific employer. However, defining what "worked" or what defines a "successful" employee is also a biased process in itself. What does the client value?

Sales numbers? Cultural fit? Retention? And crucially, what data does the client have? (Raghavan et al, 2020)

"Cultural fit" is a term which is used so frequently we forget it is a subjective measure. It is a better way of saying we will hire people who are like us, or we will not step out of our comfort zones. However, we do not question the possibility the culture might have kept some diverse talent outside the equation; or what if the culture has kept some of its own employees at bottom due to biases within the organization. The performance management evaluations are themselves be biased and subjective if not structured properly with objectively measurable criteria. Long tenure in an organization is usually considered another metric of success. However, what if the employee has been with the company for more than 10 years because he/she did not want to learn new things and was content with doing the same thing over and over again, or did not get any outside offers all that time because there was not anything particularly successful to grab attention. Usually a successful long tenure in a company means the employee has been promoted during the time or has taken on more responsibility, which is absolutely a sign of success. So, a basic calculation looking at time in an organization without looking at the more nuanced changes should not be the criteria for success. In the same token, gaps in employment should also not be held against an applicant. The applicant might have a disability or another circumstance which required him/her to take time off from work. The machine learning algorithm Amazon had built for its own hiring purposes using its own job applicant data since 2014 had to be scraped by the company when it realized the algorithm was biased. The models were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period. However, the database was a reflection of the heavy male dominance across the tech industry. In effect, Amazon's system taught itself male candidates were preferable. The algorithm penalized resumes which included the word "women's," as in "women's chess club captain." To the company's credit, it did not keep pushing the use of product when it noticed the bias despite all the investment made on the system. However, it is a good reminder and case study for us when looking at bias in dataset. We need to remember that even when sensitive/protected characteristics (like race, gender, age, etc.) are explicitly ignored in the model, there can still be some data points which can be proxies for these characteristics (zip code, college name, etc..), which can still reflect the same systematic injustices and bias in the dataset. Long story short, predictions based on historical data of a company for a customized tool can further deepen the underrepresentation of females, non-binary applicants,

ethnic minorities, people with disabilities and so on – exactly the type of issue the company wishes to avoid or correct in the first place.

ASSESSMENT:

Assessment stage is where applicants are asked to go through different exercises to understand their fit for a certain role. In a traditional sense, the assessment step might include interviews, simulations, case studies, tests or games. The main types of algorithmic assessment tools are focused on facial, speech or emotion analysis during candidates' interviews or gamified tests on the other. In their research of evaluating the claims and practices of 18 vendors of algorithmic pre-employment assessment, Raghavan (and et al, 2020) cite lack of publicly available information, and lack of information about the validity of these assessments as biggest obstacles to empirically characterizing industry practices. This holds true for most of the assessment algorithms used in the market today.

Inferred traits may not actually have any causal relationship with performance, and at worst, could be entirely circumstantial (Bogen and Rieke, 2018). In other words, the correlations which the algorithms found to build a model, or the traits which the developers built into coding may have nothing to do with a person's success on the job. So not only we are faced with a black box when it comes to these algorithms (i.e. the workings of the algorithm is not understood or can be explained), but even if we had access to the code and the algorithm itself was explainable, the explanation might not necessarily mean anything.

As Reema Patel, head of public engagement at the Ada Lovelace Institute, puts it "There's no data that demonstrates that facial recognition technology to profile people works, and effectively, what we're looking at is a form of pseudoscience that has a potential risk of discriminating against disabled people" (Lee, 2019). The assessment may not work well for people with differences in facial features and expressions if they were not considered when gathering training data and evaluating models; body recognition systems may not work well for a person with disability characterized by body shape, posture, or mobility differences; or analysis tools which attempt to infer emotional state from prosodic features are likely to fail for speakers with atypical prosody, such as people with autism (Guo, Kamar, Vaughan, Wallach, Morris. 2019)

Put aside the fact 1 billion people, or 15% of the world's population, experience some form of disability according to World Bank and the fact there is not enough work done to solve all the

different biases this population faces, the algorithmic bias in assessment tools does not stop with only the those with disabilities.

EPIC filed a complaint with the FTC alleging that recruiting company HireVue has committed unfair and deceptive practices in violation of the FTC Act. use of micro-expression matching (analyzing the candidate's facial expressions, their gestures, whether they're making eye contact, their body language, their speaking speed and the candidate's choice of words). Yes, HireVue is the most commonly cited example in this category, but it is far from being the only one. Micro-expression matching or analysis also works against those applicants whose native language is different than the language used in the tool; or the facial analysis systems struggle to read the faces of women with darker skin (Buolamwini and Gebru. 2018). As a result, the system either filters out all these candidates either as not fit for hiring, or erroneously flags their data as invalid outliers. Vendors like Faception, a facial personality analytics tool, suggests their proprietary computer vision and machine learning technology can profile people and reveal their personality based only on their facial image; claiming they can tell if a person has a high IQ, or is more likely an academic researcher, or terrorist. I will constrain from myself from going in a deep dive argument of what sounds like phrenology, a Lombroso-ist approach and the whole unscientific and malevolent aspects of this approach. However, it does raise a red flag because this vendor also lists smart cities, recruitment, retail and insurance in its product verticals.

SOCIAL PROFILE AGGREGATION:

Let's say a candidate has gone through all these stages and is shortlisted for a job offer. Despite the fact a number of states ban employers from looking at candidate's social profiles to get more information, not all states or countries do. A number of algorithmic tools can now scrape all your social profiles and post on the internet and make recommendations about you to employers by classifying you in certain categories. Michal Kosinski and colleagues have shown machine learning algorithms can predict scores on well-established psychometric tests using Facebook "likes" as data input which are the digital equivalent of identity claims: "Likes" tell others about our values, attitudes, interests, and preferences (Kosinski, Stillwell & Graepel,2013). On a separate note, as Duarte et al suggest these tools using natural language processing technology "have limited ability to parse the nuanced meaning of human communication, or to detect the intent or motivation of the speaker." Definitions of what constitutes toxic or concerning content are often vague and highly subjective. (Duarte, Llanso, and Loup. 2017)

In a world where our digital footprint becomes our twin persona and where almost everyone can get their hands on our information, the democratic process and our ability to openly share your views on different issues also comes under pressure. You might not want to take a stand on important societal issues if you know a future employer may make an adverse decision on your employment because of what they saw. Background checks can also surface details about an applicant's race, sexual identity, disability, pregnancy, or health status, which employers should not consider during the hiring process. Employers should not sacrifice the integrity of the recruitment process in an effort to catch a handful extreme cases of unacceptable behavior. The benefit does not justify the impact on free speech.

CONCLUSION:

There are certainly great opportunities to use AI to analyze a company's structure and see potential issues with imbalances across employee population, underrepresentation of different groups across various processes, etc; or use AI in a responsible manner to improve your processes. Algorithmic bias may exist even when there is no discriminatory intent on part of the vendor if there if the data was not good, and no employer invests in a product solely to cut costs if they know there might be certain bias and even discrimination issues. However, blindly onboarding with a software without doing a deep dive due diligence is also not a responsible way of conducting business either.

Algorithms are not independent of their developers, nor is the data of the populations upon which they are built without the potential of embedded bias. It is not enough for companies to self-govern their products when the stakes are high. We need better governance mechanisms to be able to hold vendors accountable in more effective ways. We need policies and regulations in place to fight structural injustices and transform societies through fair access to opportunities.

REFERENCES:

Barocas, Solon and Selbst, Andrew D., *Big Data's Disparate Impact* (2016). 104 California Law Review 671 (2016). https://ssrn.com/abstract=2477899 or http://dx.doi.org/10.2139/ssrn.2477899

Barrett, Lisa Feldman, et al. *"Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements." Psychological Science in the Public Interest*, vol. 20, no. 1, July 2019, pp. 1–68, https://doi.org/10.1177/1529100619832930

Bendick, Marc & Nunes, Ana. (2011). *Developing the Research Basis for Controlling Bias in Hiring.* Journal of Social Issues. 68. 238-262. 10.1111/j.1540-4560.2012.01747.x. https://www.researchgate.net/publication/235556983_Developing_the_Research_Basis_for_Controlling_Bias_in_Hiring

Bogen, Miranda and Rieke, Aaron. *Help wanted: An exploration of hiring algorithms, equity, and bias*. Technical report, Upturn, 2018. https://www.upturn.org/reports/2018/hiring-algorithms/

Bolukbasi, Tolga et al. *"Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings."* https://arxiv.org/pdf/1607.06520.pdf

Buolamwini, Joy and Timnit Gebru. *"Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."* FAT (2018). http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Carpenter, Julia, *Google's algorithm shows prestigious job ads to men, but not to women*. Independent. 2015 https://www.independent.co.uk/life-style/gadgets-and-tech/news/googles-algorithm-shows-prestigious-job-ads-to-men-but-not-to-women-10372166.html

Chamorro-Premuzic, T., Winsborough, D., Sherman, R., & Hogan, R. (2016). *New Talent Signals: Shiny New Objects or a Brave New World*? Industrial and Organizational Psychology, 9(3), 621-640 https://doi.org/10.1017/iop.2016.6

Dastin, Jeffrey, *Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. 2018 https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Duarte, Natasha, Llanso, Emma and Loup, Anna, *Mixed Messages? The Limits of Automated Social Media Content Analysis,* Center for Democracy & Technology, November 2017, https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf

Electronic Privacy Information Center (EPIC). *EPIC Files Complaint with FTC about Employment Screening Firm HireVue*. 2019. https://epic.org/2019/11/epic-files-complaint-with-ftc.html

Geyik, Sahin Cem, Stuart Ambler, and Krishnaram Kenthapadi. *"Fairness-Aware Ranking in Search & Recommendation Systems with Application to LinkedIn Talent Search."* Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (2019): https://arxiv.org/abs/1905.01989

Guo, Anhong & Kamar, Ece & Vaughan, Jennifer & Wallach, Hanna & Morris, Meredith. (2019). *Toward Fairness in AI for People with Disabilities: A Research Roadmap*. https://arxiv.org/abs/1907.02227

Heater, Brian, *Facebook settles ACLU job advertisement discrimination suit*. TechCrunch. https://techcrunch.com/2019/03/19/facebook-settles-aclu-job-advertisement-discrimination-suit/

Kim, Pauline, *Big Data and Artificial Intelligence: New Challenges for Workplace Equality* (December 5, 2018). University of Louisville Law Review, Forthcoming. https://ssrn.com/abstract=3296521

Kim, Pauline, *Manipulating Opportunity* (October 9, 2019). Virginia Law Review, Vol. 106, 2020, Forthcoming.https://ssrn.com/abstract=3466933

Kleinberg & Jens Ludwig & Sendhil Mullainathan & Cass R. Sunstein, 2019. "*Discrimination In The Age Of Algorithms,"* NBER Working Papers 25548, National Bureau of Economic Research, Inc. https://ideas.repec.org/s/nbr/nberwo.html

Kosinski, M., Stillwell, D., & Graepel, T. (2013). *Private traits and attributes are predictable from digital records of human behavior*. Proceedings of the National Academy of Sciences of the United States of America, 110(15), 5802–5805. https://www.pnas.org/content/110/15/5802

Lee, Alex. *An AI to stop hiring bias could be bad news for disabled people.* Wired. 2019. https://www.wired.co.uk/article/ai-hiring-bias-disabled-people

O'Neill, Cathy, *The Era of Blind Faith in Bid Data Must End*, TedTalk, 2017) https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end?language=en

Raghavan, Manish et al. "*Mitigating bias in algorithmic hiring: evaluating claims and practices."* Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (2020): https://arxiv.org/pdf/1906.09208.pdf

Rosenbaum, Eric, *Silicon Valley is stumped: A.I. cannot always remove bias from hiring*, CNBC. https://www.cnbc.com/2018/05/30/silicon-valley-is-stumped-even-a-i-cannot-remove-bias-from-hiring.html

Schulte, Julius. *AI-assisted recruitment is biased. Here's how to make it more fair*. World Economic Forum. 2019 https://www.weforum.org/agenda/2019/05/ai-assisted-recruitment-is-biased-heres-how-to-beat-it/

Quillian, Lincoln, Pager, Devah, Hexel, Ole, Midtbøen, Arnfinn H.. *The persistence of racial discrimination in hiring*. Proceedings of the National Academy of Sciences Oct 2017, 114 (41) 10870-10875; https://www.pnas.org/content/pnas/114/41/10870.full.pdf)

Thorsten Joachims, Laura Granka, Bing Pan, Helene Hembrooke, and Geri Gay. 2005. *Accurately interpreting clickthrough data as implicit feedback*. In *Proceedings of the 28th annual international ACM SIGIR conference on Research and development in information retrieval* (*SIGIR '05*). Association for Computing Machinery, New York, NY, USA, 154–161. https://dl.acm.org/doi/10.1145/1076034.1076063

Title VII of the Civil Rights Act of 1964: https://www.eeoc.gov/statutes/title-vii-civil-rights-act-1964

Venkatraman, Sankar. *This Chart Reveals Where AI Will Impact Recruiting (and What Skills Make Recruiters Irreplaceable)*, LinkedIn Blog, 2017. https://business.linkedin.com/talent-solutions/blog/future-of-recruiting/2017/this-chart-reveals-where-AI-will-impact-recruiting-and-what-skills-make-recruiters-irreplaceable

Vincent, James, *Google's algorithms advertise higher paying jobs to more men than women*. The Verge. 2015 https://www.theverge.com/2015/7/7/8905037/google-ad-discrimination-adfisher

World Bank, *Disability Inclusion*. 2020. https://www.worldbank.org/en/topic/disability

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Airlines for America

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Sent via email: BiometricRFI@ostp.eop.gov

RE: RFI Response: Biometric Technologies

Airlines for America (A4A), on behalf of its members,[1] offers the following response to the Office of Science and Technology Policy's (OSTP) request for information, "Public and Private Sector Uses of Biometric Technologies" (Biometrics RFI).[2] Identity verification is a cornerstone of security and facilitation in aviation. Our members have invested in their own initiatives and worked closely with our partners in the Department of Homeland Security (DHS) to leverage biometric technologies to this end. Our principal goals are enhancing security and improving the passenger experience through the use of biometric identify verification. To accomplish these goals, aviation's use of biometrics must be fast, accurate and reliable.

Technological advances in recent years have significantly improved facial recognition matching rates across all demographics, and successfully adapted to new passenger environments and requirements, including the mask requirements for COVID-19. We strive for the highest standards in privacy, transparency, consent and security to encourage passenger acceptance and to achieve operational benefits of biometric technology. There are distinct yet complimentary roles that industry and DHS perform in this space, and continued collaboration is critical to meet our goals.

Biometric Verification in Aviation

The use of biometric technology in aviation helps automate identity and citizenship verification requirements with a higher degree of confidence. Airlines verify a passenger's identity at several points during the customer journey, including check-in, bag drop, lounge access and boarding. The Transportation Security Administration and U.S. Customs and Border Protection also verify a passenger's identity as part of their security and admissibility processes. In most

[1] A4A's members are: Alaska Air Group, Inc.; American Airlines Group, Inc.; Atlas Air Worldwide Holdings, Inc.; Delta Air Lines, Inc.; FedEx Corp.; Hawaiian Airlines; JetBlue Airways Corp.; Southwest Airlines Co.; United Airlines Holdings, Inc.; and United Parcel Service Co. Air Canada is an associate member.
[2] OSTP, Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 FR 56300 (Oct. 8, 2021) (hereinafter, "Biometrics RFI").

cases, these processes are conducted manually, requiring a passenger to present a physical document proving the passenger's identity, citizenship status and proper entry requirements (*e.g.*, passport, driver's license, and visa) which is then visually matched to the individual. The benefits of automation are still limited by a need for a traveler to present identity and travel documents and access to appropriate and sometimes multiple government databases. A biometrically enabled travel experience can provide the traveler the choice to opt-in or opt-out of certain facilitation benefits, and at the same time, provide fidelity on how, when, and for what purpose their data is being used.

In Partnership with DHS

In some cases, airlines may partner with DHS in identity verification (*e.g.*, Biometric Exit). An airline may own and/or operate the technology to capture a passenger's image, then transmits an encrypted image to government secure infrastructure and matching mechanisms to verify a passenger's identity.

Transforming the Passenger Experience

Some airlines are exploring options to conduct facial matching of the passenger physically present against the airline's own database of stored images to transform the passenger journey. Biometric verification of passengers creates a true seamless experience for the passenger. This transformation leverages biometric facial matching from check-in to bag drop to boarding, with explicit consent from the passenger. When facial matching is applied throughout the passenger journey, operational efficiencies and security benefits are realized in tandem.

Benefits of Biometric Verification

Biometric verification creates a safer, seamless, and contactless passenger experience, and its convenience and scalability will help airlines adapt to passenger volume growth and operate more efficiently. As the department responsible for the security of air travel, DHS equally benefits from biometric technologies.

Operational Efficiency and Adaptability

Over the past decade, advancements in biometric technologies have demonstrated both security and facilitation benefits. Further, technology has advanced to the point where security and facilitation can be mutually reinforcing. Prior to the COVID-19 pandemic, the growth in domestic and international travel demanded adoption of technology solutions that maximized existing personnel and resources. In the summer of 2018, the World Travel and Tourism Council noted that "the travel industry could create 100 million new jobs in the next 10 years if…supported by infrastructure investments and biometrics and other technologies are deployed to make travelling more efficient and safe."[3] As air travel recovery continues, the

[3] C. Burt, *Biometrics will help travel sector job creation: WTTC*, BIOMETRICUPDATE.COM (May 16, 2018) *available at* https://www.biometricupdate.com/201805/biometrics-will-help-travel-sector-job-creation-wttc.

airline industry will face the same dilemmas it faced in 2019—increasing levels of passenger traffic with limited infrastructure capabilities.

Automating facial matching facilitates the secure and seamless processing of a growing number of passengers within physically constrained airport environments and minimizes disruptions to operations and wait times for passengers. Data from several of our member's biometric pilots show that the time required for processes like bag drop and boarding is significantly reduced by using biometric technology. Faster passenger processing enables timely and efficient operations, for example, enabling more on-time departures and potentially reducing aircraft turn-around times.

Safe and Contactless

The COVID-19 pandemic has accelerated the consideration of biometrically enabled solutions that afford a contactless process that better promotes the health and safety of our employees and passengers. Continued improvements in technology and processes will help reduce verification times, remove repeated touch points and reduce passenger bottlenecks. Investments today in low-contact processes will make airlines and the traveling public more resilient to potential future health crises, reducing the health risk associated with close interactions between passengers and airline employees, and ease staffing concerns as travel resumes.

Responsible Use

As biometric technology continues to improve in speed, accuracy and reliability, our members are eager to adopt it in a responsible manner.

Accuracy and Bias

To realize our goals of improving security and the passenger experience, all technology and process variables in biometric verification must support accuracy and reliability. Disproportionate error rates across specific demographics – commonly referred to as "bias" – is counterproductive to our security goals and our commitment to passengers. The biometrics and computer vision industry in partnership with the Federal Government has made substantial gains in addressing bias and improving the accuracy of their algorithms. Airlines serve customers globally. We recognize the importance of and are committed to accuracy in algorithmic performance across all ethnicities and genders.

Inaccuracy rates, even at small percentages, have outsized impacts on populations as large and diverse as air travel passengers. False negatives and false positives in the air travel environment can severely undermine the government's ability to fulfill its security mission, undercut carriers' ability to confer benefits and facilitate the passenger experience, and tax operational resources for government and industry alike. High inaccuracy rates, therefore, do not scale for the security or airline business cases for biometrics.

With that in mind, we are encouraged by the tremendous technological strides in industry and commitment of our DHS partners to accuracy in facial matching. A 2019 National Institute of Standards and Technology (NIST) report on the performance of facial recognition algorithms across different demographic groups shows that the development of this technology is already highly accurate and improving.[4] In both one-to-many and one-to-one facial matching, the most accurate high-performing algorithms achieved greater accuracy than humans, with low false positives and negatives across most demographic groups. Further, the current reality of masked passengers during the COVID-19 pandemic has spurred continued development and refinement of matching algorithms. Algorithms refined during the pandemic showed increased matching rates of masked passengers to the pre-pandemic algorithms, according to NIST.[5] We applaud the industry's rapid adaptability and overall commitment to continuous improvement.

Beyond the matching algorithm, there are additional variables in biometric verification that can affect accuracy and reliability. For example, we can control the quality of the image used for comparison by ensuring ideal conditions in lighting and image resolution. It is important to recognize that such complex technological tools can and should be adapted to the situations to which they are applied. As best practices emerge, our members are committed to adopting the most appropriate approach for different use cases, to deliver the optimal experience and service to the flying public.

Privacy and Data Security

Privacy and security of our passengers' biometric data is of the utmost concern. Automated facial matching has privacy and data security protections built in to protect the biometric information in-transit and at-rest. As required by DHS when using DHS matching capability, photos taken for the purpose of automated facial matching are not retained and are purged by air carriers following their secure verification by DHS. Airline connections to secure, encrypted DHS systems for verification ensure passenger data is protected in-transit.

In addition, our members treat customers' biometric information with the same care and diligence as other customer data. The airline industry is already well-equipped to protect the privacy of passenger data given its experience complying with global data protection regimes, such as the EU General Data Protection Regulation. Our members' use cases are focused on the passenger travel journey.

Consent

Passengers must consent to leveraging their biometric information for automated facial matching. Although frequent fliers may be more familiar with biometric technology, non-frequent fliers often do not share the same awareness. The higher the passenger acceptance of automated facial matching, the stronger the realization of security, safety, and efficiency

[4] Grother, P., Ngan, M., and Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NIST.IR 8280. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[5] Ngan, M., Grother, P. and Hanaoka, K. (2020), Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. NIST.IR.8331. Available at: https://doi.org/10.6028/NIST.IR.8331.

benefits. Therefore, we work with DHS to educate passengers on how the technology is being used and which personal data elements are being shared or stored.

On behalf of our members, we thank OSTP for providing the opportunity to submit information on the aviation use-case for biometrics. As explained in this response, security and facilitation is at the core of biometric use in the air travel environment. Biometric technology provides increased security for passengers while creating second-order effects of reducing health risk in travel and providing growth opportunities for operators. Our members work closely with DHS on improving the experience and protections for passengers. If you have any questions on this Biometrics RFI response, you can contact Lauren Beyer at [redacted].

Respectfully submitted,

[redacted]

Lauren Beyer
VP, Security and Facilitation

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Alliance for Automotive Innovation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

SUBMITTED ELECTRONICALLY VIA EMAIL

Suresh Venkatasubramanian
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW
Washington, DC 20504

RE: Request for Information on Public and Private Sector Uses of Biometric Technologies

Dear Dr. Venkatasubramanian:

The Alliance for Automotive Innovation ("Auto Innovators") is pleased to submit comments to the Office of Science and Technology Policy ("OSTP") in response to its Request for Information ("RFI") on public and private sector uses of biometric technologies. Auto Innovators appreciates the opportunity to provide input and feedback on this important issue.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents the manufacturers that produce nearly 99 percent of cars and light trucks sold in the United States. Members of Auto Innovators include motor vehicle manufacturers, original equipment suppliers, technology companies, and others within the automotive ecosystem. The auto industry is the nation's largest manufacturing sector and contributes $1.1 trillion to the United States economy and represents 5.5 percent of the country's GDP. As a significant engine for our nation's economy, the auto sector is responsible for 10.3 million jobs and $650 billion in paychecks.

Automotive Use Cases

Our member companies are leaders in innovation and are integrating cutting-edge technologies into consumer vehicles that are transforming mobility and steering us towards a cleaner, safer, and smarter transportation future. A number of these innovations – including automated driving and other advanced safety technologies, as well as other features that support drivers and passengers – may rely on or otherwise incorporate biometrics-related capabilities.

For example, facial detection technology is increasingly being used in vehicles with advanced driver assistance features, particularly vehicles with partial automation features, in driver engagement monitoring systems. In these driver engagement monitoring systems, cameras in the passenger cabin may be used to track eye movement, monitor head position, and perhaps even measure eyelid activity to warn drivers who become inattentive to the driving task or over-reliant on the automated features.

Similar facial detection capabilities or heartbeat sensors may also be used to detect if a driver is having a medical emergency that may impede their ability to safely operate a vehicle. Breath sensors, fingertip sensors, or facial detection sensors may eventually help detect if a driver is alcohol- or drug-impaired. Facial detection may also support features that darken portions of the sun visor to prevent sun glare for drivers and passengers. In these cases, the technology is not used for identification or verification. It is used to infer driver or occupant state.

Auto companies are also developing technologies that rely on facial detection or heartbeat sensors to help detect whether a child has been inadvertently left unattended in the backseat of a vehicle and to support more accurate seat belt reminders or airbag deployment controls. Facial detection technologies may also be used as part of advanced driver assistance systems or automated driving systems to detect pedestrians or other vulnerable road users for collision avoidance purposes. For these use cases, the technology is not used for identification, verification, or inference of driver or occupant state. Instead, it is used to help ascertain whether an object may be a person.

Finally, face scans or fingerprints may be used for verification of authorized vehicle users. These capabilities can help prevent vehicle theft by denying access to unauthorized users or increase convenience by allowing users to unlock doors and start the vehicle without the need for a key. Similarly, face scans or fingerprints may facilitate personalization of in-cabin systems and settings, assisting drivers and helping to reduce driver distraction. As a verified driver enters the vehicle, the seats, mirrors, climate controls, and radio stations may be changed to the driver's preference and the driver's phone may automatically sync with the vehicle. These biometrics-related capabilities may also facilitate parental controls, such as limits on vehicle speed and audio volume, while a vehicle is driven by a new driver. In these cases, the biometric information is not being used for the identification purposes and is instead being used for verification purposes.

Specific Recommendations

As OSTP continues its important work in this area, Auto Innovators respectfully offers the following recommendations.

Leverage Existing Industry Efforts

There are existing industry efforts related to biometric technology that OSTP may be able to leverage or amplify as best practices. For example, in 2014, automotive manufacturers released Privacy Principles for Vehicle Technologies and Services ("Privacy Principles") to protect information collected through in-vehicle services. These comprehensive Privacy Principles, which are enforceable by the Federal Trade Commission, establish a set of baseline privacy protections related to the collection and use of such information. They also establish heightened protections for certain categories of information, including biometric information.

Under the Privacy Principles, companies must provide clear, meaningful, and prominent notices about the collection of biometric information, the purposes for which such information is collected, and the types of entities with which such information may be shared. In addition, the Privacy Principles specifically require affirmative consent for the use of biometric information for marketing purposes or for sharing biometric information with unaffiliated third parties for their own use. The Privacy

Principles also include commitments related to – among others – data minimization, data security, and respect for context.

OSTP should build upon these sorts of industry efforts where they exist. Should OSTP identify areas where technical standards or best practices would be particularly useful but do not currently exist, it should encourage industry to develop such standards or best practices.

Balance Benefits and Risks

Auto Innovators appreciates that the RFI seeks information on both the benefits and risks of biometric technologies. By fully understanding and – where possible - quantifying the benefits and risks posed by the technology, government and industry can focus on fostering the appropriate balance that enables these technologies for promising use cases, including those automotive use cases identified above, and appropriately manages or reduces the risks posed by them. Seeking this balance, rather than requiring zero risk, is essential. If policymakers hold biometric technology to an unattainable zero risk standard, important and – in some cases – lifesaving use cases may be lost.

For example, we certainly share OSTP's concerns with the potential for differential effectiveness, outcomes, and harms for different demographic groups with biometric technology. However, we also recognize that human decision-making may reflect inherent or implicit biases. Biometric technology has the potential to reduce, minimize, or even eliminate such human biases. This potential should be considered in and factored into any assessment or analysis of biometric technologies and bias.

Narrow the Initial Scope

By including inference of cognitive/emotional state in the RFI, OSTP has put forward a significantly expansive definition of "biometric technology" with far-reaching implications. As this is undoubtedly a complex issue that requires a thoughtful and deliberate approach, Auto Innovators recommends that OSTP focus its initial efforts through a targeted and focused definition that is aligned with a more traditional understanding of biometric technology.

For example, we recommend that OSTP limit its initial efforts to the use of biometric information for recognition purposes only. We further recommend that OSTP consider limiting this initial effort to the use of biometric information for identification and exclude the use of such information for verification. With a targeted initial focus, OSTP may be better positioned to make meaningful progress that may be leveraged or adapted more broadly going forward.

Prioritize High-Risk Use Cases

Biometric technologies are currently being used or will be used in a variety of contexts and a diversity of applications. Undoubtedly, some of these use cases pose more significant risks for harmful societal outcomes than others. In this work, OSTP should prioritize the high-risk uses of biometric technologies that are likely to lead to harmful societal outcomes over those that are unlikely to lead to such outcomes. For example, OSTP should consider initially focusing on biometric technologies that are used for surveillance or for law enforcement purposes. Alternatively, OSTP may consider focusing

initially on uses that have significant legal impact or implication, such as those related to employment, education, housing, or health care.

Ensure Broad Stakeholder Engagement

Auto Innovators appreciates that the RFI and the related public listening sessions indicate an intent by OSTP to obtain feedback from the broader communities of interest and to hear the perspectives of a wide range of stakeholders. We urge OSTP to maintain an approach that is actively representative and includes a broad set of disciplines and stakeholders and that provides ample opportunity for public input.

We sincerely appreciate the opportunity to provide this feedback to OSTP as it embarks on this important work. We look forward to continuing to work with you on this and other matters.

Sincerely,

Tara Hairston
Senior Director, Technology, Innovation, & Mobility Policy

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Amelia Winger-Bearskin

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Tuesday, October 19, 2021 1:48:49 PM

Decentralization was (and still is) the hope of many of us early builders of the first generation of online weirdos, the first children to grow up with the internet, and the last generation to remember life before it existed. In those early days, we saw the internet as a real promise, that it would make information free, democratize media, and grant new forms of economic self-sufficiency. Many of us believed we could change the way the world works from behind our glowing screens.

Some of us actually did that, and many things have changed,

But not exactly in the ways we imagined.

The promise was information would be free - what we got was, we got to be the free information as third parties harvested our data.

The promise was democratized media - what we got was media that threatens democracy.

The promise was a new economy - what we got was the gig economy, with more precarity and higher inequality.

The promise of the early internet lost nearly all its idealistic moral gravitas. Now when we talk about promises and the internet we're just talking about a Javascript concept, another best practice in a software engineer's development stack.

In any other field whose name has the word engineering in it, outcomes like this wouldn't fly.

imagine a civil engineer or a structural engineer who is tasked with building the Brooklyn Bridge. A trucking company asked the engineers, "Ok we need to plan our routes across this new bridge, how many trucks with how many loads can safely go across and maintain the safety of the bridge." The structural engineer says "Hey look, technology is neutral, I build the bridge but I don't tell people how to use it. If someone wants to break the bridge and it all falls down, it is what it is, I mean that is not my fault."

But with software, especially social networks and the digital media ecosystem,

we are perfectly ok with tech companies telling us that the systems they have designed are neutral even as they break safety, democracy, privacy, fraud, make our children unsafe or are abusive or cause deep harm to our country.

There is not a responsibility to know its limits, its load, or what could happen to the lives involved should it break.

If we start to believe that it's not our responsibility as the builders of these systems, then we are really building systems of harm. We are building bridges and not caring for those who trusted us to drive across them.

I created Wampum.codes to address exactly this issue.
Wampum.codes is an ethical framework for software development based on the principles of co-creation as understood by my people (Seneca-Cayuga Nation of Oklahoma.)

Like all members of the Iroquois Confederacy, we made wampum. A lot of people have a misconception about what wampum is - they think it was a form of currency. It was not currency - we used it as a tool for recording and regulating the different political and economic agreements that governed daily life. It was a decentralized means of recording contracts, something like a pre-Colombian blockchain, that encoded not just financial transactions, but also ethical values.

The project of Wampum.codes is to try and imagine how we can weave ethics back into 21st-century technologies.

The core concepts are to put an extra step in every step of the software development pipeline (for the development of all work on computers, yes including AI), take a few hours a quarter to align your goals, and look at risk mitigation. Often times you will find your developers, UX designers, leadership all believe they all have the same values and just need to articulate them, build some rules and logic into their systems, imagine a better future and really listen to one another around fears, joy and possibilities for the things they want to see in the world.

We can embed these values as dependencies in code the same way we do in the rest of our package.json

CEOs, Founders and employees who work in tech are eager for change, they WANT new systems to encode values and ethics into the source code for new decentralized projects and systems.

While waiting for experts and policymakers to make these decisions- we, makers and builders need to be developing systems of harm mitigation and threat modeling so that our products designed to help the world do not harm it. We need robust regulation, testing methods and guidelines and it is up to us to start developing protocols side by side with every line of code we write. This is our field, we know how to do it, and we are the ones who need to step up. By implementing a decentralized protocol around ethics in software, we can step in the right direction.

We live our lives according to a moral code. The time has come to code our morals.

Best,

Amelia Winger-Bearskin, [redacted]
Banks Preeminence Chair and Associate Professor of Artificial Intelligence and the Arts, University of Florida, Digital Worlds Institute

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

American Civil Liberties Union

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

Via Email

Office of Science and Technology Policy
[redacted]

RE: Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (FR Doc. 2021-21975)

The American Civil Liberties Union writes in response to the Office of Science and Technology Policy's October 2021 Request for Information on Public and Private Sector Uses of Biometric Technologies. This submission surveys a number of concerns with use of biometric technologies by government and private actors, and presents policy recommendations. Due to space constraints, this submission can only touch on some of the ACLU's concerns with the adoption and use of biometric technologies.

I. General Concerns About Biometric Technologies

A. Biometric identification and tracking technologies

Because biometric identifiers are personally identifying and generally immutable, biometric technologies pose severe threats to civil rights and civil liberties by enabling privacy violations—including loss of anonymity in contexts where people have traditionally expected it, persistent tracking of movement and activity, and identity theft. Additionally, flaws in the use or operation of biometric technologies can lead to significant civil rights violations, including false arrests and denial of access to benefits, goods, and services. These problems disproportionately affect people of color and members of other marginalized communities.

1. Biometric technologies enable mass tracking and identification

Although the limited collection and use of certain biometrics, such as fingerprints, dates back many decades, the development of machine-learning-based biometric technologies, paired with the proliferation of digital-age network technologies, has resulted in categorically new powers in the hands of government and corporate actors to quickly identify, track, and surveil people. Prior to the digital age, collection and use of biometrics was slow and laborious, and thus not possible at scale. Today, however, machine-learning algorithms allow near-instantaneous collection and/or exploitation of an array of biometrics, including those drawn from physical or biological attributes (e.g., face recognition, voice recognition, iris or retina scans, fingerprints, and DNA) and activity (e.g., gait recognition and keystroke recognition). These capabilities can be used both to identify people in an instant, and to pervasively track their movements in the physical world and online, such as by using face recognition to track a person across a network of video surveillance cameras. The ability of these technologies to capture biometrics at a distance or from video footage can evade detection and can easily be carried out without

knowledge or consent of affected individuals. Even biometric identifiers that traditionally had to be collected from individuals in-person, such as fingerprints, iris scans, and DNA, can now sometimes be captured remotely, raising newly pressing concerns.

2. Failures of biometric technologies can result in civil rights violations and denials of access to benefits and services

Because of design flaws, hardware limitations, and other problems, biometric technologies can fail to function as advertised, leading to failed identifications. When flawed technologies fail to accurately identify unknown individuals or verify the identities of people seeking access to benefits or services, these failures can result in civil rights violations. The harms of failed identifications disproportionately affect people of color, lower-income people, people with disabilities, and members of other marginalized groups.

While all biometric technologies are error-prone, problems with face recognition technology raise particular concerns in light of its rapid proliferation. Multiple studies show that face recognition algorithms have markedly higher misidentification rates for Black people, people of color, women, and children.[1] This bias is partly attributable to the fact that datasets used to train face recognition algorithms have been "overwhelmingly composed of lighter-skinned subjects." Additional sources of bias are introduced when face recognition systems rely on digital camera images because, when taking photos of darker-skinned faces, the cameras often fail to provide the degree of color contrast that the algorithms need to produce and match faceprints.

Even when face recognition technology functions well in controlled test conditions, it is prone to fail in real-world applications. The accuracy of face recognition is directly affected by the quality of the images being searched—error rates will be greater when two photographs contain different lighting, shadows, backgrounds, poses, or expressions. Face recognition can be extremely poor at identifying a person in a low-resolution image or a video, or at accurately finding matches when searching against a large database of images, in part because so many people within a given population look similar to one another.

Finally, even when biometric technologies work at a technical level, their adoption can create barriers to access to essential services for people living on low

[1] *See* NIST, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; John J. Howard, Yevgeniy B. Sirotin & Jerry L. Tipton, *Quantifying the Extent to which Race and Gender Features Determine Identity in Commercial Face Recognition Algorithms*, Dep't Homeland Sec. Sci. & Tech. (May 2021), https://www.dhs.gov/sites/default/files/publications/quantifying-commercial-face-recognition-gender-and-race_updated.pdf; K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race* (2019), https://arxiv.org/abs/1904.07325; Joy Buolamwini et al., *Gender Shades*, MIT Media Lab, https://www.media.mit.edu/projects/gender-shades/overview; Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 6, 1789–1801 (Dec. 2012), https://ieeexplore.ieee.org/document/6327355; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU Free Future (July 26, 2018), https://bit.ly/2OkETHe.

incomes, people with disabilities, older people, and members of other marginalized communities. Biometric identity verification requirements that rely on access to, familiarity with, or ability to operate technology (such as smartphones, web cameras, or high-speed internet connections) can disproportionately harm individuals who lack access to or the ability to use those systems. And due to disparate rates of technology access by race, income, age, and disability status, these burdens will fall disproportionately on members of already marginalized communities.

B. Biometric technologies for inference of emotion, cognitive state, or intent

Biometric technologies also purport to be able to infer information beyond identity, but biometric inference technologies suffer from grave flaws—to the point of being, in many cases, nothing more than snake oil. These technologies are typically built on naive assumptions about the scientific objectivity and discoverability of internal mental states that simply do not hold up. For example, companies are increasingly promoting products that purport to detect emotion or affect, such as "aggression detectors." But psychologists who study emotion agree that this project is built on a bed of intellectual quicksand because there is no reliable or universal relationship between emotional states and observable biological activity.

The same faulty premise underlies other biometric technologies, such as products that purport to detect "suspicious activity" through video analytics and those that claim to detect lies or deception through eye movements. Lie detection is a notorious sinkhole of pseudoscience—despite a century of efforts, scientists have firmly refuted the scientific reliability of polygraphs. The link between high-level mental states such as "truthfulness" and low-level, involuntary external behavior is just too ambiguous and unreliable to be of use.

II. Use of Biometric Technologies by Law Enforcement and Immigration Authorities

A. Face recognition technology

Law enforcement use of face recognition technology poses a number of serious threats, making it dangerous both when it fails and when it functions.

Misidentifications resulting from law enforcement reliance on face recognition technology have resulted in multiple false arrests. Unsurprisingly, given the racially biased failure rates of the technology, documented cases of false arrests resulting from incorrect face recognition "matches" have disproportionately involved Black men. For example, three Black men in Michigan and New Jersey—Robert Williams, Michael Oliver, and Nijeer Parks—spent time in jail for crimes they did not commit after police relied on faulty face recognition 'matches' to arrest them. They are each now suing police.

Compounding the problem of false identifications by police-operated face recognition technology is the lack of transparency by police and prosecutors when face recognition has contributed to an individual's arrest or prosecution. In order to adequately test the reliability of identifications, defense attorneys are entitled to receive not only notice that face recognition technology was used, but also information about the error rates of the particular algorithm used (including any disparate error rates by race or other demographic categories) and the complete list of possible matches from which a human examiner selected the defendant as a match. Prosecutors rarely provide such information to defense teams, however.

The most common current use of face recognition technology by police involves trying to identify suspects from photographs or video. However, the threat of face recognition *surveillance* looms. Several U.S. cities have purchased software that purports to be able to run face recognition searches on live or stored video, and several law enforcement agencies have piloted such technology. Deployment of face recognition or similar remote biometric tracking and surveillance capabilities would pose a catastrophic threat to privacy, by putting in the hands of government the ability to identify and track anyone or everyone as they go about their daily lives. Face recognition technology has been used to identify people attending Black Lives Matter and other protests, and the chilling effect of police deployments of biometric identification technologies that allow fast and pervasive monitoring of people cannot be overstated.

In recognition of these dangers, at least 23 jurisdictions—from Boston, to Minneapolis, to Jackson, Mississippi, to San Francisco, to the State of Vermont—have enacted legislation halting law enforcement or government use of face recognition technology. Others, such as the State of Maine, have enacted strict restrictions on law enforcement access to the technology.

Meanwhile, at the federal level, the FBI has gained access to hundreds of millions of Americans' driver's license photos to use in face recognition searches, and DHS has begun pursuing a sweeping vision of expanded use of face recognition in the air travel context. Indeed, DHS has already laid out—and begun following—a very specific, clear, and well-defined pathway for how its current programs (CBP use at airline departure gates and arrival checkpoints, and growing TSA use) will lead to a much broader implementations of face surveillance at the airport. And from there, this technology will be poised to expand far beyond the airport, following in the footsteps of other aviation security measures (such as bag searches, magnetometers, PreCheck, and CLEAR) that have spread beyond aviation contexts and into American life, threatening to create a checkpoint society the likes of which the U.S. has never known.

B. DNA

Use of DNA for biometric technologies is particularly concerning because of its immutability and the depth of personal information it can reveal—including not only identity, but also family relationships, ancestry, and propensity for health conditions. Moreover, because many law enforcement databases are made up of samples collected through the criminal system—for example, at arrest or conviction—these databases are racially biased in that they

have a higher proportion of samples from Black people than the proportion of Black people in the U.S. population. Further compounding the problem are situations in which people are compelled to give their DNA to these databases in exchange for a plea deal, asylum seekers not charged with a crime are compelled to give DNA samples, or even children are tricked into discarding DNA which is then added to databases. Thus, because of the realities of over-policing among Black and brown people, these law enforcement databases may create a feedback loop.

Moreover, the ability to acquire an individual's DNA without their knowledge or consent from an item they have touched—as law enforcement agents frequently do today—and use it to identify that person's past and future relatives, or to impute their facial geometry, calls for tight protections against abuse. Another area of concern is the ease with which law enforcement can access certain privately maintained genetic genealogy databases, which allow millions to be identified through their DNA because a distant relative used a direct-to-consumer genetic test.

Another area of concern in DNA biometric technology is error-prone or blackbox technologies that claim to analyze DNA rapidly, or to identify contributors in complex DNA samples that would be uninterpretable using traditional methods. Probabilistic genotyping algorithms claim to identify genotypes in mixed DNA samples, but because the software employing these algorithms is maintained by private companies, audits of this technology are infrequent or impossible—and when they do happen, can reveal errors affecting large numbers of criminal investigations. These examples represent clear failures of regulators to insist on rigorous scientific validation and accuracy standards for tools used in the criminal legal system.

III. Employment and Public Benefits

A. Identity verification for unemployment insurance and other public benefits

Identity verification using biometrics to access unemployment and other public benefits gained popularity during the pandemic and has since infiltrated essential government services. Specifically, ID.me, a private company, has contracts with at least twenty-seven states' unemployment agencies as well as numerous federal agencies to provide remote identity verification, with many agencies providing no in-person alternative. ID.me uses face recognition technology to compare uploaded images of a government identification with a mobile phone or webcam selfie. While touted as a means to prevent fraudulent claims and identity theft, there are many potential harms associated with using remote identity verification and face recognition in essential government services. ID.me keeps all biometric data, even after a person closes their account, and thus individuals are forced to choose between accessing the benefits they need and protecting their biometric data and privacy. Moreover, the ongoing concerns about the accuracy of face recognition technology when identifying people of color and inequities in technology access for low-income people and people of color mean that the individuals who most critically need unemployment support and public benefits may face the greatest barriers to accessing them.

B. Face and voice analytics during interviews

Face and voice recognition technology is being used to collect and analyze biometric data during employment interviews. Vendors of predictive interview hiring tools dubiously claim to

measure an applicant's skills and personality traits through automated analysis of verbal tone, word choice, and facial expressions. This technology raises an enormous risk of amplifying employment discrimination and violating civil rights laws. Predictive hiring tools often rely on training data regarding who would be a successful employee that reflects existing institutional and systemic biases in employment. Predictive tools that rely on facial and audio analysis raise even more risk that individuals will be automatically rejected or scored lower because of accents, disabilities, skin color, or because they are transgender, nonbinary, or gender nonconforming. Indeed, the very traits that these tools purport to measure are often themselves proxies for disabilities, gender, race, or other protected characteristics, as opposed to traits that are causally linked to job success. The lack of transparency in the use of these tools only adds to the harm—applicants know that they are being subjected to an online recorded interview, but often do not know that the interview will be analyzed through automated means or the standards that will be used to assess the interview. As a result, applicants often do not have enough information about the process to know whether to seek a disability accommodation.

C. Monitoring employees for productivity/attention

Workplace surveillance systems collect data about employee activities using smart phones and other systems that collect biometric data. The data used in these systems power algorithmic management systems that have expanded as a standard in most sectors of the U.S. economy. This technology has created new challenges for workers regarding basic workplace conditions and employment insecurity. Constant workplace surveillance is highly psychologically stressful. It can also lead to an employer's demand for accelerated output without increased pay (worker speedups) and increased racial profiling and bias from algorithms used in the management system. Worker organizing may be restricted and the most vulnerable workers are subjected to constant stress of losing their jobs, exacerbating already existing economic inequalities. Further, there are few restraints on an employer's ability to surveil workers, who have limited privacy rights while on the job. Workers also do not always have the ability to challenge algorithmically derived employment decisions, including discipline or firing, because monitoring practices are often difficult to detect.

D. Employee timecard systems and access to secure areas

Time and attendance systems may use fingerprint, face, and retina scans to record work time and give employees access to secure areas. Employers using this technology assert that this technology prevents time fraud and improves security. Although biometric time systems have become more widespread in recent years, very few states have laws governing how companies collect, store, and disclose employees' data or whether employees need to give informed consent when their data is collected. An employee who refuses to provide their biometric data may be terminated since employers are not obligated to provide an alternative method for workplace time and access systems.

IV. Housing

Face recognition is being used in both public and private housing to control who has entry access to buildings and communities. The use of face recognition raises serious concerns

about privacy harms and racial discrimination. Use of face recognition technology in housing communities without the consent or knowledge of residents can result in residents' unwitting inclusion in a biometric database, and in the automated monitoring of the comings and goings of residents and their guests. Privacy harms may also arise when housing authorities make the system's data available to law enforcement or other third parties. This practice particularly subjects individuals who cannot afford alternative housing options to surveillance. Discriminatory inaccuracies in face recognition technology may create harm to residents of color and undermine safety and security. Additionally, many systems that offer the technology for entry access also double as general surveillance systems, which raise the same privacy and discrimination harms. Tenants have voiced concerns when housing authorities attempted to install security surveillance that uses face recognition technology in both public and private housing.

V. Education

Students are increasingly required to use devices and applications, or be in spaces, that subject them to collection of their biometric data.

Remote exam proctoring and monitoring, which has seen explosive growth during the Covid-19 pandemic, has been plagued by face recognition technology that fails to recognize students of color, monitoring software that tracks students' eye movements, head movements, and keystroke patterns to flag "suspicious behavior" in a manner biased against disabled students, and opaque retention practices surrounding these data. Software that does not recognize students of color can lock them out of crucial exams or incorrectly flag them as "cheating."

Biometric technologies also raise concerns in physical schools. Companies are marketing voice-analysis aggression detectors, which involve the installation of special microphones in school hallways and other spaces that constantly monitor the voices of students to "assess threats." This technology has not proven to be accurate, and has been triggered by coughing and other innocuous sounds. Additionally, Black students and special education students are disproportionately flagged as "threats."

Similar concerns arise from the use of face recognition in schools to monitor video feeds for individuals placed on a school or district watchlist. In addition to the risk of false alerts—which will disproportionately harm students of color—the accumulation of faceprint data and constant surveillance over time presents serious privacy concerns for students.

VI. Commerce, Credit, and Banking

Biometrics are also finding uses in commerce, credit, and banking. Some retail stores, as well as venues such as concerts and stadiums, are using face recognition to scan their customers. Though few stores will disclose what they're doing, and marketing could be a motivation, the main purpose seems to be security—specifically, looking for people who have been blacklisted from a company's property to ensure they don't return. This kind of secretive, unregulated watchlisting is an ominous descendant of a long history of private and quasi-private watchlists, going back to the labor battles of the early 20th century, when workers and organizers were blacklisted as "troublemakers" and could have trouble getting a job. Even more than the

government's nightmarish system of watchlists, private-sector face recognition watchlists lack due process or other safeguards against abuse.

The collection of data about people's visits, characteristics, and behavior for marketing purposes is also being pitched by companies as a reason for stores to secretly use face recognition on their shoppers. Again, it's hard to know how widespread such uses are given the secrecy involved.

Biometrics are also being used by businesses such as banks for identity verification. Banks have built giant voiceprint databases, for example, and are also turning to technologies like fingerprints and "behavioral biometrics" such as keystroke analysis.

VII. Policy Recommendations

A. Government use of biometric technologies

As the ACLU and dozens of other organizations have previously explained, the twin dangers of highly consequential misidentifications and pervasive surveillance mean that government agencies should not be deploying face recognition technology. At a minimum, the White House should:

- Place a moratorium on all federal government use of face recognition technology and other forms of biometric technology so long as bias pervades these systems and Congress has not acted to authorize the use of the technology in specific circumstances and with sufficient safeguards to protect our privacy interests and prevent harms caused by this dangerous, unregulated technology;

- Prevent state and local governments from using federal funds to purchase face recognition technology or access face recognition technology; and

- Support the Facial Recognition and Biometric Technology Moratorium Act, introduced by Senator Markey. This bill would make a federal moratorium law and would place additional limitations on federal funding of these technologies.

When other biometric technologies are used, they should only be used if they have a demonstrably negligible failure rate in real-world applications; a lack of differential accuracy rates for people of different races or ethnicities, gender, or any other protected characteristics considered individually and intersectionally; rely on training data that was collected in a manner that did not violate the privacy of the data sources; and include strict safeguards that protect the privacy of individuals subject to those technologies.

1. Law enforcement uses of biometric technologies

As explained above, law enforcement agencies should not be permitted to use face recognition technology. To the extent other biometric technologies threaten to permit pervasive mass tracking of people's movements and activities, law enforcement should likewise be barred from using them. Any biometric technology that law enforcement seeks to use to identify particular individuals should be subject to strict standards for accuracy and reliability and subject to rigorous accuracy testing. Tests of some biometric technologies currently run by the National Institute of Standards and Technology are a positive model for such testing. Additionally, police should not be permitted to collect known individuals' biometrics without a search warrant or, in some circumstances, following an arrest based on probable cause.

Law enforcement sequencing of DNA in investigations should not use SNP profiling or whole-genome sequencing, which reveals significantly more information about a person's ancestry, medical proclivities, and other private details than traditional methods. Local law enforcement agencies that receive federal funding should also be prohibited from maintaining their own DNA databases, which often lack the security protections and quality standards of the FBI's CODIS database.

2. Non-law enforcement government uses of biometric technologies

As explained above, the federal government should halt use of face recognition technology. If face recognition technology or other biometric technologies are ever to be properly used for identity verification in unemployment insurance or other benefits-eligibility determinations, they must be strictly regulated, including ensuring accuracy, reliability, and privacy as outlined above. Government agencies procuring such technologies from private vendors must conduct due diligence on these technologies, and require vendors to produce records disclosing their training data and detailing all studies that have been conducted on the technology's failure rates and differential accuracy rates. Once a biometric technology is deployed for identity verification, government agencies should gather anonymized, individual claimant-level data showing outcomes for attempts to verify identity, mode of verification, specific reason for identity verification failures, and claimant demographic information. The records collected as part of the agency's pre-procurement due diligence and the post-deployment anonymized claimant information should be published on the agency's website.

Agencies using biometric technologies for identity verification should ensure that they provide plain-language notice describing the identity verification process, available in as many languages as is feasible, as well as plain-language notice of the reasons for any denial and the corrective steps that can be taken. They should also provide an easy and obvious means of submitting alternative evidence of identity. Appeals processes for denials must be reliable and easily accessible. Agencies must also provide reliable and easily accessible in-person alternatives to biometric identity verification processes for people with limited technology access or who have privacy concerns.

B. Private uses of biometric technologies

Private entities should be barred from capturing or using biometric identifiers without first providing detailed, plain-language notice and obtaining express consent, and may not disparately treat people based on their withholding consent. The Illinois Biometric Information Privacy Act has successfully provided a base minimum of such protection for more than a dozen years, and the White House should support similar protections at the federal level.

The use of biometric information by private entities in the areas of employment, housing, credit, education, or any other areas protected by federal civil rights laws should be strictly regulated by agencies tasked with civil rights enforcement. Agencies should use the full scope of their authority to:

- Gather and publicize information on private uses of these technologies in the spheres under their purview;

- Issue regulations and guidance that set auditing requirements for processes using biometric information, including requiring regular auditing for discriminatory effects on protected classes as well as intersectional identities throughout a technology's conception, design, implementation, and use; proactively looking for and adopting less-discriminatory alternatives; assessing how training data was sourced and whether it is representative and accurate; ensuring that the technology is measuring lawful and meaningful attributes; ensuring clear and effective notice and recourse processes, and that people with disabilities are provided reasonable accommodations; and providing for public release of internal and external audit reports; and

- Aggressively engage in enforcement actions against private actors whose technologies violate federal civil rights protections.

* * * * *

Thank you for your consideration of these comments. The ACLU would welcome the opportunity to further discuss these critical issues. Please contact Nate Wessler [redacted] and Olga Akselrod [redacted] with any queries.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

American Civil Liberties
Union of Massachusetts

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

[redacted]

ACLU of Massachusetts RFI Response: Biometric Technologies

Police use of machine learning-enabled biometric technologies like facial recognition poses unprecedented threats to basic civil rights and civil liberties, impedes racial justice, and undermines open, free, democratic society. These technologies can be used to identify and track people and groups, using their facial, iris, voice, and other features, turning fast-growing surveillance camera networks into inescapable dragnets enabling the mass tracking of people's movements, habits, associations, and political and religious activities.

The regulatory landscape pertaining to biometrics has changed dramatically in the past few years. But despite significant progress in parts of the country, most states—and the federal government—have not imposed democratic guardrails on police use of facial recognition or other remote biometric surveillance technologies.

Importantly, facial recognition is not one thing. Police can use facial recognition technology in at least three distinct ways, each raising different problems for civil rights and civil liberties: (I) identification and image matching, (II) surveillance, and (III) affect recognition. Short of banning the technology entirely, some states—like Maine and Massachusetts—have opted to regulate police use of image matching in limited situations, subject to law requiring centralization, privacy protections, and democratic controls. But for reasons described below, it is not possible to meaningfully regulate the use of facial recognition technology for surveillance or affect recognition. Indeed, the grave threats to privacy, freedom of speech and association, and racial justice posed by police use of these technologies can only be averted by prohibiting their use entirely.[1]

I – Police use of facial recognition for identification and image matching

Law enforcement in the United States has used facial recognition for identification and image matching purposes for at least twenty years. Facial recognition for image matching and identification is the most common police use of the technology in the United States. Police use image matching to confirm the identity of a person in an image, or to put a name to a face. Typically, this is done by using a facial recognition algorithm to compare a still image (e.g. from human review of surveillance camera footage, a social media account, a police surveillance photograph, or other source) to a database of identified faceprints (e.g. a driver's license or state identification database).

The first decade of the 21st century saw a quiet but massive expansion of law enforcement use of the technology for this purpose, thanks to National Highway and Traffic Safety Administration grants to state motor vehicle and licensing agencies to acquire facial recognition systems. While these systems were purchased to help registries identify fraud in the licensing process, their use was subsequently expanded to include police investigations.

According to records obtained by the ACLU, for example, the Massachusetts Registry of Motor Vehicles obtained a facial recognition system in 2006 and only months later sent a memo to state and local police offering to perform facial recognition searches on their behalf. The registry went on

[1] Below we provide the ACLU of Massachusetts' ("ACLUM") views on police use of biometrics technology, focusing specifically on facial recognition. This submission reflects the views of the ACLUM, and not necessarily the National ACLU or other ACLU affiliates.

to perform hundreds of facial recognition searches for police and federal agencies per year, subject to no regulation or privacy protections.[2]

The FBI likewise maintains its own facial recognition program and database, containing at least 640 million images of American adults, taken from both criminal and civil government processes across the country.[3] The FBI ran 157,000 searches between fiscal year 2017 and April 2019.[4]

In most states and at the federal level, police use of facial recognition for image matching and identification remains entirely unregulated. The following are important considerations for policymakers evaluating how to regulate police use of facial recognition for image matching and identification purposes: (A) databases; (B) algorithmic bias; (C) accountability and oversight; and (D) privacy protections.

A. Databases

Not all databases are created equal. When police or federal agents use image matching facial recognition technology to try to confirm the identity of a person, or to identify an unknown person in an image, they can use any number of databases. Lawmakers and policymakers must consider two important factors when evaluating which data sets ought to be accessible to police for image matching searches: image quality and racial justice.

First, the quality of images in these databases matters. In recent years, images taken for official purposes like passports, mug shots, and drivers licenses are typically standardized, making them more appropriate for facial recognition image searching. Image subjects are advised to take off hats, glasses, and other things that obstruct a full view of the face; the images are taken from the front with high-quality digital cameras; the images are taken in full light, with no shadows on the face; and the images are stored in hi-resolution format. None of these things are consistently true of images scraped from social media sites, like those that populate privately-owned and controlled databases like the one maintained by Clearview AI.[5] Instead, the image quality in these data sets varies widely, raising the likelihood of misidentification and wrongful arrest. Policymakers should therefore prohibit police use of images "taken from the wild" as comparison data when performing image matching searches.

Second, different data sets raise different racial justice and equity concerns. For many years, data has consistently shown that Black and Latino people have faced higher arrest rates than white people for various crimes, like drug offenses, despite engaging in criminal activity at similar rates.[6] As a result, Black and brown people are more likely than white people to populate mug shot databases, even if they have never been found guilty of a crime—let alone a serious crime. Historic and ongoing racial disparities in arrest rates across the country have resulted in mug shot databases that are unjustifiably Blacker and browner than the general population. Allowing police to use mug shot databases for facial recognition searches would therefore exacerbate historical and existing racial disparities in policing by extending that bias into the future, unfairly subjecting people of color to enhanced

[2] "State scans license Mass. License photos to find matches with suspects," December 20, 2016, Boston Globe. https://www.bostonglobe.com/metro/2016/12/20/state-scans-mass-driver-license-photos-find-matches-with-suspects/xyVIxWkPL95hQbx4sUI2WM/story.html

[3] Michael Balsamo, "Watchdog says FBI has access to about 640m photographs," June 4, 2019, AP. https://apnews.com/article/technology-ap-top-news-politics-6f45d569c3084c5ca823ced145de8f82

[4] Jennifer Lynch, "Same Problem, Different Day: Government Accountability Office Updates Its Review of FBI's Use of Face Recognition—and It's Still Terrible," June 6, 2019, EFF. https://www.eff.org/deeplinks/2019/06/same-problem-different-day-government-accountability-office-updates-its-review

[5] Kashmir Hill, "The secretive company that might end privacy as we know it," January 18, 2020, New York Times. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[6] Pierre Thomas, John Kelly, and Tonya Simpson, "ABC News analysis of police arrests nationwide reveals stark racial disparity," June 11, 2020, ABC News. https://abcnews.go.com/US/abc-news-analysis-police-arrests-nationwide-reveals-stark/story?id=71188546

scrutiny and surveillance, in effect supercharging and automating inequality. Additionally, mug shot databases contain images of people suspected—not convicted—of criminal activity. The unfair racial makeup of these databases and the presumption of innocence both counsel in favor of prohibiting police use of mug shot databases for facial recognition purposes.

B. Algorithmic bias

Not all facial recognition algorithms are created equal, and many systems are not ready for primetime. As has been extensively documented by researchers and the federal government, facial recognition algorithms can exhibit race, gender, and age bias.[7] These biases were initially discovered by the groundbreaking research of world-renowned scientists Joy Buolamwini and Timnit Gebru,[8] and they are now widely acknowledged by the scientific community.[9]

In 2019, the non-partisan federal government National Institute of Standards and Technology ("NIST") published a landmark study presenting further evidence that facial recognition algorithms across the board are biased against certain groups.[10] NIST found that most of the nearly 200 algorithms tested performed worse on Black, Asian, and Native American faces, as well as women, the elderly, and children. In addition, when evaluating nationality, faces from West Africa, the Caribbean, East Africa, and East Asia resulted in more uncertainty and more false matches. Across the board, facial verification and identification scans performed best on middle-aged white men and worse on everyone else.[11]

Face recognition technology works best when using front-facing, clear, high-resolution, high-light images. NIST uses these high-quality probe images to test bias and accuracy in facial recognition systems. But in criminal investigations, police often do not use high-quality probe images—the images are often of poor quality, showing people in bad lighting, at strange angles, or with objects obstructing their faces. Consequently, NIST's survey results are misleading; the algorithms NIST studied likely perform much more poorly under real world conditions.

Police frequently argue that lawmakers and the public shouldn't concern themselves too much with these problems, because facial recognition is just one tool in the law enforcement officer's toolbox, and human review of facial recognition search results accounts for any bias and inaccuracy issues.[12] But studies show people are more likely to believe the results of a facial recognition search than their own eyes.[13]

Thus far in the United States, errors resulting from biased algorithms have tended to have the gravest impact on Black people. Police secrecy surrounding the use of facial recognition means we do not know how many people have been wrongfully arrested due to facial recognition errors. But thanks to increased public debate and press scrutiny about the technology, we now know of three such cases in recent years—all of whom are Black men.[14]

[7] Kade Crockford, How is Face Recognition Surveillance Technology Racist?, ACLU, June 16, 2020. https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/
[8] Joy Buolamwini, "Gender Shades," MIT Center for Civic Media. https://www.media.mit.edu/projects/gender-shades/overview/.
[9] John Basil, Republicans And Democrats Concerned About Face Recognition Technology, Your Erie, July 13, 2021. https://www.yourerie.com/news/local-news/republicans-and-democrats-concerned-about-facial-recognition-technology/
[10] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT)
Part 3: Demographic Effects, NIST, December 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
[11] Id.
[12] Qumodo Ltd., Automatic Facial Recognition: Why Do We Need A Human In The Loop?, Medium, March 26, 2019. https://medium.com/@1530019197930/automatic-facial-recognition-why-do-we-need-a-human-in-the-loop-de8366d10680
[13] Lauren Chambers & Emiliano Falcon-Morano, Bias All the Way Down: Research Shows Domino Effect When Human Use Facial Recognition Algorithms, ACLU, Privacy SOS, Sept. 2020. https://privacysos.org/blog/bias-all-the-way-down-research-shows-dominoeffect-when-humans-use-face-recognition-algorithms/.
[14] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," December 29, 2020, New York Times. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

These problems counsel in favor of regulation and law that, short of banning police use of facial recognition entirely, imposes rigorous oversight and accountability of police use of facial recognition for image matching. For the reasons described below, this oversight can only be achieved by centralizing police facial recognition technology.

C. Accountability and oversight

Oversight and accountability of police use of facial recognition technology for image matching in serious criminal investigations poses a substantial regulatory challenge. But as Maine and Massachusetts have demonstrated, it is possible to devise and implement regulatory frameworks wherein police use of facial recognition for image matching technology is centralized at one government agency per state, requiring all police use of the technology to flow through those central entities, limited to very serious criminal investigations, and subject to privacy and due process protections. The federal government could likewise require all law enforcement image matching to run through one centralized service and impose stringent checks and balances on its use. Doing so would mitigate threats to civil rights and civil liberties, facilitate meaningful oversight and accountability, and reduce the threat of wrongful arrests, while also protecting the integrity of the criminal legal system, by ensuring consistent technologies, standards, procedures, training, and techniques are applied across the board.

Centralization addresses the following key problems, described below in detail: I. Scale and police misconduct; II. Consistent technology and training.

I. Scale and police misconduct

There are roughly 18,000 law enforcement agencies in the United States, governed by a patchwork of local, state, and federal laws imposed and overseen by city councils, mayors, county governments, legislatures, and courts. There is no uniform, consistent, national method by which law enforcement agencies are subject to democratic control, transparency, oversight, or accountability.

Police accountability is a real challenge in the United States, in part because of the distributed nature of the power structure. Local control can yield positive results in jurisdictions with courageous local elected officials backed by organized residents. But local control just as often means there is effectively no meaningful oversight or accountability over policing—a problem that grows worse with the accelerating demise of local newsrooms. If a local mayor doesn't want to risk political suicide by challenging a corrupt police department, residents rely on the FBI to step in. But the FBI—an institution with its own significant civil rights and civil liberties problems—cannot police all police; if it tried, it would do nothing else and still fail.

It is extremely difficult to hold police accountable in the United States, and to ensure they uphold the law. As a result, in police departments large and small, across the United States, police officers and departments routinely violate the law.[15] According to an AP report published in 2016, police officers across the United States regularly abuse their access to surveillance databases.[16] A Massachusetts State Trooper issued a rare reprimand for misusing his access to criminal record offender data (a crime in Massachusetts) told a reporter "it was a common practice for troopers to run someone's name through the CORI system for reasons besides law enforcement."[17] The former

[15] Timothy Mclaughlin and Renita D. Young, "Chicago police routinely violated civil rights: U.S. Justice Department," January 13, 2017, Reuters. https://www.reuters.com/article/us-chicago-police/chicago-police-routinely-violated-civil-rights-u-s-justice-department-idUSKBN14X1YR
Sarah Rankin, "Virginia AG sues town, alleging discriminatory policing," December 30, 2021, ABC News. https://abcnews.go.com/US/wireStory/virginia-ag-sues-town-alleging-discriminatory-policing-82005933

[16] Sadie Gurman, "Across US, police officers abuse confidential databases," September 28, 2016, AP. https://apnews.com/article/699236946e3140659fff8a2362e16f43

[17] Colman Herman, "Ex-trooper reprimanded for CORI violations; Says State Police officers routinely used system inappropriately," May 7, 2019, Commonwealth Magazine. https://commonwealthmagazine.org/criminal-justice/ex-trooper-reprimanded-for-cori-violations/

trooper appeared shocked to be punished for what he perceived to be routine violations of the law by police in Massachusetts.

Facial recognition image matching gives police unprecedented power to identify people in sensitive situations: seeking substance use treatment, attending political demonstrations and meetings, visiting politicians and elected officials, speaking with journalists, and getting treatment for serious health conditions like cancer. Police could use facial recognition image matching to identify who is speaking to a reporter working on a police corruption story, or to identify everyone who goes in and out of the mayor's office while she is working on heated police union contract negotiations. Police could use facial recognition technology to get the name and address of a beautiful woman they see walking down the street. A police officer friendly to the January 6 insurrectionists could use the technology to identify even low-level staffers photographed in the West Wing or in Congress. In short, police can use the technology to violate people's rights in ways previously impossible, for political and personal purposes.

It is particularly easy for police to use face recognition technology to violate people's rights when the technology is 100 percent under the control of the police themselves, subject to no meaningful outside scrutiny. The app Clearview AI, for example, gives police officers the ability to use facial recognition for image matching on their personal cell phones.

For the reasons described above, it is impossible to ensure widely distributed police use of facial recognition technology would comport with even the strictest law meant to regulate its use. If 18,000 policing entities in the United States of America are lawfully allowed to possess facial recognition technology, the technology will be abused by close to 18,000 policing entities every year. We do not maintain the oversight and accountability architecture we would need to ensure the technology will not be abused and misused in the hands of so many police departments. Centralizing the technology in the hands of one entity per state, and one at the federal level, will help enable courts, legislators, journalists, and civil rights advocates to provide meaningful oversight and accountability of its use.

II. *Consistent technology and training*

The facial recognition market is crowded with hundreds if not thousands of different technologies sold by as many companies, based here in the United States and around the world. Each system's algorithm performs differently, and each user interface offers different options to end users like police officers and forensic analysts. The wide variety of facial recognition technology available to policing entities could, left unregulated, lead to chaos in the criminal legal system. If each of the 18,000 policing entities in the United States is allowed to purchase or lease access to its own facial recognition system, each of them could end up using systems that operate with different levels of accuracy and reliability, using different training and operating procedures as suggested or required by the manufacturers. Such a widely distributed technology field poses insurmountable challenges to government entities responsible for overseeing policing agencies, as well as to courts and criminal defense attorneys. This is not a hypothetical problem; in the United States policing entities too often don't even know what facial recognition systems their employees are using—or that they are used at all.

A June 2021 U.S. Government Accountability Office ("GAO ") report illustrates the point.[18] The GAO surveyed 42 federal agencies that employ law enforcement officers, asking questions about their use of facial recognition technology. The survey results reveal a chaotic and disorganized

[18] U.S. Government Accountability Officer, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, June 29, 2021. https://www.gao.gov/products/gao-21-518

situation. For example, while 14 agencies said they use non-federally owned facial recognition technology to support criminal investigations, only one agency could name that system.

Similar problems have unfolded across the country at the state and local level, as companies like Clearview AI have aggressively and directly marketed their technologies to even lower-level police officers. In many cases, police have used facial recognition technology without the knowledge—let alone approval—of their own superiors.[19]

When police use facial recognition for image matching in criminal investigations, the stakes are extremely high. Consistent standards and technologies must be applied across policing entities, to protect against wrongful arrests and to ensure the integrity of the criminal legal process. Centralization is the only way to achieve consistency and enable oversight and accountability.

D. Privacy protections

Centralization of police use of facial recognition for image matching is necessary, but it is not enough to protect the public interest. The following privacy protections must also be enshrined in law: I. Limitation to serious crimes; II. Warrant requirement; III. Due process protections.

I. Limitation to serious crimes

Law enforcement agencies should not use face recognition in all types of criminal investigations. The more police use the technique, the more likely they will make mistakes, leading to wrongful arrests and other harms. Loose rules enabling the police to use facial recognition for any type of criminal investigation also provide cover for misuse and abuse. For example, a police officer who wants to know the name of a person or group of people at a protest could justify a search using their images by alleging that they were trespassing or committing disorderly conduct when the photo was taken. This kind of intrusion cannot be tolerated in a free society. But unfortunately, these kinds of abuses are not hypothetical.[20]

Police should not be able to use facial recognition to identify people suspected of minor crimes. Instead, this invasive and controversial technique should be limited to the most serious types of crimes, such as murder, attempted murder, arson, rape, and kidnapping.

II. Warrant requirement

Facial recognition gives the government the power to put a name to any face, an unprecedented privacy invasion akin to forcing every person to wear a police-scannable barcode tattooed on their face. People have a reasonable expectation that the government will not invade their privacy in this manner without good reason and court approval.[21] Just like with cell phone location searches, which similarly allow the government to perform surveillance of people in public in a manner never before possible, the standard to obtain evidence derived from facial recognition should be the probable cause warrant.

Facial recognition searches ought to be limited to those cases where law enforcement agencies can show a judge probable cause that an unidentified individual in an image has committed a violent

[19] Ryan Mac, Caroline Haskins, Antonio Pequeño IV, "Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here," August 25, 2021, Buzzfeed. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table?ref=bfnsplash&utm_term=4ldqpho

[20] For example, in June, reporters disclosed that South Florida police used facial recognition technology to identify peaceful protestors in the aftermath of George Floyd's murder. Public records obtained by journalists "revealed that at least three agencies—the Broward Sheriff's Office and the Boca Raton and Fort Lauderdale police departments—submitted more than a dozen images that referenced protests or protesters, but no crimes." On several occasions, the documents revealed, law enforcement agencies tried to identify people using terms like "Possible protest organizer 'leaders of liberty'" and "associate of protest organizer 'leaders of liberty.'" See: Joanne Cavanaugh Simpson and Marc Freeman, South Florida Police Quietly Ran Facial Recognition Scans To Identify Peaceful Protestors. Is That Legal?, The South Florida Sun Sentinel, June 26, 2021. https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html

[21] Hirose, Mariko, Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology, Connecticut Law Review, 2017. https://opencommons.uconn.edu/law_review/377

felony, that the probe image is of sufficient quality to be subjected to facial recognition and has not been altered, and that the facial recognition search will reveal evidence of the crime. The standard exceptions to warrant requirements ought to apply, in emergencies and where an immediate threat to human life makes obtaining a warrant impractical.

III. Due process protections

The law must provide due process protections for persons arrested pursuant to criminal investigations involving the use of facial recognition technology.

Public defenders report that too often, police in the United States have not disclosed the use of facial recognition technology to criminal defendants. Without mandatory disclosure requirements, law enforcement appears to be shielding information about their use of facial recognition technology from courts and defendants. This practice threatens defendants' basic due process rights and the integrity of our criminal legal system. Criminal defendants must be able to interrogate any digital witness used against them, no matter whether police call it a "tip" or themselves consider it evidence.

If police investigate and then ultimately charge people with crimes after using facial recognition in a criminal investigation, defendants must be able to access critical details about those searches. It is essential that defendants have access to: information about the algorithm used to perform the search (including, if available, the results of accuracy and bias tests); depositions of technicians who perform the searches to find out what investigatory steps were taken after the search; the full results of the search, including images of other people if these were returned; information about the technical "confidence level" at which the system identified the defendant; and other information critical to mount a defense.

The law must additionally state that any result of a facial recognition search does not, without other evidence, establish probable cause justifying arrest, search, or seizure. Finally, the law must require agencies responsible for conducting facial recognition image searches to report the following information to the public on at least an annual basis, for each facial recognition search: the type of technology used, the agency requesting the search, the type of crime(s) under investigation, the race and other demographics of the person depicted in probe images searched, whether an arrest resulted from the search, and whether the search was undertaken subject to a warrant or in an emergency or exigent circumstance.

Part II – Mass Surveillance of Individuals

Machine learning enabled biometric technologies like facial recognition technology are dangerous when they work and when they don't. When they work, these technologies allow the government to track every person's public movements, habits, and associations, not on one day, but on all days—merely with the push of a button. When the technologies fail, racial and gender biases disproportionally harm women and people of color, putting them at risk of wrongful arrest and worse.

Unlike facial recognition for image matching, face surveillance analysis applied to video networks is not commonly deployed by police in the United States. The time is ripe to insist, through law and regulation, that we never build these systems in our communities. The extremely high costs imposed on our communities by face recognition surveillance do not outweigh its marginal benefits. For this and the reasons below, government agencies including police should be permanently prohibited from analyzing video data with face recognition and other machine learning enabled remote biometric surveillance technology.

I. Oversight and accountability are impossible

Unlike facial recognition for image matching, using face recognition for surveillance necessitates a distributed approach. As we describe above, it is possible and relatively simple to standardize and centralize police use of facial recognition for image matching. No such standardization or centralization is possible with face *surveillance*, because of the physical architecture of the technology.

Facial recognition surveillance works by applying automated analysis technology to video data produced by networked surveillance cameras, like those that exist in most major cities today. That means to use the technology, each city's police department would by necessity operate its own facial surveillance network. The distributed nature of the surveillance makes effective oversight and accountability impossible, which is unacceptable—particularly given the heightened risks of this kind of surveillance.

II. *B. Facial Recognition is the Perfect Tool for Oppression*

People in free and open societies should be able to walk around their communities, visit friends and family, seek medical treatment, go to church, and attend political events without worrying that the government is secretly keeping tabs on their every movement, habit, and association. A jealous police officer should not have the capacity to monitor the activities of his girlfriend as she moves about a city; a star-struck officer should not be able to use advanced technology to track the movements of her favorite celebrity; and an officer with a political grudge should not be able to monitor the movements, habits, or associations of a political candidate he opposes.

Today, most cities maintain video surveillance networks across large geographic areas. Each year, governments add more cameras to these networks. The systems can be useful when serious crimes and car accidents occur, because officers can query video from a specific camera at a specific location, on a specific time and date, to look for evidence. The use of face surveillance and other biometric algorithms to automate the analysis of a city's video data qualitatively changes the network, effectively allowing the government to query stored and real-time video images as if each frame were catalogued using the names of each person captured in each frame.

Today, video data is dumb, waiting for police to look at it when something goes wrong. Tomorrow, police could use face surveillance and other biometric analysis algorithms to apply a Google-like search feature to all video data, enabling officials to track and catalogue the movements, habits, and associations of any person, or of all people, merely with the click of a button. This kind of surveillance will not impact all people equally. Like other forms of surveillance, police use of face surveillance applied to video data will harm Black, brown, immigrant, and poor people first and worst.[22]

It is not an accident that the regimes making quick use of the technology for this purpose are authoritarian governments, like those in China and Russia.[23] As scholars have written, face recognition surveillance is "the perfect tool for oppression."[24]

[22] Kade Crockford, "How is face recognition surveillance technology racist?" June 16, 2020, ACLU. https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/

[23] The Chinese government's use of the technology is instructive. According to several reports, the Chinese government uses its network of surveillance cameras integrated with facial recognition technology to monitor millions of Uighurs in Xinjiang. "The facial recognition technology," the *New York Times* reports, "looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review. The practice makes China a pioneer in applying next-generation technology to watch its people, potentially ushering in a new era of automated racism." See: Paul Mozur, One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority, April 14, 2019, New York Times. According to these reports, the PRC has used face surveillance to track how many people of certain ethnic backgrounds are in a location at once, to monitor individual people's movements and activities—including their religious worship habits—and even to flag that someone entered their house from the rear, instead of the front door. Recent reports indicate that police in China's largest provinces are developing a surveillance system they say they want to use to track journalists and international students, among other "suspicious people." See: "Exclusive: Chinese province targets journalists, foreign students with planned new surveillance system," November 29, 2021, Reuters. https://www.reuters.com/technology/exclusive-chinese-province-targets-journalists-foreign-students-with-planned-new-2021-11-29/

[24] Woodrow Hartzog and Evan Selinger, Facial Recognition is the Perfect Tool for Oppression, August 2, 2018, Medium. https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

Our own experience with surveillance mission creep in the United States cautions against allowing government agencies to build surveillance technology that gives officials these powers. Initially, police might say they will only use the technology for terrorism or other extreme events. But time and time again, technologies and powers granted to US government agencies for terrorism are later expanded and used for routine policing, for example in the war on drugs. Surveillance technology implementation and policy only move in one direction; once technologies are implemented, they are not withdrawn. The only way to protect the public interest from the kinds of abuses described above is to enact laws forbidding government agencies from building the architecture of face surveillance.

III. *Face surveillance doesn't work very well*

Facial recognition technology can be inaccurate and racially discriminatory.[25] But the problems researchers have identified with facial recognition image matching systems are magnified when the technology is used to surveil people in public. For example, in 2017, police in London attempted to identify people on a hotlist at a carnival, by using face surveillance algorithms to analyze real time video data. The system wrongfully identified people 98 percent of the time.[26] Nearby, police in Wales reported similarly bad outcomes in a similar test: 91 percent failure.[27] "On 31 occasions police followed up the system saying it had spotted people of concern," the Guardian reports of the test, "only to find they had in fact stopped innocent people and the identifications were false."[28]

IV. *Facial Recognition Poses Grave Constitutional Concerns*

The use of facial recognition for surveillance raises grave constitutional concerns that can only be addressed by prohibiting its use.

First, dragnet biometric monitoring of individuals while they are exercising rights protected by the First Amendment would chill freedom of expression, freedom of speech, and exercise of religion.

Second, the technology poses a fundamental threat to our basic Fourth Amendment privacy rights and right to be left alone.

Law enforcement officials have argued that we have no privacy in public spaces, but the Supreme Court disagrees. In a historic ruling in *Carpenter v. U.S.*, Chief Justice John Roberts held that new technologies enabling retroactive and real-time mass surveillance fundamentally change the balance of power between the government and the people. In that case, the Court ruled that law enforcement officials must get a warrant to obtain historical cell-site location data from phone companies.[29]

Eventually, courts may very well apply *Carpenter's* reasoning to ubiquitous face tracking in public space. But that case was not decided until 2018, decades after Americans began to use cell phones. We cannot wait decades for the courts to rule on the constitutionality of facial recognition technology or other machine learning enabled remote biometric surveillance technologies. We must ban the use of this technology for this purpose now, before police buy and install dragnet surveillance infrastructure.

Third, we must distinguish facial recognition from even the most invasive tracking technologies that the courts have considered to date. Cell phone tracking is fundamentally different from facial recognition in at least two significant ways. First, you do not have to bring your phone with you if

[25] Kade Crockford, How is Face Recognition Surveillance Technology Racist?, ACLU, June 16, 2020. https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/
[26] Vikram Dodd, UK Police Use Of Facial Recognition Technology A Failure, Says Report, May 14, 2018, The Guardian. https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure.
[27] Ibid.
[28] Ibid.
[29] Case page for Carpenter v. United States, SCOTUSblog. https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/.

you want to go somewhere anonymously—a political demonstration, a clinic, a bar, or a motel. But you cannot leave your face at home. Second, for a government official to access information from your phone, they must in most cases either possess the device itself or request access from a third-party service provider. In either case, they must obtain a warrant. But judicial authorization and oversight become substantially less effective tools to prevent misuse and abuse if a government agency acquires facial recognition technology and can use it in-house without going through any other gatekeeper. For this reason, legislative or executive intervention is imperative—*before* government acquisition and use of the technology becomes endemic.

For these reasons, legislatures and executive branch officials should prohibit police use of facial recognition for surveillance, and intervene to ensure the physical architecture for this kind of dragnet monitoring is never built.

Part III – Affect recognition and other remote biometric monitoring tools

Facial recognition is not the only machine learning enabled biometric technology that allows the government to use our features to monitor us without our knowledge or consent. Very limited studies exist to show how these technologies work. And none of them are promising.

First, automatic gender recognition, a subfield of face surveillance technology, regularly misgenders transgender and gender-nonconforming people.[30]

Second, algorithms that claim to identify how someone is feeling based on their facial expressions are unreliable and based on pseudoscience. For example, one study used so-called "affect recognition" software to analyze images of NBA players' official portraits and found it more likely to classify Black players as angry and contemptuous despite smiling like their white counterparts.[31] Moreover, research from leading scholar Dr. Lisa Barrett at Northeastern University has shown that it is simply not possible to reliably discern how someone feels based on the physical characteristics of their face.[32]

Without law prohibiting its use, it is only a matter of time before companies try to sell this kind of snake-oil technology to police to use in interrogations, on our streets, and even in our schools. The government should prohibit police use of these untested, dangerous technologies.

Conclusion

Machine learning enabled biometric technologies pose grave risks to free and open societies, racial justice, and core civil rights and civil liberties. Short of banning its use entirely in policing, governments should tightly regulate police use of image matching, by centralizing its use and subject it to strict limitations and court oversight. But effective regulation is not applicable to face surveillance or affect recognition. These latter forms of facial recognition ought to be permanently prohibited in government.

[30] Matthew Gault, Facial Recognition Software Regularly Misgenders Trans People, February 19, 2019, Vice. https://www.vice.com/en_us/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people.

[31] Lauren Rhue, Emotion-Reading Tech Fails The Racial Bias Test, The Conversation, January 3, 2019,. https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.

[32] Lisa Feldman Barrett, et al. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest, vol. 20, no. 1, July 2019, pp. 1–68, DOI: 10.1177/1529100619832930.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

American Medical Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

[redacted]

January 12, 2022

Dr. Eric S. Lander
Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Re: RFI Response: Biometric Technologies

Dear Dr. Lander:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the Request for Information (RFI) from the Office of Science and Technology Policy (OSTP) regarding public and private sector uses of biometric technologies, published in the Federal Register on October 8, 2021 (86 Fed. Reg. 56300). The AMA appreciates OSTP's acknowledgement that the use of biometric information has the potential to both help and harm individuals and the public. This letter will focus on three of OSTP's requested topics: (1) descriptions of use of biometric information for recognition and inference; (2) exhibited and potential harms of a particular biometric technology; and (3) exhibited and potential benefits of a particular biometric technology.

Descriptions of use of biometric information for recognition and inference

The AMA is actively monitoring the use of biometric information for recognition and inference in immigration, privacy of genetic information, and use of electronic prescribing of controlled substances (EPCS). Specifically, we have advocated to the Department of Homeland Security (DHS) against the use of facial recognition in the immigration process for reasons that will be outlined below in "Exhibited and potential harms of a particular biometric technology." Also discussed in that section of our response is the AMA's concern around results of mail-order and over-the-counter (OTC) genetic tests. Finally, we summarize our support of the use of biometric technologies for EPCS in "Exhibited and potential benefits of a particular biometric technology." We are also actively monitoring emerging state laws addressing facial recognition. Several laws have been enacted while others are proposed. Some laws address certain contexts (e.g., immigration or law enforcement) while others focus on necessary controls. Several laws require court orders or warrants before facial recognition technology may be used, public notice requirements, and/or explicit statutory authorization for the technology's use.

The AMA's stance on these issues was developed through a balancing of considerations, including potential individual harms resulting from use of the biometric information, envisioned benefits to the users of the technology in question, accuracy of a given technology, equity, and AMA policy. Our overall approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our

policymaking body, the House of Delegates (HOD), which support strong personal privacy protections. AMA policy and ethical opinions on privacy and confidentiality provide that an individual's privacy should be honored unless waived by the person in a meaningful way, is de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of privacy or breaches of confidentiality. When breaches of confidentiality are compelled by concerns for public health and safety, these breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest entities and individuals as possible to achieve the necessary end.

Exhibited and potential harms of a particular biometric technology

Facial recognition

The AMA has significant concerns with the use of facial recognition in certain contexts, including immigration. Facial recognition technology has serious racial, gender, and age biases that lead to considerably decreased accuracy for this technology. Additionally, any entity seeking access to an individual's health information (including biometric information) must pass the stringent test of showing why its professed need should override the individual's most basic right in keeping his or her own information private. Absent such a justification, and because facial recognition has been shown by multiple studies to be inaccurate due to bias, the AMA does not support its use by federal, state, or local governments.

Studies have found that accuracy of facial recognition technology is linked to physical factors, including: pose, illumination or expression of a face, cosmetics, glasses, hair, or other easily changeable characteristics that may cover parts of a face; general image quality; inherent facial characteristics, particularly skin reflectance or underlying facial structure; and aging over time. A study from the National Institute of Standards and Technology (NIST) found that the majority of facial recognition algorithms in the industry possess biases that span race, gender, and age.[1] "While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied," said Patrick Grother, a NIST computer scientist and the report's primary author."[2]

The NIST study evaluated most of the software algorithms available at the time (nearly 200 algorithms from 99 developers). It focused on each individual algorithm's ability to perform one of two tasks, each of which are among facial recognition's most common uses:

> The first task, confirming a photo matches a different photo of the same person in a database, is known as "one-to-one" matching and is commonly used for verification work, such as unlocking a smartphone or checking a passport. The second, determining whether the person in the photo has any match in a database, is known as "one-to-many" matching and can be used for identification of a person of interest.[3]

To evaluate whether each algorithm can sufficiently complete the "one-to-one" and/or "one-to-many" matching protocols, researchers collected data on the two types of potential software errors: false

[1] https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[2] *Id.*
[3] *Id.*

positives and false negatives. A false positive means that the software wrongly recognized photos of two different individuals as the same person, while a false negative means the software failed to match two photos that show the same person. As such, there are countless factors that can, and do, negatively impact the accuracy of "one-to-one" and "one-to-many" matching.

Any federal policy suggesting the use of facial recognition technology must demonstrate that it is accurate and unbiased. Race and ethnicity are fundamental demographics to consider when determining the quality and accuracy of facial recognition technology. This is especially relevant considering that the algorithms designed to pilot these facial recognition technologies are not objective in nature but fluctuate widely depending on the demographic of the creator themselves. As an illustration of these algometric biases, NIST's test revealed that facial recognition algorithms that were developed in China showed low false positive rates on East Asian faces.[4] On the other hand, facial recognition algorithms that were developed in the U.S. and Western Europe were 10 to 100 times more likely to inaccurately identify a photograph of a Black or East Asian face, compared with a White one.[5] With such a wide variation across algorithm development, this produces significant discrepancies in the false non-match rate, which has been found to be between 0.1 percent and 10 percent.[6] This variation is unacceptable in a technology policy that will impact individuals from all races and ethnicities.

Additionally, a July 2020 Government Accountability Office (GAO) report analyzing DHS' pilot facial recognition program noted that DHS' facial recognition technology is still struggling with algometric biases.[7] GAO officials stated that DHS' analysis of its pilot facial recognition programs is limited due to lack of data on age, gender, and ethnicity for travelers entering and exiting the country. The report also notes that verification algorithm performance was lowest on women, Black people, and very young or very old people in comparison to performance on middle-age [W]hite men. Put differently, "[i]n verification algorithms, false positive rates for [W]hite males and [B]lack females varied by factors of 10 to more than 100, meaning the lowest-performing algorithm could be over 100 times more accurate on [W]hite male faces than on [B]lack female faces. Additionally, for verification and identification vendor tests, false positives were higher for women than men."[8] These differences are very likely to result in more frequent misidentification for the individuals who would be subject to use of facial recognition technology.

Moreover, additional studies found constant biases in favor of White men with error rates never worse than 0.8 percent when determining the gender of light-skinned men. However, women in the studies were more often inaccurately identified with a correlation between darker skin tone and a higher error rate.[9] For medium skinned women the error rates were between 20.8 and 34.7 percent. But, for the darkest-skinned women in the data set the error rates increased to between 46.5 and 46.8 percent.[10] For those women, the technology was doing little more than guessing their gender at random. The U.S. companies that owned this facial recognition algorithm claimed an accuracy rate of more than 97 percent. However, the data sets used to assess this performance were more than 77 percent male and more than 83 percent White.[11] As such, this technology not only had biased results, but the proprietors of these technologies claimed a

[4] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[5] *Id*.
[6] https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/.
[7] https://www.gao.gov/assets/gao-20-522.pdf.
[8] *Id*.
[9] https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212?s=09.
[10] *Id*.
[11] *Id*.

greater accuracy than warranted based on the limited data set on which the algorithm was trained. These studies underscore our concerns with the federal government using a technology to identify individuals when such technology is unable to distinguish gender and race accurately and consistently.

Genetic information

The AMA has had significant involvement in policy and clinical discussions concerning the quality and accuracy of genetic testing over the past decade. An individual's genetic information (i.e., DNA) is the biological element responsible for determining one's identity. Accordingly, DNA is inherently identifying; genetic data cannot be de-identified. Use of direct-to-consumer (DTC) genetic tests has grown exponentially over the past decade, with an estimated 100 million individuals expected to have undergone the testing by the end of 2021.[12] The U.S. Food and Drug Administration classifies these tests as medical devices, but they also are a mechanism for massive information-gathering whereby personal, self-disclosed information, including a person's genome, can be used by the company or third parties to sell products and services. However, unbeknownst to most customers, this information can be used against them. While federal law—the Genetic Information Nondiscrimination Act (GINA)—prevents health insurance companies and employers from discriminating based on genetic information, these restrictions do not apply to life, disability, or long-term care insurance companies, which can result in insurance application rejections not only for the applicant but for their family members who may not have consented to use of DTC genetic data.[13] Users of consumer genetic testing should be advised of the potential risks of their participation. To address these concerns, the AMA urges the federal government to advance the following policies:

- Prevent genetic testing entities without explicit, informed, and noncoerced user consent from transferring information about a user such as birthdates and state of residence to third parties which may result in the re-identification of the user based on surname inference;
- Prohibit pharmaceutical companies, biotechnology companies, universities, and all other entities with financial ties to genetic testing companies from sharing identifiable information, including DNA, with other parties without informed consent of the user;
- If a data security or privacy breach occurs with a DTC genetic company or its collaborators, require the company to inform all users and relevant regulatory bodies of the breach and the impact of the unprotected private data on those individuals.
- Ensure that research using consumer genomic data derived from saliva or cheek swabs or other human samples is treated as research on human subjects requiring informed consent with, or similar to, those required by the Department of Health and Human Services Office for Human Research Protection, using an "opt in" option to allow more consumer choice in the consent process; and
- Add long-term care, disability insurance, and life insurance consumer protections to GINA.

Additionally, while the AMA strongly supports the quality of such testing where health care professionals are extensively trained and have established protocols for the collection of specimens, the performance of tests, and returning results (including identifying the limitations of the testing), we have strong concerns when DNA collection, testing, and return of results are not undertaken by trained health care professionals under the rigorous protocols of the Clinical Laboratory Improvement Amendments. This is

[12] https://www.pewtrusts.org/en/research-and-analysis/reports/2021/10/the-role-of-lab-developed-tests-in-the-in-vitro-diagnostics-market.
[13] https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008.

because errors (including contamination, incorrect procedures, and misinterpretation) undermine the quality and accuracy of the DNA testing and, if inappropriately performed, could have disastrous consequences for individuals and their families.

To authenticate identifiable biological evidence, those who are responsible for managing this process must be carefully trained in the handling and collection of samples. The biometric samples are extremely susceptible to contamination; thus, the quality and usability of the specimen will be lost with exposure to even miniscule amounts of DNA from others than the applicant. Such contamination may occur if multiple samples are handled at one time or if the handler touches a non-sterile surface while in possession of the DNA specimen. To appropriately analyze the collected samples, a polymerase chain reaction (PCR) process is performed. If the specimen is contaminated by another person's DNA, the PCR process will copy the DNA that is present within the specimen, including the impurity, and there will be no ability to distinguish between the DNA of the person of interest and the DNA of the contaminant. In addition, these biometric samples are highly sensitive to environmental factors.[14] Introduction of moisture, sunlight, or narrow temperature changes, factors that are easily overlooked and underestimated, also destroy the integrity of the DNA specimen.[15] Sample quality and meticulous conservation of the procedures required for biometric data analysis determine accuracy and usability of DNA evidence.

Exhibited and potential benefits of a particular biometric technology

EPCS is important to support high-quality patient care and to reduce fraud, tampering, and diversion of prescriptions for controlled substances. EPCS utilizes multifactor authentication, including biometric authentication as one of the acceptable methods. A well-designed electronic prescription system adds value to physicians' practice of medicine and supports better patient care. Yet, to accomplish greater uptake of EPCS across the nation, the Administration must update its regulations around the use of biometric authentication in EPCS.

The SUPPORT for Patients and Communities Act (SUPPORT Act) included a requirement that Medicare Part D prescriptions for controlled substances be electronically prescribed. The SUPPORT Act also directed the U.S. Drug Enforcement Administration (DEA) to update its EPCS regulations pertaining to the biometric component of multifactor authentication. It is critically important for the DEA to modernize its EPCS rules to increase the number of DEA registered physicians utilizing EPCS. By significantly reducing drug diversion and fraudulent prescriptions for opioid analgesics and other controlled substances, increased adoption of EPCS by physicians could contribute to ending the nationwide epidemic of opioid-related deaths. Physicians want to adopt EPCS, utilize biometric authentication, and have it integrated into their practice workflows. However, physicians have expressed great frustration that they are hampered by the limited selection of biometric products required by the DEA for EPCS, which are high-cost and poorly integrated. The current DEA requirements for multifactor authentication have been a significant hurdle in adoption of EPCS. In particular, the rigid and burdensome requirements for biometrics included in the DEA's 2010 interim final rule preclude physicians from deploying user-friendly biometric devices already found in their practices.
The AMA continues to urge the DEA to reexamine the scope of technology that is compliant with EPCS requirements and allow for lower-cost, high-performing biometric devices (e.g., fingerprint readers on laptop computers and mobile phones) to be leveraged in multifactor authentication. Additional information can be found in the AMA's June 22, 2020, letter to the DEA.

[14] https://www.nist.gov/system/files/documents/2019/08/19/standards_for_prevention_monitoring_and_mitigation_of_dna_contamination_draft.pdf.
[15] https://www.ncjrs.gov/nij/DNAbro/evi.html.

Conclusion

We appreciate the opportunity to respond to this RFI and welcome the opportunity to discuss our views further with OSTP. If you have any questions, please contact Laura Hoffman, Assistant Director, Federal Affairs, at [redacted].

Sincerely,

[redacted]

James L. Madara, MD

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

ARTICLE19

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Dear Members of the Office of Science and Technology Policy,

Thank you for the opportunity to submit input on public and private sector uses of biometric technologies.

ARTICLE 19 is an international human rights organization that seeks to protect and promote freedom of expression. It is headquartered in London and has offices in the United States, Bangladesh, Brazil, Kenya, Mexico, Myanmar, Netherlands, Senegal, and Tunisia. We are submitting this input based on our significant empirical and legal work around the world.

Our work on biometrics over the last decade has included analysis of the human rights implications of these systems and evidence of how their design, development, and deployment in a growing number of domains. These include specific consideration of how these technologies are used for identity verification, identification, surveillance, and inference of attributes, including emotional states and those protected by law. This submission provides crucial findings from our work, information about how stakeholders are affected, and principles that should govern the use of biometric technologies, particularly in light of the fact that biometric technologies rely on increasingly sophisticated and complex artificial intelligence and machine learning systems. Data exploitation; identification and tracking; inference and prediction of information; profiling to sort, score, categorize, assess, and rank individuals; and how these relate to decision making, rights, resource allocation, are among the issues addressed.

With respect to emotion recognition technology, there are no ethical uses for its use and despite claims that this technology can improve with time, given the pseudoscientific and racist foundations of emotion recognition on one hand, and fundamental incompatibility with human rights on the other, the design, development, deployment, sale, and transfer of these technologies should be prohibited and banned. This type of technology is built around three discredited and erroneous scientific assumptions: that facial expressions are universal; that emotional states can be unearthed from them; and that such inferences are reliable enough to be used to make decisions.

There is a need to examine how existing discourses, such as human rights law, data protection, sectoral privacy regulation, and research ethics, relate to different applications and methods of biometric technologies. Overriding challenges to the deployment of biometric technologies include informational asymmetry, the opacity and secrecy of biometric profiling and surveillance; discrimination, unfairness, inaccuracies, and bias; re-identification and de-anonymization; and lack of legal regulatory frameworks as well as technical expertise in policymaking. This submission also addresses the deployment of biometric technologies in China specifically, which lacks human rights safeguards and is a major exporter of such technology around the world.

In this submission, we wish to provide you with resources and highlight some crucial findings from our work that we hope will inform this consultation and any broader efforts, such as efforts to develop an AI Bill of Rights.

1. In January 2021, we released a report, "Emotional Entanglement", on the emotion recognition market in China and its implications for human rights. Here, we critically analyse claims made by 27 Chinese companies that sell this technology for three use cases: public security, education, and driving safety. Some of our main findings are as follows:
    a. **The design, development, sale, and use of emotion recognition technologies are inconsistent with international human rights standards.** While emotion recognition is fundamentally problematic, given its discriminatory and discredited scientific foundations, concerns are further exacerbated by how it is used to surveil, monitor, control access to opportunities, and impose power, making the use of emotion recognition technologies untenable under international human rights law (pp. 36–44).
    b. **Emotion recognition technologies' flawed and long- discredited scientific assumptions do not hinder their market growth in China.** Three erroneous assumptions underlie justifications for the use and sale of emotion recognition technologies: that facial expressions are universal, that emotional states can be unearthed from them, and that such inferences are reliable enough to be used to make decisions. Scientists across the world have discredited all three assumptions for decades, but this does not seem to hinder the experimentation and sale of emotion recognition technologies (pp. 18–35).

c. **Chinese local governments' budding interest in emotion recognition applications confer advantages to both startups and established tech firms.** Law enforcement institutions' willingness to share their data with companies for algorithm-performance improvement (p. 22), along with local government policy incentives (pp. 18, 20, 22, 24, 25, 33), enable the rapid development and implementation of emotion recognition technologies.
d. **The emotion recognition market is championed by not only technology companies but also partnerships linking academia, tech firms, and the state**. Assertions about emotion recognition methods and applications travel from academic research papers to companies' marketing materials(pp. 22, 25-26) and to the tech companies' and state's public justifications for use (pp. 20, 22-33). These interactions work in tandem to legitimize uses of emotion recognition that have the potential to violate human rights.
e. **Chinese law enforcement and public security bureaus are attracted to using emotion recognition software as an interrogative and investigatory tool.** Some companies seek procurement order contracts for state surveillance projects (pp. 18-22) and train police to use their products (p. 22). Other companies appeal to law enforcement by insinuating that their technology helps circumvent legal protections concerning self-incrimination for suspected criminals (pp. 42-43).
f. **While some emotion recognition companies allege they can detect sensitive attributes, such as mental health conditions and race, none have addressed the potentially discriminatory consequences of collecting this information in conjunction with emotion data.** Some companies' application programming interfaces (APIs) include questionable racial categories for undisclosed reasons (p. 41). Firms that purportedly identify neurological diseases and psychological disorders from facial emotions (pp. 41-42) fail to account for how their commercial emotion recognition applications might factor in these considerations when assessing people's emotions in non-medical settings, like classrooms.
g. **Chinese emotion recognition companies' stances on the relationship between cultural background and expressions of emotion influence their products**. This can lead to problematic claims about emotions being

presented in the same way across different cultures (p. 40) – or, conversely, to calls for models trained on 'Chinese faces' (p. 41). The belief that cultural differences do not matter could result in inaccurate judgements about people from cultural backgrounds that are underrepresented in the training data of these technologies – a particularly worrying outcome for ethnic minorities.

h. **None of the Chinese companies researched here appears to have immediate plans to export their products.** Current interest in export seems low, (p. 40) although companies that already have major markets abroad, such as Hikvision and Huawei, are working on emotion recognition applications (pp. 23, 27, 29-33, 40).

2. Building on this, in April 2021, ARTICLE 19 also published its biometrics policy which warns against the use of biometric technologies, especially on national security and counterterrorism grounds, without a sufficient legislative framework to protect human rights. We consider that a human rights-based approach ought to be embedded at the start of the design and development of any technology. A summary of our recommendations is as follows:
    a. States should ban biometric mass surveillance
    b. States should ban the design, development and use of emotion recognition technologies
    c. Public and private actors who design, develop and use biometric technologies should respect the principles of legitimacy, proportionality and necessity
    d. States should set an adequate legislative framework for the design, development and use of biometric technologies
    e. Government authorities must ensure that the design, development and use of biometric technologies are subject to transparency and open and public debate
    f. Transparency requirements for the sector should be imposed and thoroughly implemented by both public and private sectors
    g. States should guarantee accountability and access to remedies for human rights violations arising from biometric technologies
    h. The private sector should design, develop and deploy biometric systems in accordance with human rights standards.

3. More generally on AI, in April 2019, we published a report "Governance with Teeth", which documents how "ethical" approaches to AI are toothless when treated as an end in and of themselves, how they obscure responsibility and buy time for private companies to experiment with AI technologies, including biometrics, while causing real harm to people. We highlighted the importance of a human-rights based approach in regulating AI.

4. Finally, in our April 2018 published in conjunction with Privacy International, "Privacy and Freedom of Expression in the Age of Artificial Intelligence" we identified the human rights implications of these systems in detail. Each of the novel interferences with privacy are significant and have an impact on the a range of other human rights and societal norms. Many of the issues raised in this report are relevant to consider with respect to the concerns about the use of biometric surveillance:
    a. to identify people who wish to remain anonymous;
    b. to infer and generate sensitive information about people;
    c. to profile people based upon population-scale data;
    d. to make consequential decisions using this data, some of which profoundly affect people's lives or the ability of groups to freely associate and express themselves

We would be happy to discuss any aspect of these reports with you and provide evidence as may be necessary. We look forward to additional opportunities to provide input to this consultation.

Best,

Dr. Courtney C. Radsch
U.S. and Tech Policy Advisor
ARTICLE 19
www.article19.org

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Attorneys General of the District of Columbia, Illinois, Maryland, Michigan, Minnesota, New York, North Carolina, Oregon, Vermont, and Washington

January 14, 2022

Via Electronic Submission

Dr. Eric Lander
Director, Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: RFI Response: Biometric Technologies
86 FR 56300

Dear Dr. Lander:

We, the undersigned Attorneys General of the District of Columbia and the states of Illinois, Maryland, Michigan, Minnesota, New York, North Carolina, Oregon, Vermont, and Washington, submit this letter in response to the Office of Science and Technology Policy's (OSTP) request for information on Public and Private Sector Uses of Biometric Technologies.[1] As our respective states' chief law enforcement officers, we are charged with protecting the public interest, particularly against unlawful discrimination and unfair trade practices. We appreciate the opportunity to respond to this request for information and address these issues.

The COVID-19 pandemic has made Americans more reliant on technology than ever. Remote workforces are the new normal, and our children continue to rely on online learning tools. Consumers increasingly use technology for virtual meetings, applying for jobs and credit, to access important records, and to make everyday purchases. The proliferation of artificial intelligence (AI) and advanced biometric technology in our online lives has great potential. These evolving technologies can provide increased accuracy, speed, and convenience for many consumers. But they also come with serious concerns about bias, privacy, and transparency. Our offices have a strong interest in ensuring that AI and biometric technologies do not exacerbate inequalities, are deployed responsibly, and are secure. Across the country, jurisdictions are regulating this evolving

[1] Office of Science and Technology Policy, *Request for Information on Public and Private Sector Uses of Biometric Technologies*, 86 FR 56300 (Oct. 8, 2021).

industry.[2] We support OSTP's stated goal of creating a "bill of rights for an AI-powered world"[3] and urge you to mandate strong protections against these vulnerabilities. Importantly, any such federal protections should supplement, not pre-empt, state and local measures (including those discussed below) that we and other States have put into place to protect our residents.

Bias in Biometric Technology Must Be Prevented.

In a perfect world, using AI would eliminate both implicit and explicit human bias, and create more equitable results. But there is no shortage of examples of biometric tools that have significant bias built into them.

For example, the National Institute of Standards and Technology (NIST) has found that facial recognition software misidentifies Native Americans, Asians, and African Americans at significantly higher rates than white people.[4] It also noted increased failures at identifying women, the elderly, and children, noting that "[m]iddle-aged white men generally benefited from the highest accuracy rates."[5] Facial recognition software has also proven to be less reliable for identifying individuals' gender when they have a darker skin tone.[6] Voice recognition tools display significant racial bias, as well,[7] particularly in failing to recognize certain accents and African American Vernacular English.[8] Remote testing software that was deployed widely in 2020 to protect against cheating in schools failed to account for disabilities and neurocognitive disorders.

[2] *See, e.g.,* Ark. Code § 4-110-101, *et seq.* (Personal Information Protection Act); Cal. Civ. Code §§ 1798.81.5 (reasonable data security law); Cal. Civ. Code §§ 1798.100, *et seq*. (California Consumer Privacy Act of 2018); 740 I.L.C.S. 14/1, *et seq.* (Illinois Biometric Information Privacy Act); Me. Rev. Stat. tit. 25, § 6001 (regulates government use of facial recognition technology); MD. Code Ann., Com. Law §§ 14-3501 *et seq*. (Maryland Personal Information Protection Act); N.Y.C. Admin. Code §§22-1201-1205 (biometric privacy law for commercial establishments); Or. Rev. Stat. 646.605(12)(a)(iv) (Oregon Consumer Information Privacy Act); Tex. Bus. & Com. Code Ann. § 503.001 (biometric privacy law); Wash Rev. Code § 19.375.020 (biometric privacy law).

[3] Dr. Eric Landry, et al., *Americans Need a Bill of Rights for an AI-Powered World*, WIRED (Oct. 8, 2021), available at https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.

[4] Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, The Washington Post (Dec. 19, 2019), available at https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[5] *Id.*

[6] Joy Buolamwini, et al., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, IN PROCEEDINGS OF THE CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, pp. 77-91 (Feb. 2018), available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[7] Alex Perala, *Study Finds Racial Bias in Leading Speech Recognition Systems*, FIND BIOMETRICS (March 24, 2020), available at https://findbiometrics.com/study-finds-racial-bias-in-leading-speech-recognition-systems-903246/.

[8] Claudia Lopez, *Speech Recognition Tech is Yet Another Example of Bias*, SCIENTIFIC AMERICAN (July 5, 2020), available at https://www.scientificamerican.com/article/speech-recognition-tech-is-yet-another-example-of-bias/.

As a result, students with movement disorders, ADHD, PTSD, and other conditions or disabilities[9] can be falsely flagged for cheating when their eye, face, and body movement do not match the expected baselines.[10] Significantly, the use of flawed biometric technologies has led law enforcement agencies to falsely identify people as a suspect in a crime,[11] and it has led to improper denials of employment and credit opportunities with no recourse or explanation.[12] Left unchecked, biometric technology bias can have real and devastating impacts on people's lives.[13]

But these problems are not inherent to the technology; the technology is simply reliant on the data (and people) used to build it. In fact, the same NIST study that found high rates of false positive matches in non-white faces found significantly less disparity in technology that was developed in Asian countries.[14] This shows that where bias is acknowledged, monitored, and accounted for, it can be prevented.[15] The District of Columbia recently introduced legislation

[9] Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, Center for Democracy & Technology (Nov. 16, 2020), available at https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/.

[10] Shea Swauger, *Our bodies encoded: Algorithmic test proctoring in higher education*, HYBRID PEDAGOGY (Apr. 2, 2020), available at https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/.

[11] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NEW YORK TIMES (Dec. 29, 2020), available at https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html. ("In February 2019, Nijeer Parks was accused of shoplifting candy and trying to hit a police officer with a car at a Hampton Inn in Woodbridge, N.J. The police had identified him using facial recognition software, even though he was 30 miles away at the time of the incident. . . . He is the third person known to be falsely arrested based on a bad facial recognition match. In all three cases, the people mistakenly identified by the technology have been Black men."); *see also* Rashawn Ray, *5 questions policymakers should ask about facial recognition, law enforcement, and algorithmic bias*, THE BROOKINGS INSTITUTION (Feb. 20, 2020), available at https://www.brookings.edu/research/5-questions-policymakers-should-ask-about-facial-recognition-law-enforcement-and-algorithmic-bias/.

[12] Caitlin Chin, *Assessing employer intent when AI hiring tools are biased*, THE BROOKINGS INSTITUTION (Dec. 13, 2019), available at https://www.brookings.edu/research/assessing-employer-intent-when-ai-hiring-tools-are-biased/.

[13] *See, e.g.*, Bolajoko Olusanya et al., *Transcutaneous bilirubin nomograms in African neonates*, PLOS ONE (Feb. 13, 2017), available at https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0172058 (finding that measurement tools that underestimate jaundice risk for darker-skinned patients may lead to delayed interventions in life-threatening neonatal health conditions); Elise Ruter, *Study shows skewed dermatological datasets result in less accurate models*, MEDCITY NEWS (July 20, 2021) (research shows that overrepresentation of lighter skin tones results in disparities in AI model ability to diagnose skin conditions for patients with darker skin).

[14] Press Release, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019), available at https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[15] Stephen Ritter, *Biometrics Aren't Inherently Biased—We're Training Them Wrong*, FORBES (Nov. 4, 2020), available at https://www.forbes.com/sites/forbestechcouncil/2020/11/04/biometrics-arent-inherently-biased---were-training-them-wrong/?sh=1d57e3a21ebd.

designed to combat discrimination and biases in algorithms and AI.[16] This legislation will prohibit companies from using discriminatory algorithms in key decision-making processes, and it will require entities to perform annual audits of their technology to identify any disparate impact the technology may have on protected groups.[17] We also support a recent push to require tech companies to make their coding and algorithms more transparent to regulators so there can be independent evaluation of the underlying data.[18] With biometric information being used in new and developing ways, it is critical that we take concrete, aggressive steps now to put a stop to discrimination in these processes, and the OTSP's bill of rights will be crucial in this endeavor.

Biometric Information Must be Protected, and Consumers Must Be Fully Informed.

The brief history of public and private use of biometric information has shown it to be a minefield for mishandling and misuse. The same technological advances that have increased the available uses of biometrics have also resulted in new ways for hackers and bad actors to use this information to gain access to sensitive information. For example, artificial fingerprint databases have been created capable of "spoofing" a fingerprint access scanner,[19] and Apple recently had to upgrade its Face ID technology because a "3D model constructed to look like the enrolled user may be able to authenticate via Face ID."[20]

Moreover, unlike traditional passwords or pin codes, biometric data cannot simply be changed when a database is breached.[21] Therefore, it must be held with the highest security, and people must know how that information is being used. Unfortunately, we have already seen how

[16] Press Release, *AG Racine Introduces Legislation to Stop Discrimination In Automated Decision-Making Tools That Impact Individuals' Daily Lives*, OFFICE OF THE ATTORNEY GENERAL FOR THE DISTRICT OF COLUMBIA (Dec. 9, 2021), available at https://oag.dc.gov/release/ag-racine-introduces-legislation-stop. (Additionally, businesses will be required to disclose when algorithms are used in decision-making processes in education, employment, housing, credit, and other areas.)

[17] *Id.*

[18] Michael Kearns, et al., *Ethical Algorithm Design should guide technology regulation*, THE BROOKINGS INSTITUTION (Jan. 13, 2020), available at https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation/.

[19] Philip Bontrager, et al., *DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution*, 2018 IEEE 9TH INTERNATIONAL CONFERENCE ON BIOMETRICS THEORY, APPLICATIONS AND SYSTEMS, BTAS 2018 (October 2018), available at https://www.cse.msu.edu/~rossarun/pubs/BontragerRossDeepMasterPrint_BTAS2018.pdf.

[20] Apple Support, *About the security content of iOS 15 and iPadOS 15* (published Oct 26, 2021), available at https://support.apple.com/en-ca/HT212814.

[21] Lenildo Morais, *Biometric Data: Increased Security and Risks*, SECURITY MAGAZINE (May 6, 2020), available at https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks. ("The security of biometric authentication data is of vital importance, even more than the security of passwords, as passwords can be easily changed if exposed. A fingerprint or retinal scan, however, is immutable. Disclosure of this or other biometric information can put users at permanent risk and create significant legal exposure for the company that loses the data. In the event of a breach, it creates an enormous challenge because physical assignments, such as fingerprints, cannot be replaced. Biometric data in the hands of a corrupt entity also has very frightening but real implications.")

vulnerable some biometric information can be.[22] The privacy risks are significant and are growing with the technology. It is vital that real, enforceable security protocols are developed and implemented across the industries utilizing biometric data.

The security and privacy risks discussed above are often exacerbated by a lack of transparency by entities using biometric data. Without clear information about when, why, and how biometric information is collected, used, bought, and sold by a company, consumers cannot make informed decisions about their biometric information or take steps to protect themselves when there is a security issue.

Just this past summer, the popular social media app TikTok changed its privacy policy to include a new section notifying users that the app was collecting biometric data, including "faceprints and voiceprints."[23] This change was automatic within the application, and users do not have an ability to grant or deny permissions.[24] This came even after TikTok agreed to a $92 million settlement in a lawsuit that alleged it illegally collected and sold biometric data from U.S. users.[25] This is just one example of ways in which everyday technology can collect and distribute biometric information from unsuspecting individuals, potentially putting their identity and security at risk.

Additionally, several lawsuits filed against Clearview AI, Inc. (Clearview) highlight the extent to which businesses are capitalizing on people's biometric information without the individual ever transacting or interacting with them in the first place.[26] Clearview has been accused of collecting images found online to create a database of billions of faceprints without the knowledge or consent of any of those contained in the database. Clearview then sold access to that database to many third parties. None of the individuals included had consented or were aware that their images had been collected or sold.[27]

[22] Chris Baraniuk, *Biostar security software 'leaked a million fingerprints,'* BBC NEWS (August 14, 2019), available at https://www.bbc.com/news/technology-49343774. ("More than a million fingerprints and other sensitive data have been exposed online by a biometric security firm, researchers say. … As well as fingerprint records, the researchers say they found photographs of people, facial recognition data, names, addresses, passwords, employment history and records of when they had accessed secure areas.")

[23] Sarah Perez, *TikTok just gave itself permission to collect biometric data on US users, including 'faceprints and voiceprints,'* TECHCRUNCH (June 3, 2021), available at https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/.

[24] *Id.*

[25] Corinne Reichert, *TikTok to pay $92M to settle lawsuit over data privacy*, CNET (Feb. 25, 2021), available at https://www.cnet.com/tech/mobile/tiktok-to-pay-92m-to-settle-lawsuit-over-data-privacy/.

[26] *See, e.g., American Civil Liberties Union v. Clearview AI, Inc., et al.*, Complaint, Case No. 20 CH 4353 Cook County Circuit Court (filed May 28, 2020), available at https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint; *State of Vermont v. Clearview AI, Inc.*, Complaint, Docket No. 226-3-20 Cncv, Vermont Superior Court, Chittenden Unit, Civil Division (filed Mar. 10, 2020), available at https://ago.vermont.gov/wp-content/uploads/2020/03/Complaint-State-v-Clearview.pdf.

[27] *Id.*

States and local jurisdictions are increasingly undertaking regulatory efforts to protect the privacy of their residents. [28] Illinois, with its Biometric Information Privacy Act,[29] was the first state to enact a comprehensive law governing the collection and use of biometric information. Since then, the states of California, New York, and Washington, and the cities of Berkeley, New York, Oakland, Portland, and San Francisco, have enacted laws specifically prohibiting the use of biometric information in certain circumstances, such as to clock-in to a job or to identify suspects in a crime.[30] Additionally, the District of Columbia and several other states have passed legislation to address biometric privacy concerns.[31] In these jurisdictions, although the collection and use of biometric data may not regulated, the information is protected as personal identifiable information (PII), mandating a certain level of security and requiring entities to provide notice when the information has been compromised.[32] These statutes are responsive to the harm consumers face from companies that otherwise have little incentive to prioritize cybersecurity. While the District and states should and will continue to take action to protect their residents, all Americans should have these protections, and this patchwork effort would be greatly assisted by a national effort.[33] Entities that collect and use biometric data, such as TikTok and Clearview, do not restrict themselves to certain states or localities. The threat of a biometric data breach does not end at our jurisdictional borders and local jurisdictions alone cannot protect their residents; national and international action is vital.[34]

We strongly urge OSTP to incorporate robust and measurable security and transparency protocols into the technology bill of rights. This should include, but not be limited to (1) a requirement that biometric data be maintained at least as securely as other protected personal identifiable information (as is already required by many state laws); (2) a prohibition on the sale or transfer of biometric data to third parties; (3) clear and conspicuous disclosures to users of when biometric data is being collected and its intended use; (4) a requirement that users affirmatively *opt-in* to biometric data collection, rather than opt-out; (5) a simple mechanism for consumers to delete biometric data collected by companies; and (6) a ban on the use of discriminatory algorithms

[28] Michael A. Rivera, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 Fordham Intell. Prop. Media & Ent. L.J. 571 (2019), available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1717&context=iplj.

[29] Biometric Information Privacy Act, 740 I.L.C.S. 14/1, *et seq.*

[30] Berkeley, CA, Mun. Code § 2.99; Cal. Lab. Code § 1051; Cal. Pen. Code § 832.19 (prohibition on police use of biometric surveillance systems [eff. until Jan. 1, 2023]); N.Y. Labor Law § 201-A (fingerprinting of employees prohibited); N.Y.C. Admin. Code §§ 22-1201-1205 (biometric privacy law for commercial establishments); Oakland, CA, Mun. Code § 9.64; Portland City Code § 34.10.010; San Francisco, CA, Mun. Code § 19B; Wash Rev. Code § 19.375.020.

[31] D.C. Code § 28-3851, *et seq.*; Ark. Code § 4-110-105; California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, *et seq*.; N.C. Gen. Stat. §§ 75-61, 75-65; N.Y. Gen. Bus. Law §§ 899-AA, *et seq.*; Or. Rev. Stat. 646A.604; Vt. Stat. Ann. tit. 9 § 2435; Wash. Rev. Code Ann. § 19.255.10.

[32] *Id.*

[33] As mentioned above, if OSTP or other federal agencies take action in this space, they should be explicit that such measures do not pre-empt state and local standards.

[34] Frank Nolan, *Implications of U.S. laws on collection, storage, and use of biometric information*, EVERSHEDS SUTHERLAND (US) LLP (July 2020), available at https://us.eversheds-sutherland.com/portalresource/Biometrics%20whitepaper_July%202020.pdf

coupled with a requirement that companies perform an annual audit to monitor for discrimination and immediately take action to rectify any discrimination revealed by such audit.

We appreciate the opportunity to comment on these important issues, and we applaud the OSTP for its thorough consideration of our concerns.

Sincerely,

[redacted]

KARL RACINE
Attorney General for the District of Columbia

[redacted]

KWAME RAOUL
Illinois Attorney General

[redacted]

BRIAN E. FROSH
Maryland Attorney General

[redacted]

DANA NESSEL
Michigan Attorney General

[redacted]

KEITH ELLISON
Minnesota Attorney General

[redacted]

LETITIA JAMES
New York Attorney General

[redacted]

JOSH STEIN
North Carolina Attorney General

[redacted]

ELLEN F. ROSENBLUM
Oregon Attorney General

[redacted]

THOMAS J. DONOVAN, JR.
Vermont Attorney General

[redacted]

BOB FERGUSON
Washington State Attorney General

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Avanade

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

FEEDBACK TOPICS (Please see input for topics 3, 4, and 6):

1. Descriptions of use of biometric information for recognition and inference
2. Procedures for and results of data-driven and scientific validation of biometric technologies
3. Security considerations associated with a particular biometric technology.
4. Exhibited and potential harms of a particular biometric technology
5. Exhibited and potential benefits of a particular biometric technology
6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case.

Descriptions of use of biometric information for recognition and inference:

Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

Procedures for and results of data-driven and scientific validation of biometric technologies:

Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

Security considerations associated with a particular biometric technology.

Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.

- **Voice Recognition – Voice recognition technology, also known as speaker recognition, exists to enable a machine to recognize and differentiate different humans, based upon the pattern of speech. Data points used to differentiate speakers can include cadence, tone of voice, inflection, as well as word selection, amongst many other attributes; different models will use different data points. This technology has been the victim of a security breach in banking – a non-identical twin was able to mimick the voice of his brother, the account holder, to successfully access banking details. https://www.bbc.co.uk/news/technology-39965545**
- **Facial Recognition – Facial recognition technology allows a machine to differentiate between one face and another. This technology can identify humans in either static imagery, or moving video. The technology is flawed when used in isolation, as "deepfakes" and filters, are able to replace one human face with another. Mitigations should be applied, including attempting to ensure video is live (asking actions or phrases to be described), using infrared to confirm the muscle movement behind the face, or in combination with other authentication methods.**
- **Fingerprint Recognition – Fingerprint recognition is a relatively understood technology. Flaws in the use of fingerprinting relate to the securing and disclosure of fingerprint copies that have been stored. Once a fingerprint copy is stolen, this cannot be retrieved – and individuals are at risk of having their fingerprint data re-used or copied (for example, using 3d printed overlays) for the rest of their life. Mitigations include storing one-way encrypted copies of fingerprints only, making it possible to distinguish humans, whilst making it impossible to recreate and copy the original fingerprint.**
- **What is perhaps slightly more palatable when it comes to trust and preventing the undesired dissemination of personal biometric information is instead the storage and usage of a 'hash' of the original biometric information, rather than the original biometric information itself. For example, where the storage of fingerprints is not feasible or undesired, a one way 'hash' of an individual's fingerprints are often stored and used instead for a particular scenario such as door entry. As the hash method could be propriety to the implementation, it has the benefit of being both secure and any potential data leak could not include the original biometric information.**

Exhibited and potential harms of a particular biometric technology:

We expect your office to get substantial feedback on the underlying inaccuracies and biases (especially for non-male people of color) that have been demonstrated in countless and various biometric surveillance systems. For example: Biometrics ethics: why facial recognition still has racial bias (raconteur.net).

Rather than pile on more examples of inaccuracies and biases, we would like to call your office's attention to two other board categories of ethical concern than should be given care review and scrutiny for all new policy and process decisions:

- **Racial Bias and Colonialism in the basic concepts and processes of automated surveillance:**
  - **Artificial Intelligence from Colonial India: Race, Statistics, and Facial Recognition in the Global South**
  - **How the rise of 'digital colonialism' in the age of AI threatens Africa's prosperity**
  - **The problems AI has today go back centuries**
  - **Research summary: Algorithmic Colonization of Africa**
- **Harmful mental/emotional impacts of surveillance:**
  - **What Constant Surveillance Does to Your Brain**
  - **New surveillance AI can tell schools where students are and where they've been**
  - **Remote testing monitored by AI is failing the students forced to undergo it**
  - **Chinese Surveillance Is Literally Getting in Workers' Heads**

Exhibited and potential benefits of a particular biometric technology:

Consider benefits including, but not limited to: Benefits arising from use in a specific domain (absolute benefit); benefits arising from using a specific modality of biometric technology (or combination thereof) compared to other modalities in a specific domain (relative benefit); and/or benefits arising from cost, consistency, and reliability improvements. Information on evidence of benefit (in the case of an exhibited benefit) or projections, research or relevant historical evidence (in the case of potential benefit) is also welcome.

Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case.

Point a) Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies

Regarding assessment and mitigation of harm, we have developed a comprehensive Digital Ethics Assessment Framework, which guides practitioners through an evaluation of 50 ethical considerations for any product, project, or system. For each category or ethical consideration, we consider both direct and indirect impacts, the relevance of those impact to the particular project, and the current and desired state to which that consideration is addressed. Addressing the ethical concern may include mitigation of risk as well as elevation of potentially positive impacts. So for example, a development team might address accessibility by reducing gaps in compliance with accessibility standards (reducing harm) and they might go further by introducing assistive technologies or processes so individuals with impairments can more actively engage (elevating positive outcomes).

The complete list of ethical considerations in our framework is as follows:

1. **Individual impacts: Accessibility, inclusivity, data collection, data control, data use, finances and opportunity, mental health and wellbeing, physical health and safety, personal time and attention, free speech, personal agency, child protection, personal legal status**
2. **Societal impacts: Impact on Politics, labor force, economy, education, health care, law enforcement, criminal justice, social services, access to information, military, international/global affairs**
3. **Environmental impacts: Energy use, material use, waste, obsolescence, pollution/operational impact, impact on animals/biodiversity**
4. **Programmatic controls: Organizational ethics, suitability, values alignment, ethical testing, traceability, diversity of contribution, compensation for contribution, access control, security, reliability, explainability, transparency, operational oversight, strategic oversight, independent oversight, stakeholder monitoring, stakeholder feedback, stakeholder recourse, human intervention, accountability**

Point e) Performance auditing and post deployment impact assessment:

We recommend, as explained in our framework, that performance auditing and post-deployment impact assessment be augmented with stakeholder impact monitoring, stakeholder feedback, and stakeholder recourse. Ongoing monitoring should have components of operational, strategic, and independent oversight.

Additional considerations

In addition to the considerations above, it is important for the sake of inclusivity to provide one or more alternatives to biometric use cases for both physical, national, religious, and other differences. For example, those that are deaf-without-speech require non audio / vocal alternatives to vocal recognition. Also those that choose to adorn their appearance for religious reasons (such as a niqab or burka) should not necessarily be made to comply with facial recognition if it is against their faith.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Aware

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

.

AWARE

Office of Science and Technology Policy

In response to Document Number: 2021-21975

Request for Information for Public and Private Sector Uses of Biometric Technologies

January 12, 2022

Submitted to:

Office of Science and Technology Policy
BiometricRFI@ostp.eop.gov

Submitted by:

Tracy Hulver | Senior Director, Product Management
[redacted]

Aware, Inc.
40 Middlesex Turnpike
Bedford, MA 01730-1404
[redacted] | www.aware.com

Public and Private Sector Uses of Biometric Technologies

Scope: OSTP invites input from any interested stakeholders, including industry and industry association groups; civil society and advocacy groups; state, local, and tribal governments; academic researchers; technical practitioners specializing in AI and biometrics; and the general public. In particular, OSTP is especially interested in input from parties developing biometric technologies, parties acquiring and using such technologies, and communities impacted by their use. Input is welcome from stakeholders, including members of the public, representing all backgrounds and perspectives.

Information Requested: Respondents may provide information for one or as many topics below as they choose. Through this RFI, OSTP seeks information on the use of biometric technologies in the public and private sectors, including on the following topics:

Please see Aware, Inc.'s responses below.

1. *Descriptions of use of biometric information for recognition and inference:* Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (*e.g.*, past, current, or planned deployment) and, if applicable, the impacted communities.

Aware allows for the capture, matching, and verification of biometric data. This includes fingerprint, facial, iris and voice. Aware customers typically want to utilize biometric data for two primary purposes: 1) capturing a biometric for matching; and 2) capturing a biometric for verification.

Our primary markets are law and policy enforcement organizations and entities that want to use biometric capture for end-user verification applications such as multifactor authentication (MFA). Biometrics are a desirable form for MFA due to the ease-of-use, speed, fidelity, and accuracy of biometric capture and matching. Aware believes that giving the user control of their biometric data is a preferred method of deploying biometric solutions. MFA is a proven way of increasing the security of an ecosystem, such as access to financial information, healthcare data, and other sensitive information. Giving the user control of how and where their biometric information is being stored and used increases privacy of the user as well as providing a strong method of securing transactions.

2. *Procedures for and results of data-driven and scientific validation of biometric technologies:* Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

There are two primary settings in which validation procedures and performance metrics are relevant: 1) in R&D, and 2) in deployment. In R&D, of critical importance are the following:

1. Devising a test set that is independent of the data used to train and/or develop biometric algorithms, in order to ensure that algorithms generalize to real world operational settings
2. Persisting that test set to provide a way to benchmark algorithm improvements
3. Measuring performance metrics that can accurately assess the relevant operational characteristics of a particular biometric technology

Performance metrics can vary depending on the type of biometric algorithm.

The following table details the primary performance metrics used by R&D for various biometric algorithms.

Biometric Algorithm	Relevant Performance Metrics
Liveness	Attack Presentation Classif. (Spoof Detection) Error Rate [APCER] vs. Bonifide Presentation Classif. (Live) Error Rate [BPCER] APCER vs. BPCER as a function of spoof type BPCER at fixed APCER as a function of race (racial bias) BPCER at fixed APCER as a function of gender (gender bias)
Verification (all biometrics)	False Non-Match Rate (FNMR) vs. False Match Rate (FMR) Failure to Enroll Rate (frequency with which the algorithm cannot generate a template for verification) FNMR vs. FMR as a function of image quality FNMR at fixed FMR as a function of race (racial bias) FNMR at fixed FMR as a function of gender (gender bias)
Identification (all biometrics)	False Negative Identification Rate (FNIR) vs. False Positive Identification Rate (FPIR) Failure to Enroll Rate (frequency with which the algorithm cannot generate a template for identification) FNIR vs. FPIR as a function of image quality FNIR at fixed FPIR as a function of race (racial bias) FNIR at fixed FPIR as a function of gender (gender bias)
Biometric Sample Quality Assessment	Regression/Classification accuracy based on groundtruthed samples

Table 1: Performance metrics for biometric technologies

Clearly, the same performance metrics are relevant in both R&D and deployment settings, but vendor access to operational metrics is severely curtailed after deployment, primarily due to privacy restrictions and client security. In deployment, metrics are often indirect measurements of biometric algorithm performance that are computed by the client, and typically reflect the impact they have on their business use case. For example, usability (failure to enroll) is often an important operational consideration at operating points that satisfy minimum client security requirements.

A supporting infrastructure that enables collection of performance data is vital to providing clients with the capability to monitor operational system performance. As an example, Aware provides a reporting mechanism on backend servers that enables clients to observe incoming data streams and to review the results of algorithm measurements. This can be used to adjust thresholds or operational configurations to optimize system performance. In addition, data streams can be anonymized and provided to Aware to further improve and enhance algorithm performance in cases where a collaborative relationship exists with a deploying partner.

3. *Security considerations associated with a particular biometric technology*. Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.

Although this question specifically refers to security, we see security and privacy as two intimately connected, but separate and critically important factors in promoting the widespread use and adoption of biometrics. For the purpose of this discussion, we define the two as follows. Security in biometrics can be considered from two perspectives: security of a particular biometric in transactions as it relates to error rates, and the security of the biometric in transit or at rest, as it relates to its possible compromise. Privacy in biometrics relates to concealing the connection between an individual's identity and their biometrics, regardless of the success or failure of any security measures in place. A solution that provides complete privacy for a biometric obviates (or at least reduces) the need for its security.

Security in biometrics as it relates to error rates, focuses on false match rate (FMR) in the case of verification, false positive identification rate (FPIR) in the case of identification, and attack presentation classification error rate (APCER) in the case of liveness. Willful circumvention of biometric technologies is becoming increasingly difficult as matching and liveness technologies continue to improve, enabling systems to operate at lower and lower error rates. However, these must be implemented in smart workflows that lowers the statistical risk of a single malicious user exploiting potential vulnerabilities. Biometric solutions are highly robust, but they are ultimately reliant on the statistical improbability of a single user

being able to randomly match a lookalike (in the case of verification or identification) or to spoof a liveness solution with multiple, creative attempts. For example, limiting the number of allowable failed attempts to some small number (e.g., 1 or 2) limits the ability of a user to learn and take potential advantage of a system's vulnerabilities.

There are also multiple points of potential failure in the security of a biometric system: at the point of biometric sample creation, in storage and during transmission. As an example, Aware's liveness solution provides several mechanisms during mobile image acquisition to bind the image capture to the real-time transaction, to eliminate the possibility of emulator injection attacks during image acquisition (biometric sample creation). Sophisticated watermarking techniques then guarantee the integrity of the biometric sample storage to prevent replay attacks. Finally, end-to-end encryption protects against tampering or substitution during transmission. All three points of failure must be addressed to provide secure and tamper proof execution.

Regarding privacy, recent advances in crypto-biometric authentication approaches are enabling the use of biometrics as unique keys in zero-knowledge proofs for authentication. A user uses their own biometric (which must be proven to be live) to unlock a secret known only to the interacting institution to prove their identity without giving up their own biometric. Privacy is enhanced because no biometric ever needs to leave the device of the user and no central repository of biometric templates is required to authenticate. Obviating the need for a central database also enhances the security of the authentication system because there is no biometric template to steal.

4. *Exhibited and potential harms of a particular biometric technology:* Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

Like any technology, biometrics can be used for ill or good, depending on the application. From our (vendor) perspective, the harms we consider are related to harms we can mitigate through the development and control of our own technology. For example, gender and race bias have recently been the focus of concerns regarding the use of face recognition algorithms. Aware has made a great effort and taken significant strides to develop training and scoring methodologies for our matchers that minimize race and gender bias. At a time when training data is becoming scarcer due to privacy concerns, it is more important now

than ever to develop training methodologies that are not at the mercy of the data being trained on. Blindly relying on data without a true understanding of the effect of gender and race on facial recognition and liveness is a mistake that is often made by fledgling biometric companies.

5. *Exhibited and potential benefits of a particular biometric technology:* Consider benefits including, but not limited to: Benefits arising from use in a specific domain (absolute benefit); benefits arising from using a specific modality of biometric technology combination thereof) compared to other modalities in a specific domain (relative benefit); and/or benefits arising from cost, consistency, and reliability improvements. Information on evidence of benefit (in the case of an exhibited benefit) or projections, research or relevant historical evidence (in the case of potential benefit) is also welcome.

The value of biometric fusion is often underestimated or discounted due to the cost of implementation. Multiple biometric data collection requires multiple sensors, and for that reason is often rationalized away. However, the fusion of face and voice is a powerful combination that is frequently overlooked. The technologies are easily integrated on mobile phones and can provide an added level of security not possible by either biometric alone. Further, they allow the straightforward implementation of both authentication and liveness. Score level fusion allows increased accuracy for both verification and liveness, with redundancy in biometrics if one modality is unusable due to a sub-optimal capture environment. Again, a good understanding of fusion and score mapping in particular is required to extract full advantage from such an integration. Aware's historical expertise in biometric fusion has enabled it to do this, as well as to apply that expertise to its other multi-biometric offerings.

6. *Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case:* Information regarding:

a. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;

As a publicly traded company, Aware is bound be certain ethical and business requirements that we not only follow, but embrace. In addition, because we are a global organization with customers all over the world across many different vertical markets, we abide by numerous business, security, and privacy best practices to meet both governmental and customer-required compliance and regulatory guidelines and mandates. Some of these include best practices on privacy (i.e., GDPR, NIST Privacy Framework, California Consumer Privacy Act, etc.) and security (i.e., NIST 800-53, SOC II, FedRAMP, etc.).

b. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

It is recommended that prior to an organization deploying a biometric verification system they clearly identify the biometrics and explain how the data will be captured, stored, and used. The production of a Privacy Impact Analysis is also created and made available to all parties that will be utilizing the biometric system. Next, the organization should plan on having 3 phases during the deployment 1) Proof-of-Concept (POC), 2) limited pilot, and 3) full production.

POC: During the POC, a limited number of users will be asked to interact with the biometric system and test the usability and accuracy of the biometric capture and matching. The size of the POC will vary depending on the final size and demographic makeup of the deployment but typically, limiting the POC to 5-100 users is desirable. The length of the POC will also vary depending on the availability of the users testing the system but 30-60 days should be a reasonable target. The POC should be limited to a user base that is internal to the organization of to external users who understand that they are using a non-production system. A clear set of agreed upon use cases need to be identified and what success criteria need to be met in order to move into the pilot phase. Items that require testing should not only focus on the workflow of the biometric system but also the various environmental variables that need to be tested such as, for face capture and verification different lighting environments (i.e., bright light, low light, reflected sunlight, direct sunlight, etc.) For voice capture and verification different background noise levels need to be analyzed (i.e., no background noise, windy conditions, background voice/music, talking through a mask, etc.). Adjustments to the sensitivity of the matching and liveness scores should be available for fine tuning of the biometric system to achieve the proper balance of ease-of-use and security.

Pilot: Moving into the pilot phase will expand the user base access to the system as well as expanding the overall user cases identified. Typically, a pilot will include external users accessing production systems but will limit the user community to a specific user case or cases. An example of this would be targeting a specific demographic group or geolocation for the pilot. The size of the pilot should include a representative sample of the final user community and therefore will vary greatly as to the number of users, but a rule of thumb is to target a pilot size of 10%-15% of the final deployment size. Obviously for large deployments a pilot may be accomplished in stages to ensure a manageable size of users during the project roll-out. The length of the pilot phase will vary depending on the size of the user community being included as well as the smoothness of the pilot deployment, but a timeframe of 3-9 months should be planned.

Production: Finally, after confidence in the system is achieved, full deployment can proceed.

d. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;

A detailed analysis of the requirements for data collection, storage, and use will be needed before safeguards can be implemented. The requirements will vary greatly depending upon the use cases. An example of this is that use of biometric data within a closed ecosystem such as employment enrollment and verification will be much more controllable by the organization than implementing a biometric authentication and verification system for citizens and consumers. One variable that will not change is the requirement for the ecosystem to follow best practices on privacy (i.e., GDPR, NIST Privacy Framework, California Consumer Privacy Act, etc.) and security (i.e., NIST 800-53, SOC II, FedRAMP, etc.)

These security and privacy controls will help establish best practices that the vendors as well as the organizations deploying the solution can implement and follow. Of course, local and federal laws will also have to followed where applicable.

e. Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);

A supporting infrastructure that enables collection of performance data is vital to providing clients with the capability to monitor operational system performance. As an example, Aware provides a reporting mechanism on backend servers that enables clients to observe incoming data streams and to review the results of algorithm measurements. This can be used to adjust thresholds or operational configurations to optimize system performance. In addition, data streams can be anonymized and provided to Aware to further improve and enhance algorithm performance in cases where a collaborative relationship exists with a deploying partner.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Barbara Evans

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Barbara J. Evans, Ph.D, J.D., LL.M.
Professor of Law and Stephen C. O'Connell Chair
Fredric G. Levin College of Law
Professor of Engineering
Herbert Wertheim College of Engineering

312-J Holland Hall
309 Village Drive
P.O. Box 117620
Gainesville, FL 32611
[redacted]

January 15, 2022

Office of Science and Technology Policy
Executive Office of the President
The White House
via email to BiometricRFI@ostp.eop.gov

Re: Comments of Prof. Barbara J. Evans, Ph.D., J.D., LL.M. in response to Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, *Federal Register*; 86(193):56,300-56,302 (Oct. 8, 2021)

Thank you for the opportunity to participate in Nov. 18, 2021 Biometric Technologies Listening Session and to comment in the above-captioned RFI.

I am commenting today in my personal capacity as a member of the public, rather than on behalf of my institution or the State of Florida, which is my employer. For purposes of identification, I am Professor of Law and Stephen C. O'Connell Chair at the University of Florida Levin College of Law, with joint appointment as Professor of Engineering at the University of Florida Wertheim College of Engineering, located in Gainesville, Florida. I have over 25 years' experience – both as a scholar and, before that, as a partner in private law practice – addressing regulatory and ethical issues with major infrastructure systems, including large-scale data infrastructures. My current focus is on data privacy, safety, and civil rights concerns affecting medical software and, in particular, artificial intelligence/machine learning (AI/ML) clinical decision support (CDS) software and software supporting the genomic bioinformatics pipeline. I have no conflicts to disclose.

I am attaching a legal research paper analyzing some of the questions raised by your RFI. It supplies a more complete account, with citations to relevant statutes, government advisory documents, and scholarly literature, of the points I briefly summarize below.

All of the page references below are to that research paper: Barbara J. Evans, *The HIPAA Privacy Rule at Age 25: Pushing Past Boomer Bioethics to Promote Equity in AI-Enabled Health Care* (University of Florida Levin College of Law Legal Studies Research Paper Series No 21-36) [for brevity, "Evans, LSRP 21-36"]

A one-size-fits-all approach to an AI Bill of Rights is inappropriate because the safety, privacy, and civil rights concerns raised by AI software depend heavily on the context in which it is applied.

The "Bill of Rights" analogy is memorable but it incorporates two core beliefs: First, a unitary Bill of Rights can protect people's interests in all contexts where AI/ML software is applied. Second, protecting those rights is primarily a federal concern. Both these beliefs require careful scrutiny.

In particular, I would urge OSTP to distinguish AI-enabled biometric technologies intended for use in clinical healthcare settings from those employed by retailers, educators, credit-scorers, social media providers, law enforcement, and other non-medical actors in modern "surveillance societies." *See Evans, LSRP 21-36, at pages 3-4*.

Some AI-enabled biometric software is in the nature of clinical decision support (CDS) software, offering diagnostic or treatment recommendations to healthcare professionals in clinical healthcare settings. Protecting safety and civil rights in clinical healthcare settings involves the interplay of state, federal, and non-governmental authorities already involved with these matters.

More generally, medical and non-medical AI differ in ways that may justify different civil rights protections, including for data privacy. For non-medical AI/ML tools, the United States has glaring gaps in privacy and other civil rights protections that are a worthy focus for OSTP's policymaking efforts. In clinical healthcare settings, however, the "overlay" of the federal HIPAA Privacy Rule onto state-level medical privacy rules and information fiduciary duties of healthcare providers creates a civil rights framework that is surprisingly well-tailored to the major challenges we face in an age of AI-enabled health care. *See Evans LSRP 21-36, at pages 4-5*.

This framework is, however, at times misunderstood. The HIPAA Privacy Rule is often criticized based on the (erroneous) perception that it is weaker than the European Union's General Data Protection Regulation (GDPR). In the clinical healthcare contexts where the HIPAA Privacy Rule applies, it is in many respects *stronger* than GDPR. *See Evans LSRP 21-36, at page 8*, discussing how EU Member States apply GDPR in clinical healthcare settings. It will be important not to set policy based on a misunderstanding of the protections GDPR provides.

Health equity is the major unresolved ethical and civil rights challenge with AI/ML medical software

See Evans LSRP 21-36, at pages 8-10, noting that: "Training datasets for AI/ML CDS tools tend to overrepresent men of European ancestry while underrepresenting members of other racial and ethnic groups and women. Empirical studies of how CDS tools perform for transgender patients do not even appear to exist, but it is known these patients face special health risks (such as elevated incidence of aortic aneurism in transgender women). Those risks can be obscured if AI/ML training datasets force-fit these patients into gender-binary categories without further nuancing to highlight special medical needs within those categories. AI/ML tools that perform well in high-resource, well-staffed academic medical centers often underperform at lower-resourced community hospitals where much of the American population receives care. To be blunt, much of the AI/ML CDS software developed to date is racist, misogynistic, trans-oblivious, and dispenses recommendations that vary in quality depending on your socioeconomic status."

See Evans RP 21-36, at pages 10-19, attributing much of this problem to structural and systemic inequities in U.S. health care. However, part of the problem traces to 1970s-era information privacy norms that prevail both in bioethical discourse and in information privacy theory more generally. These norms can have a disparate impact that fuels inequity in medical AI software. Eliminating those inequities is the defining ethical challenge for medical AI.

Strengthening privacy, safety, and civil rights protections for medical AI will require a carefully integrated state, federal, and non-governmental effort

The HIPAA Privacy Rule offers a powerful toolkit for addressing three defining bioethical challenges in the age of AI-enabled clinical care. Those challenges are to protect individual privacy, to keep patients safe by enabling data flows to regulators, scientists, and others charged with ensuring software safety, and to combat inequity and injustice in AI/ML medical software. *See Evans RP 21-36, at pages 24-35*, discussing regulatory pathways for assembling more inclusive, equitable training data for medical AI.

For this to be successful, however, the HIPAA Privacy Rule has certain gaps that need to be filled, and doing so will require coordination among state and federal policymakers as well as non-governmental actors. Crafting a "Bill of Rights" will require an interactive rather than top-down, federal effort. Perhaps you already have taken that into account, but it bears re-emphasis.

The HIPAA Privacy Rule was the product of careful consultations between federal and state privacy regulators to accommodate their joint roles in medical privacy. The Privacy Rule's preemption provisions, like those of the HIPAA statute, grant the States the power to improve its civil rights protections. Additionally, the 21st Century Cures Act of 2016 tasked the U.S. Food and Drug Administration (FDA) with overseeing the safety of AI/ML CDS tools. The FDA's proposed regulatory approach for CDS software would assess its performance using flows of real-world clinical health data, which the Privacy Rule enables. A one-size-fits-all approach to medical and non-medical AI privacy might impede this data-driven safety oversight.

See Evans RP 21-36, suggesting specific measures to enhance safety, privacy, and equity for medical AI. These measures include:

A. Recognize that informed consent and safe-harbor de-identification (stripping away specific identifiers from the data) do not provide effective privacy protection. Even when consent seems ethically necessary, it may not be sufficient to protect privacy.
B. Adopt policies to nudge software developers and users toward greater reliance on statistical de-identification techniques (i.e., computational privacy protections, privacy-by-design), which can provide more reliable, measurable privacy protection.
C. Educate the public that, in an age of AI-enabled medical software, having your data included in AI/ML training data helps ensure that the resulting software will provide well-informed health recommendations for you, and for people like you.
D. Require ethics review bodies (and other gatekeepers charged with overseeing access to training data for AI/ML medical software) to include members having the technical expertise necessary to oversee strong, modern computational privacy protections.
E. Strengthen "information fiduciary" requirements for parties who control AI/ML CDS tools, whether as developers, vendors, or users.
F. Implement "public benefit" requirements to ensure that any non-consensual uses of people's data will serve socially beneficial purposes, such as reducing inequities in health care.

G. Promote legal accountability for privacy violations and for inequitable, unsafe AI/ML medical software through appropriate allocation of legal liabilities.

Thank you for this opportunity to provide comments.

Sincerely,

Barbara J. Evans, Ph.D., J.D., LL.M.
Professor of Law and Stephen C. O'Connell Chair
University of Florida Levin College of Law
Professor of Engineering
University of Florida Wertheim College of Engineering
Spessard L. Holland Law Center
PO Box 117620
Gainesville FL 32611-7620


`

The HIPAA Privacy Rule at Age 25:

Pushing Past Boomer Bioethics to Promote Equity in AI-enabled Health Care

Barbara J. Evans, Ph.D., J.D., LL.M.

University of Florida Levin College of Law
Legal Studies Research Paper Series No. 21-36

`

THE HIPAA PRIVACY RULE AT AGE 25:
PUSHING PAST BOOMER BIOETHICS TO PROMOTE EQUITY IN AI-ENABLED HEALTH CARE

Barbara J. Evans*

`

THE HIPAA PRIVACY RULE AT AGE 25: PUSHING PAST BOOMER BIOETHICS TO PROMOTE EQUITY IN AI-ENABLED HEALTH CARE

INTRODUCTION

President Bill Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law on August 21, 1996.[1] Its 25th birthday passed largely unnoticed last August in an America wracked by contagion and a rough exit from Afghanistan. HIPAA was mainly an insurance statute best known in medical circles for its annoying offshoot, the HIPAA Privacy Rule,[2] which took effect in 2003-2004 after a long and contentious rulemaking.[3] Rarely in the nation's history has a regulation been so widely reviled.[4]

An alternative view, advanced here, is that the Privacy Rule was ahead of its time. Its drafters foresaw an increasingly diverse American population served by 21st-century health systems that, increasingly, would derive general medical knowledge from informational as well as clinical research.[5] In that faraway future, rigid requirements to obtain informed consent before scientific use of people's health data might block critical data flows and exacerbate healthcare disparities, inadvertently abetting injustice in health care. That future is here now, as health systems grow dependent on artificial intelligence and machine learning (AI/ML) medical software. Long scorned, the Privacy Rule might be just what the doctor ordered to advance equitable, justice-serving medical AI.

In October 2021, the White House Office for Science and Technology Policy (OSTP) launched a study of AI-enabled biometric technologies.[6] Two OSTP officials later called for a new "Bill of Rights for an AI-Powered World"[7] and OSTP is working to develop it.[8] The Bill of Rights analogy presumes a single, overarching set of principles could suffice for AI/ML software of all types in all contexts.

This article expresses grave doubt about a one-size-fits-all approach. A cautionary example is AI/ML clinical decision support (CDS) tools that offer recommendations to healthcare professionals

---

* Professor of Law and Stephen C. O'Connell Chair, University of Florida Levin College of Law; Professor of Engineering, University of Florida Wertheim College of Engineering, [redacted]

1 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

2 45 C.F.R. pts. 160, 164.

3 Barbara J. Evans, *Institutional Competence to Balance Privacy and Competing Values: The Forgotten Third Prong of HIPAA Preemption Analysis*, 46 U.C. DAVIS L. REV. 1175, 1213-15 (2013); K. Grace Ko, *Partial Preemption Under the Health Insurance Portability and Accountability Act*, 79 S. CAL. L. REV. 497, 505 (2006).

4 *See, e.g.,* COMM. ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION, INST. OF MED., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 66 (Sharyl Nass, Laura A. Levit, and Lawrence O. Gostin, eds., 2009), available at http://www.nap.edu/catalog/12458.html [hereinafter, "IOM, PRIVACY REPORT"]

5 *See* Kayte Spector-Bagdady, *Governing Secondary Research Use of Health Data and Specimens: The Inequitable Distribution of Regulatory Burden Between Federally Funded and Industry Research*, J. L. AND THE BIOSCIENCES 1, 4 (2021) (discussing the shift from human-subjects clinical research that studies people's bodies to informational research "research with all the stuff [such as data and biospecimens] derived from them.")

6 Office of Science & Technology Policy, Notice of Request for Information (RFI) on Public and Private Sector uses of Biometric Technologies, Federal Register (Oct. 8, 2021); 86(193): 56,300-56,302.

7 Eric Lander & Alondra Nelson, ICYMI:WIRED (Opinion): Americans Need a Bill of Rights for an AI-Enabled World (OSTP Blog, October 22, 2021), https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/

8 The White House, Join the Effort to Create a Bill of Rights for an Automated Society (Press Release, Nov. 10, 2021), https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/

on how to diagnose, treat, or predict the course of a patient's disease.[9] CDS tools are designed for use in clinical healthcare settings where patients' contact with the software is mediated by human actors. Its recommendations might be challenged and rejected (or accepted and implemented) by a clinician, genetic counselor, nurse, or other healthcare professional.

AI/ML CDS tools have distinct features that set them apart from large-scale data collection and processing by retailers, credit-scorers, social media providers, law enforcement, and other non-medical actors in modern "surveillance societies."[10] One distinct feature is that CDS software implicates domains of regulation for which longstanding norms of federalism allocate oversight responsibilities to both state and federal authorities (e.g., state medical practice regulators vs. federal medical product regulators).[11] Protecting the safety and civil rights of patients and others whose data is used in AI/ML CDS software requires a careful interplay of state, federal, and non-governmental authorities already involved with these matters.[12] More broadly, medical and non-medical AI differ in ways that may justify different civil rights protections, including for data privacy.[13] There is no harm in exceptionalism, as long as you can put your finger on what, precisely, warrants an exception. This article tries to do that for AI/ML CDS software.

For *non-medical* AI/ML tools, the United States has glaring gaps in privacy and other civil rights protections that are a worthy focus for OSTP's policymaking efforts. In clinical healthcare settings, however, the Privacy Rule is not 'broken' and does not need to be 'fixed,' at least not at the federal level.[14] The Privacy Rule was the product of careful consultations between federal and state privacy regulators to accommodate their joint roles in medical privacy.[15] The Privacy Rule's preemption provisions, like those of the HIPAA statute, grant the States power to improve its civil rights

---

9 *See, e.g.*, Clinical Decision Support, HealthIT.gov (Apr. 10, 2018), https://www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds [https://perma.cc/JWV8-YUGQ] (describing a range of tools that constitute CDS software). See also U.S. Food & Drug Admin., Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff (Dec. 2017) (discussing CDS software, which combines patient-specific information (such as a patient's test results or clinical history) with generally applicable medical knowledge (such as clinical practice guidelines, information from drug labeling, or insights gleaned from outcomes observed in other patients) to provide a healthcare professional with patient-specific recommendations about how to diagnose, treat, or prevent disease in clinical healthcare settings).

10 *See, e.g.,* DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE, 33-35, 114-18 (2001); FRANK PASQUALE, THE BLACK BOX SOCIETY (2015).

11 *See, e.g.*, Joel E. Hoffman, *Administrative Procedures of the Food and Drug Administration*, *in* 2 Fundamentals of Law and Regulation: An In-Depth Look at Therapeutic Products 159, 165-66 (David G. Adams *et al.* eds., 1997) (discussing the intense debate about federal power to regulate medical practice that preceded passage of the Food, Drug, and Cosmetic Act in the 1930s).

12 *See, e.g.,* American Medical Association, Confidentiality: Code of Medical Ethics Opinion 3.2.1 (undated) at https://www.ama-assn.org/delivering-care/ethics/confidentiality (exemplifying nongovernmental confidentiality norms established by professional societies and affecting the civil rights of persons whose data is used in AI/ML software).

13 *See infra* Part I.

14 *See* HIPAA Privacy Rule, 45 C.F.R. § 160.203(b) (allowing States to set more stringent privacy protections than the HIPAA Privacy Rule does).

15 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,485, 82,797-98 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164) (discussing, in the preamble to the original Privacy Rule, the role of state law in determining individual access to laboratory information and reluctance of federal regulators to preempt state medical privacy standards). *See generally* Barbara J. Evans, *The Genetic Information Nondiscrimination Act at Age 10: GINA's Controversial Assertion that Data Transparency Protects Privacy and Civil Rights*, 60 WILLIAM & MARY L. REV 2017, 2068 (2019) (summarizing consultations conducted under Exec. Order No. 13,132, 64 Fed. Reg. 43,255 (Aug. 4, 1999), addressing federalism, in which the states expressed deep concern about federal preemption of state medical privacy frameworks).

protections.[16] Additionally, the 21st Century Cures Act of 2016 tasked the U.S. Food and Drug Administration (FDA) with overseeing the safety of AI/ML CDS tools.[17] The FDA's proposed regulatory approach for CDS software would assess its performance using flows of real-world clinical health data, which the Privacy Rule enables.[18] A one-size-fits-all approach to medical and non-medical AI privacy might impede this data-driven safety oversight.

The Privacy Rule, like most 25-year-olds, is deeply misunderstood by boomer bioethicists, the postwar generation born between 1946 and 1964 that came of age as scholars in the 1970s and 1980s. The Privacy Rule laid a strong cornerstone for a clinical AI Bill of Rights, but only if policymakers, regulated institutions, and gatekeepers that control access to real-world clinical data understand its rationale and embrace the socially beneficial data practices it promotes.

I. COMPETING DATA ACQUISITION NORMS FOR AI/ML MEDICAL SOFTWARE

A. The Privacy Rule and its discontents

Since the 1970s, bioethicists have pressed for people to have a right of informed consent before their identifiable health information moves into secondary uses – that is, uses other than the one for which they intended the data.[19] Equivalent notice-and-consent norms are favored by the more recent "Information Privacy Law Project"[20] examining the ethics of data flows in the broader surveillance society where personal information is routinely collected, stored, and made visible to others and then algorithmically transformed "in the active production of categories, narratives, and norms" that can land us on no-fly lists, earn us a discount, tag us as risky or at-risk human beings, or cause a prospective employer to rule us out.[21] The phrase "de-identify or get consent" (DOGC) encapsulates what such norms typically require: get consent if the data are in a format that identifies the individual the data describe.

The Privacy Rule is a medical privacy law aimed at players in the chain of payments for clinical health care. It regulates "covered entities" – basically, private-sector actors that provide or finance clinical healthcare services (clinics, hospitals, and insurers), plus business associates that obtain identifiable data from them while supplying professional or informational services to them.[22] This leaves out many businesses commonly thought of as health-related, such as companies selling fitness trackers and consumer health applications, or pharmaceutical or medical device companies that sell medical products as opposed to medical services. The Privacy Rule governs what covered entities can

---

16 *See* 45 C.F.R. § 160.202-.203 (Privacy Rule preemption provisions); 42 U.S.C. § 1320d-7(b) (HIPAA statutory preemption provisions).

17 *See* 21st Century Cures Act, Pub. L. No. 114-255, § 3060(a), 130 Stat. 1033 (2016) (codified at 21 U.S.C.. § 360j(o)(1)(E)).

18 *See infra* Table 1, Norms 15, 16 and Part II.E, F.

19 See PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 280 (1977), *available at* https://www.epic.org/privacy/ppsc1977report/c13.htm (finding, in a study authorized under the Privacy Act of 1974 *see 5 U.S.C. § 552(a)(d)*, that health data were widely used without consent in medical research and public health studies during the 1970s, and recommending that it would be ethical to seek consent before such uses). For an example of a regulation implementing this view*, see, e.g.,* Federal Policy for the Protection of Human Subjects of Biomedical Research ("Common Rule"), 45 C.F.R. §§ 46.101–124.

20 *See, e.g.*, Neil Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006).

21 Julie Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 181-82, 186 (2008)

22 *See* 45 C.F.R. § 160.102 (2018) (providing that the HIPAA regulations, including the Privacy Rule, apply to healthcare providers such as physicians, clinics, hospitals, laboratories and various other entities, such as insurers, that transmit "any health information in electronic form in connection with a transaction covered by this subchapter [the Administrative Simplification provisions of HIPAA]" and to their business associates); *see also id.* § 160.103 (defining the terms "covered entity" and "business associate").

`

do with protected health information (PHI), which is a class of data, defined in the HIPAA statute, that the Privacy Rule protects.[23]

Bioethicists' major discontent with the Privacy Rule is that it is not a DOGC privacy scheme. The Privacy Rule allows covered entities to use or disclose PHI with individual authorization (HIPAA's name for consent) or if the data have been de-identified.[24] This lulls casual observers into thinking the Privacy Rule is a DOGC privacy scheme. Then comes the betrayal: the Privacy Rule goes on to list 25 additional ways patients' PHI can be shared, usually without consent and potentially in identifiable form (Table 1). "Even if the Privacy Rule *allows* nonconsensual access to data, is it *ethical* and is it *trustworthy*?" ethicists ask.

The Privacy Rule is what law scholar Martha Nissenbaum calls a contextual privacy scheme. It lists "informational norms" – a set of data flows considered appropriate and necessary in and around one specific context (in this case, clinical health care).[25] Information sharing that is appropriate in one context might be highly inappropriate in other contexts. Thus, inquiring about people's annual income is appropriate when they apply for a home loan, but not when asking them out on a first date.

When crafting the norms in Table 1, the U.S. Department of Health and Human Services (HHS) was "aware of the concerns of privacy and consumer advocates" about controlling access to their data, but HHS determined that "[t]he allowable disclosures and corresponding restrictions we recommend reflect a balancing of privacy and other social values.[26] The Privacy Rule was never all about your individual autonomy; it is about the contextual ends and values of clinical health care.[27] It is about making health care work and, I argue, about making healthcare work more equitably – something that, to date, American health care has failed to do.

---

23 *See* 45 C.F.R. § 160.103 (defining "protected health information" (the information that the HIPAA Privacy Rule protects) as "individually identifiable health information" and defining the term "health information" for purposes of the HIPAA Privacy Rule). *See* 42 U.S.C. § 1320d(4) (reflecting the original 1996 HIPAA statute's definition of "health information" as "any information, whether oral or recorded in any form or medium, that: (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual"). See also, Genetic Information Nondiscrimination Act of 2008 § 105(a), 42 U.S.C. § 1320d-9(a) (expanding the definition of "health information" that HIPAA protects to include genetic information). See also, 42 U.S.C. § 1320d-9(b)(1) (stating, in a new section introduced by GINA, that Congress deems "genetic information," as broadly defined by GINA at 42 U.S.C. § 300gg-91, to be health information, for purposes of making it subject to HIPAA's privacy protections).

24 *See* 45 C.F.R.§ 164.502(a)(1)(iv) (allowing PHI to be released with individual authorization); *id.* § 164.508 (describing requirements for a valid individual authorization, which is HIPAA's term for a consent). *See id* § 164.502(d) (allowing de-identified data to be used and disclosed without individual authorization).

25 *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); Adam Barth, Anupam Datta, John C. Mitchell & Helen Nissenbaum, *Privacy and Contextual Integrity: Framework and Applications*, 2006 PROCEEDINGS OF THE IEEE SYMPOSIUM ON SECURITY AND PRIVACY 184 – 98 (2006), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567438; Helen Nissenbaum, *Privacy as Conceptual Integrity*, 79 WASH. L. REV. 119 (2004).

26 *Confidentiality of Individually Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996*, U.S. DEP'T HEALTH & HUM. SERVS. § I.I (Sept. 11, 1997) [hereinafter HHS, 1997 Recommendations], https://aspe.hhs.gov/report/confidentiality-individually-identifiable-health-information [https://perma.cc/M9TK-YZQW].

27 *See* discussion *infra* Parts I.I – I.K.

`

Table 1. The Privacy Rule's 27 Norms Allowing PHI to be Used and Disclosed[28]

Can disclose or use data 1. with individual authorization 2. if deidentified a. safe-harbor deidentification b. statistical deidentification	**Fifteen norms allowing unconsented disclosure and use, subject to the minimum necessary standard*** 13. with waiver approved by IRB/privacy board 14. for payment and healthcare operations/QI 15. to public health authorities and their contractors 16. to FDA-regulated entities for activities that FDA *requires* them to do. 17. to health oversight agencies 18. limited data set subject to data use agreement 19. to people exposed to communicable disease 20. to employers for workplace safety/exposures 21. to facilitate dignified burial of the deceased 22. to facilitate organ transplants 23. for fundraising with an opt-out 24. for certain insurance underwriting purposes 25. to avert serious threats to health or safety 26. for special governmental functions (military) 27. for workers' compensation cases * **Minimum necessary disclosures can include identifiers if they are necessary to fulfill the purpose of the disclosure**
Norms on disclosures to patients/executors 3. MUST disclose designated record set to the individual upon request, under HIPAA's individual right of access to one's own data 4. Can disclose additional data to the individual 5. Disclosures to legal representative after death	
Seven norms allowing unconsented disclosure and use, not subject to minimum necessary standard but subject to alternative protections 6. to a healthcare provider for use in treating a patient – *any* patient 7. to HHS for regulatory compliance purposes 8. as required for HIPAA compliance 9. to agencies for detecting abuse and neglect 10. for judicial and regulatory proceedings 11. for law enforcement purposes 12. if required by law	

A second discontent is that the HIPAA statute defines PHI narrowly. It includes data related to people's health or to their health care if the information is "created or received by a health care provider."[29] That leaves out what might be termed "health-related information outside clinical contexts" (HIOCCs), such as data from personal fitness trackers, commercial ancestry genomic testing, or from AI tools lenders use to predict who is likely to live long enough to repay a loan. It

[28] *See* 45 C.F.R.§ 164.502(a)(1)(iv) *and see id.* § 164.508 (describing requirements for a valid authorization) [Norm 1]; *id.* §§ 164.502(d), 164.514(a) *and see id.* § 164.514(b)(1) (statistical de-identification), *id.* § 164.514(b)(2)(i) (safe-harbor de-identification) [Norm 2]; *id.* § 164.524 (providing an individual access right) and *id.* § 164.501 (defining the "designated record set" that is subject to mandatory disclosure to the individual or to a third party the individual specifies) [Norm 3]; *id.* §§ 164.502(a)(1), (b)(2)(ii) [Norm 4]; *id.* §§160.103, 164.502(f),(g)(1) [Norm 5]; *id.* § 164.502(a)(1)(ii) *and see* HHS, FAQ 512-Under the HIPAA Privacy Rule, may a health care provider disclose protected health information about an individual to another provider, when such information is requested for the treatment of a family member of the individual?, at https://www.hhs.gov/hipaa/for-professionals/faq/512/under-hipaa-may-a-health-care-provider-disclose-information-requested-for-treatment/index.html (clarifying that, except for psychotherapy notes, a HIPAA-covered doctor may disclose a patient's information to another doctor without individual authorization for use in treating "another patient" – not necessarily a family member of the person whose data is disclosed) [Norm 6]; *id.* § 164.502(b)(2)(iv) [Norm 7]; *id.* § 164.502(b)(2)(vi) [Norm 8]; *id.* § 164.512(c) [Norm 9]; *id.* § 164.512(e) [Norm 10]; *id.* § 164.512(f) [Norm 11]; *id.* § 164.512(a) Norm 12]; *id.* § 164.512(i) [Norm 13]; *id.* §§ 164.502(a)(1)(ii), 164.506. *But see* Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement (Notice of Proposed Rulemaking), 86 FED. REG. 6446 (January 21, 2021) (controversially proposing to exclude these disclosures from HIPAA's minimum necessary standard) [Norm 14]; *id.* § 164.512(b)(1)(i),(ii), 164.514(d)(3)(iii)(A), 164.514(h)(2)(ii),(iii) [Norm 15]; *id.* § 164.512(b)(iii) [Norm 16]; *id.* § 164.512(d) and see *id.* § 164.501 (defining oversight agencies) [Norm 17]; *id.* §§ 164.514(e)(3)(i), 164.514(e)(4) [Norm 18]; *id.* § 164.512(b)(iv) [Norm 19]; *id.* § 164.512(b)(v) [Norm 20]; *id.* § 164.512(g) [Norm 21]; *id.* § 164.512(h) [Norm 22]; *id.* § 164.514(f) [Norm 23]; *id.* § 164.514(g) [Norm 24]; *Id.* § 164.512(j) [Norm 25]; *id.* § 164.512(k); *id.* § 164.512(l) [Norm 27].

[29] *Supra* Note 23.

`

strikes many observers as crazy that HIPAA protects the inference that Sally is pregnant if it came from a test her clinician ordered, but not if a retailer's AI algorithm mined Sally's recent purchasing data and concluded she must be pregnant.[30] A contrarian view, explored here, is that this is not crazy and, in fact, is a sensible policy that is just poorly understood.[31]

A third discontent is the perception that Privacy Rule is weaker than the European Union's (EU) General Data Protection Regulation (GDPR),[32] often touted as the putative privacy *Ideal* to which the United States should aspire. In the clinical healthcare context where the Privacy Rule applies, it is in many respects stronger than GDPR. The Privacy Rule sets a federal floor of clinical data protection: states are free to set higher standards but cannot go lower.[33] In contrast, GDPR grants the 27 EU Member States leeway to go higher *or lower* than GDPR's baseline consent standard.[34] A 2021 report for the European Commission details the many ways Member States enable unconsented flows of health data.[35] In clinical healthcare contexts, many Member States allow unconsented data flows functionally equivalent to those in Table 1.[36] Where clinical data privacy is concerned, the perceived GDPR privacy *Ideal* exists only in the ill-informed American imagination.

B. Invidious discrimination in AI/ML CDS software

Law considers discrimination "invidious" when people are treated in damaging ways because of race, gender, or class, without a rational reason to do so (for example, there could be a good reason to disadvantage a historically privileged group to correct past injustices).[37] AI/ML CDS tools show great promise for improving health care but recent empirical studies reveal their ominous side: they can serve as instruments of invidious healthcare discrimination.[38]

Training datasets for AI/ML CDS tools tend to overrepresent men of European ancestry while underrepresenting members of other racial and ethnic groups and women.[39] Empirical studies of how

---

30 Charles Duhigg, *How Companies Learn Your Secrets*, THE NEW YORK TIMES MAGAZINE (Feb. 16, 2012).

31 *See* discussion *infra* Parts I.J - I.K.

32 European Union General Data Protection Regulation (Regulation (EU) 2016/679).

33 45 C.F.R. §§ 160.202-.203 (Privacy Rule preemption provisions).

34 *See* GDPR Art. 6 (requiring consent for processing of personal data *id. § 1(a)* but allowing unconsented processing for various purposes such as legal compliance, "to protect the vital interests of the data subject or another natural person," for tasks "carried out in the public interest" *see id. §§ 1(b)-(f)* and allowing Member States to specify provisions "to adapt the applications of the rules" in some of these circumstances). *See* GDPR Art. 9 (addressing the processing of "special categories of personal data," which include health data and requiring consent *id. § 2(a)* but allowing Member States to establish different conditions and safeguards for data used in "preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services" *id. § 2(h)* and for public health *id. §2(i)* and for public interest purposes including scientific research *id. §2(j)*. *See also* EU/GDPR Art. 89 (allowing Member State law to derogate from various rights provided by GDPR when those "rights are likely to render impossible or seriously impair the achievement" of various public-interest goals including scientific research).

35 European Commission, Director General of Health and Food Safety, Assessment of the EU Member States' rules on health data in the light of GDPR (Specific Contract No. SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03) (European Union, 2021).

36 *Id.*

37 *See* USLegal, *Invidious Discrimination Law and Legal Definition* at https://definitions.uslegal.com/i/invidious-discrimination/; Legal Information Institute, *Invidious discrimination* at https://www.law.cornell.edu/wex/invidious_discrimination#:~:text=Treating%20a%20class%20of%20persons,criminal%20law.

38 *See, e.g.,* U.S. GOV'T ACCOUNTABILITY OFF., ARTIFICIAL INTELLIGENCE IN HEALTH CARE: BENEFITS AND CHALLENGES OF TECHNOLOGIES TO AUGMENT PATIENT CARE 24 (GAO-21-7SP, November 2020).

39 *For concerns with racial biases in AI/ML datasets and algorithms, see, e.g.*, Adewole S. Adamson & Avery Smith, *Machine Learning and Health Care Disparities in Dermatology*, 154(11) JAMA DERMATOLOGY 1247 (2018); Ruha Benjamin, *Assessing Risk, Automating Racism*, 366(6464) SCIENCE 421-22 (2019); Ziad Obermeyer B. Powers, C. Vogeli & S.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Better Identity Coalition

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Comments to the White House Office of Science and Technology Policy (OSTP)

RFI on Public and Private Sector Uses of Biometric Technologies

January 2022

The Better Identity Coalition appreciates the opportunity to provide comments to the White House Office of Science and Technology Policy (OSTP) on its Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 27 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, telecommunications, technology, fintech, payments, and security.

Of note, the Coalition does not exist to advocate for the interests of vendors in the space, though about half of our members are vendors. Rather, our policy priorities are driven by firms that depend on digital identity solutions to run their businesses. Our members are united in their view that government is essential to the development and adoption of better identity and authentication solutions. First, because government policies can catalyze or inhibit innovation in digital identity. And second, because government – as the only authoritative issuer of identity in the United States – has an inherent role to play in the digital identity ecosystem.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In July of 2018, we published *Better Identity in America: A Blueprint for Policymakers*[1] – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity in the U.S.

At the core of our Policy Blueprint is the recognition that criminals and other adversaries have caught up with the systems America has used for remote identity proofing and verification, and that the security, privacy, and user experience challenges that this fact presents requires the use of newer and better technologies. Our Blueprint highlights why government – as the only authoritative issuer of identity – is in the single best position to address the challenges we have today and make identity better.

While biometrics are not specifically addressed in our Policy Blueprint, biometrics and other artificial intelligence (AI) enabled technologies are playing an increasing role in remote identity proofing and verification, as well as authentication. Understanding that this RFI is part of a broader OSTP effort to craft an "AI Bill of Rights" and consider what policies should apply to the use of AI, we think it is logical to look at biometrics as one of a number of AI-enabled technologies used in identity and authentication.

As we detail in our response, in many cases, these technologies are delivering great benefits – helping not only to deliver enhanced security and convenience, but also more equitable outcomes.

[1] See https://www.betteridentity.org/s/Better_Identity_Coalition-Blueprint-July-2018.pdf

That said, "many" is not "all," and there are some legitimate concerns around inappropriate uses of AI in identity, as well as questions as to the appropriate boundaries around where and how these technologies should be used. On balance, we believe the benefits exceed the harms today, but harms – both actual and potential – certainly exist. It is critical that any policy efforts are crafted in a way that maximizes potential benefits from AI in the use of identity solutions while minimizing the harms.

We have arranged our response in two sections: one that outlines our general policy recommendations, and a second that is a more in-depth discussion on how AI is being used in identity verification and authentication today. The latter addresses RFI Topics 1 and 5, while the policy recommendations address Topics 1, 2, 5, and 6.

I. Policy Recommendations

As OSTP considers the appropriate use of biometric technologies and other AI-enabled tools in identity verification and authentication, we offer eight key points:

1. AI technologies are an increasingly important tool in identity – particularly given the ongoing battle we are in against cybercriminals. These criminals are doubling or in some cases quintupling down on identity-centric attacks, putting the security and privacy of people's data and money at risk. The good guys need every tool in the toolbox to guard against these attacks.

   AI-enabled identity tools are emerging in the market, in part, to address some of the key challenges that NIST flagged in its Digital Identity Guidelines, when it stated:

   "Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.[2]"

   On that point, criminals themselves are starting to develop their own AI-powered tools to support cyber-attacks. While terrifying, this should not be surprising; the same technology innovations that can be used to protect us will also be exploited by adversaries to try to attack us. Our members are seeing this in the early stages with criminals and nation-states using AI-powered bots to launch automated password spray and credential stuffing attacks. Attackers are always innovating, and we should be preparing for them to be using AI against us in new and innovative ways.

2. To the point that there are policy concerns about the use of AI, the answer is not to ban its use but rather to identify the specific concerns and craft policies to address them. A

[2] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

blanket ban on certain technologies will almost certainly play into the hands of criminals and put consumers and businesses at great risk. Likewise, restrictions that are not narrowly tailored to address specific risks or harms may inadvertently preclude constructive applications of AI-powered identity tools. Finally, to the extent existing laws and policies on privacy, security, and human rights already regulate AI, any new AI policy or "AI Bill of Rights" should not contradict or duplicate this, but rather build upon existing legislation.

3. It is important that policymakers do not lose sight of the ways AI and ML can help with inclusion and equity. Financial services firms are already starting to use AI to enable new approaches to identity proofing that can help bring more services to the "credit invisible" – such as more easily auto-approving more people for loans – relative to legacy tools that don't use AI.

   While there are some concerns that algorithms used here might be biased – and that "putting the machines in charge" will lead to inequitable outcomes – most of what we have seen in the use of AI in these types of solutions is improving equity and inclusion. For example, if a bank is looking at credit report data for identity proofing, but a consumer has a thin file (as is common for young people, immigrants, and historically marginalized groups), some AI-enabled tools can be used to incorporate and analyze alternative data sources and approve applicants at a higher rate. Tools that leverage AI are often able to help fill in the "gaps" and provide an alternative path to approval. Likewise, if someone with a thin file has a driver's license, AI-enabled tools that validate whether an ID document is real or counterfeit – and use biometrics to analyze whether the selfie matches the photo on the ID – can be used to enable easy digital account opening.

4. An important part of issues surrounding the use of AI in identity verification is the fact that many of the technologies are opaque: despite the efficiency of many algorithms, it still difficult to explain their decisions to most people. Moreover, performance of what at first glance looks to be similar products may vary, with some products delivering results that are accurate and equitable, while others do not. We have seen a number of instances where unreliable products fail and then the entire industry is faced with allegations of "bias" – when the issue is not the industry but certain vendors, or how their technology is applied.

   These issues can be greatly mitigated by independent certification and testing programs that can evaluate vendor claims and validate what works, what does not, and how.

   There is good work underway here today in the identity sector: FIDO Alliance (an identity standards and certification body with both industry and government participation) has launched an initiative to create a new testing and certification program for remote ID proofing tools – creating a way to independently validate the

claims made by vendors and also determine whether there are any specific quirks or biases in a product or algorithm that may need to be addressed.[3] In addition, NIST has done some great work to help vendors and implementers address potential bias concerns in its recent draft Special Publication 1270, "A Proposal for Identifying and Managing Bias in Artificial Intelligence."[4]

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the Federal Deposit Insurance Corporation (FDIC) have also engaged on this front – on January 11, they announced a new Tech Sprint effort focused on measuring the effectiveness of digital identity proofing for financial services. In their announcement[5] they noted:

"Digital identity proofing is a foundational element to enable digital financial services to function properly. This element is challenged by the proliferation of compromised personally identifiable information (PII), the increasing use of synthetic identities, and the presence of multiple, varied approaches to identity proofing. Simultaneously, technological developments are enabling dynamic identity evidence such as state mobile driver's licenses (mDLs) or other identity credentials that are frequently updatable and interoperable, as well as behavioral analytics."

5. With regard to biometrics, all "face recognition technology" is not the same, both in terms of how the technology works, as well as the potential biases and risks. The technical and policy issues involved in terms of a 1:1, on-device match of a face on a smartphone, for example, are wildly different from applications of face recognition technology in surveillance applications; these applications do not even share most of the same technologies. Likewise, the issues involved with both of those applications are different from those involved with the use of face recognition technology in a controlled setting when someone is applying for a driver's license or passport, or processing through a border control checkpoint.

   We have seen a number of instances where the press or policymakers have inappropriately conflated issues tied to one application of face recognition with another – for example, suggesting that problems associated with surveillance applications mean that face recognition should not be used on someone's smartphone. It will be important for OSTP and other policymakers to ensure that any polices around the use of biometrics technology are appropriately targeted to specific applications, and the specific risks or harms associated with those applications.

6. Many of the concerns we are seeing about the use of biometrics and other AI-powered identity tools – and the policy proposals to address these concerns – are based on

[3] See https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/
[4] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270-draft.pdf
[5] See https://www.fdic.gov/fditech/techsprints/measuring-effectiveness.html

shortcoming on how certain products or technologies perform today in terms of accuracy or bias. However, technology is advancing rapidly, and we believe OSTP and other policymakers should be preparing for a future where some of these technologies are remarkably accurate. We are already seeing the use of next generation approaches to face liveness and face matching that do not measure refracted or reflected light, for example; this can help to address some of the accuracy struggles that earlier face biometric technologies had with some populations with darker skin.

Looking ahead 5-10 years, we believe the broader policy questions will center less around accuracy and more on the topic of "if, where, and how" AI-powered tools should or should not be used.

7. One way to explore the appropriate use of – and potential pitfalls with – AI-enabled identity tools in regulated industries is through the use of "regulatory sandboxes" established in partnership with the government. In the United Kingdom, for example, the Information Commissioner's Office (ICO) has used sandboxes as a way to conduct research on measuring and mitigating algorithmic bias facial recognition technology. The research included best practices in data labelling, performance measurement and optimum bias mitigation techniques, all in the wider context of ensuring protection of personal data.[6] The US, to date, has not embraced this sort of sandbox approach, but we believe it may be a promising way for government to partner with industry to address potential concerns about AI-enabled identity verification solutions.

8. The single best way to address concerns with regard to bias in AI being used in identity proofing tools is to pass the *Improving Digital Identity Act of 2021*.[7] In that every product using AI to try to determine identity is trying to "guess" what, in most cases, only the government really knows. There is no better way to address concerns about probabilistic systems run amuck than to enable new deterministic systems that rely on the actual source of identity in government. America is not going to truly solve identity proofing without the kinds of identity attribute validation services that the bill calls for.

   On this front, OSTP can help. The *Improving Digital Identity Act* is largely focused on directing the White House to establish and "Improving Digital Identity Task Force" to establish a government-wide effort to develop secure methods for Federal, state and local agencies to validate identity attributes to protect the privacy and security of individuals and support reliable, interoperable digital identity verification in the public and private sectors.

[6] For details on one vendor's work with the ICO, see https://ico.org.uk/media/fororganisations/documents/2618551/onfido-sandbox-report.pdf

[7] See https://www.congress.gov/bill/117th-congress/house-bill/4258

The idea behind these attribute validation services is simple: Governments should modernize legacy paper-based identity systems around a privacy-protecting, consumer-centric digital model that allows consumers to ask the agency that issued a credential to stand behind it in the online world – by validating the information from the credential. The Social Security Administration (SSA) and state governments – the latter in their role as issuers of driver's licenses – are the best positioned entities to offer these services to consumers.

While the White House could wait for Congress to direct it to establish this Task Force, a better choice would be for the White House to establish such a Task Force through executive action, such as an Executive Order.

By leading a drive in the White House to directly tackle digital identity challenges, OSTP can help develop new identity solutions that can address concerns about bias in AI-powered tools.

Note that this idea is not new: it was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity,[8] which, in response to the wave of attacks leveraging compromised identities, set a clear goal for the country:
"The Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021."

As a key element of this action item, the Commission stated:
"*The government should serve as a source to validate identity attributes to address online identity challenges."*

Per the report:
"The next Administration should create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online.

"As part of this effort, the interagency task force should be directed to incentivize states to participate. States—by issuing drivers' licenses, birth certificates, and other identity documents—are already playing a vital role in the identity ecosystem; notably, they provide the most widely used source of identity proofing for individuals. Collaboration is

[8] See Action Item 1.3 of the report. The full report is at:
https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

key. Industry and government each have much to gain from strengthened online identity proofing.

"The federal government should support and augment existing private-sector efforts by working with industry to set out rules of the road, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry attributes."

Government should act on this recommendation, with a particular focus on having the Federal government:

1) Establish the interagency task force called for by the Commission to identify how government agencies can offer these services. We believe OSTP can play a leadership role here, in conjunction with OMB and the National Security Council.

2) Lead development of a framework of standards and operating rules to make sure this is done in a secure, privacy-preserving way. NIST is in an ideal position to lead here.

3) Identify any legal or regulatory barriers that Federal or state agencies need to address to enable these services.

4) Fund work to get it started. We note that the GSA has for some time had an office in its Technology Transformation Service (TTS) to support better government-wide approaches to identity proofing. This office should be fully funded and empowered to drive action across government.

This idea was endorsed in policy in 2019 when the Office of Management and Budget (OMB) issued M-19-17,[9] which stated:
"Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing· events, as selected by OMB and permissible by law, shall establish privacy-enhanced data validation APIs for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent.

"These selected agencies, in coordination with OMB, shall establish standard processes and terms of use for public and private sector identity proofing services that want to consume the APIs."

Despite this OMB memo, little has taken place since then to advance these attribute validation initiatives. To the extent there are concerns about the overuse of AI in

[9] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

identity verification, this is the single most meaningful step the government could take to address these concerns.

II. How AI is being used in identity today

At a high level, there are two core challenges we are trying to solve in digital identity:

1. Identity Proofing and Verification – figuring out whether someone is who they claim to be at account opening. Exploiting weaknesses in our identity proofing infrastructure is what has allowed criminals to steal tens of billions of dollars from state unemployment insurance (UI) programs, as well as commercial firms in financial services, retail, and other sectors.[10]

2. Authentication – Once an account has been created, how do you create systems that can securely log customers in to or recover that account? This has become quite important in a world where passwords just don't cut it anymore, and cybercriminals are exploiting the weaknesses of passwords and other weak authentication tools to launch billions of attacks each day.

These challenges align with the way that NIST has broken down its guidance on digital identity. Identity Proofing and Verification is covered by NIST in SP 800-63A while Authentication is covered in SP 800-63B.[11]

On the Identity Proofing and Verification side, there are two primary use cases where AI and machine learning (ML) play an important role:

1. Remote ID proofing tools that ask a consumer to take a photo of their ID (such as a driver's license), as well as a selfie picture. In many of these products, AI/ML is used to help validate whether an ID document is real or counterfeit, as well as whether the selfie matches the photo on the ID. The role of AI/ML in these products is generally one where they "study" different documents and "learn" over time how to better tell a real driver's license or passport from a fake.

   In addition, AI/ML is also often used in the biometric aspects of the products, such as facial comparison and matching. Here, we are starting to see some firms address concerns about ways to spoof "liveness" of faces – as well as the accuracy and consistency of some weaker face matching algorithms – by shifting to algorithms based on 3D models of faces, rather than traditional 2D photos.

[10] The Federal Reserve has flagged that synthetic identity fraud is the fastest growing type of financial crime in the United States. See https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

[11] See https://pages.nist.gov/800-63-3/ for NIST's full Digital Identity Guidelines.

It is worth noting that Congress recognized the importance of these solutions in financial services in 2018 when it passed the *Economic Growth, Regulatory Relief, and Consumer Protection Act*.[12] Section 213 of that bill was called the *Making Online Banking Initiation Legal and Easy (MOBILE) Act*, and it preempted some state laws that prevented banks from scanning a driver's license to support mobile applications for new accounts.

Today, the types of solutions detailed in the MOBILE Act are widely used – but not all of them use AI, and performance of the products is inconsistent between vendors. In general, we have seen that the products that have an AI component are more accurate than those that do not.

As we noted earlier, one organization has launched an initiative to test and certify these solutions, with a focus on establishing performance criteria for these products and partnering with a number of independent testing labs to measure whether products meet these performance criteria.[13] To the extent that there is a concern that AI or ML technology used in some of these products might not measure up, new testing and certification programs like these will be a major asset. Many vendors are saying "trust us, our products work" – certification programs will verify that they actually do.

2. Data-centric approaches to ID proofing that improve accuracy through use of AI. Here, vendors in the space look at many different signals and data sources, and use AI to help predict over whether an applicant might be fraudulent or not – analyzing data and signals with algorithms that are constantly evolving and improving thanks to AI and that help companies root out fraud, including synthetic identity fraud, and make more accurate decisions.

   Signals and data sources may include what can be inferred about a device being used to apply for an account, or the way a user interacts with that device as they enter their information digitally. Examining a wider set of signals and data sources provides a multi-dimensional view of identity for enriched verification, and simultaneously allows vendors and implementers to identify patterns of repeated identity fraud across government agencies and the private sector driven by sophisticated crime rings. Given that it is these crime rings that were at the heart of much of staggering identity fraud losses in the past year,[14] this is an increasingly important use of AI.

   Overall, many of our members in the financial services space report that without AI/ML and risk-based models it would be impossible to approve as many applications for financial services or catch as much fraud.

[12] See Public Law 115-174

[13] See https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/

[14] An excellent summary of losses to government agencies was conducted by the Pandemic Response Accountability Committee (PRAC) https://www.pandemicoversight.gov/our-mission/identity-theft-in-pandemic-benefits-programs

On the Authentication side, AI and ML also play an important role as part of "authentication analytics" solutions that look at dozens of different data points and signals about how an individual is 1) trying to authenticate or 2) interacting with a device or application after initial authentication. These include both "behavioral biometrics" tools as well as tools that look at other data points.

AI has become increasingly important as adversaries focus on compromising authentication credentials to execute cyber attacks.[15]

Here, we are seeing firms in financial services and other sectors use tools that look at data such as behavior, location, typing pattern, access requests (i.e., a record of trying to get to something they should not have access to), etc. The tools then study all these elements and then use AI to make a prediction as to whether anything seems "off" or shows a sign of account or device compromise.

By pairing more traditional authentication with analytics solutions that use AI to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords and blocking credential-focused cyber-attacks.

The emergence of reliable authentication analytics tools is contributing to the rise of a new model for authentication called "continuous, risk-based authentication." Here a traditional authentication factor like a password or MFA is paired with analytics tools that analyze different signals. Some might automatically remediate a sign of fraud by refusing authentication, in other cases it might trigger a signal that is then used to ask a user for additional factors of authentication. To be clear, not all of these tools use AI, but many do.[16]

As major banks and cloud providers see tens or hundreds of millions of fraudulent attacks each day on their login systems, AI has emerged as an essential tool to detect and block them.

We greatly appreciate OSTP's willingness to consider our comments and suggestions and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at [redacted] or [redacted].

[15] The Cybersecurity and Infrastructure Security Agency (CISA) at DHS has flagged these concerns multiple times (see https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-268a) and the White House has made stopping attacks on compromised credentials a centerpiece of its new Federal Zero Trust Strategy (see https://zerotrust.cyber.gov/federal-zero-trust-strategy/).

[16] This model of "continuous authentication" was highlighted in a paper last year published by the Health-ISAC. https://h-isac.org/wp-content/uploads/2021/02/H-ISAC_All-About-Authentication-White-Paper.pdf

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Bipartisan Policy Center

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Bipartisan Policy Center Response to OSTP's RFI on Public and Private Sector Uses of Biometric Technologies

Introduction

The Bipartisan Policy Center (BPC) is committed to developing viable, consensus-driven solutions to improve public and private sector use of biometric technologies. We appreciate the Office of Science and Technology Policy's (OSTP) invitation to provide information about the use of these technologies and impacted stakeholders and efforts to develop a bill of rights for an automated society. BPC works with a wide range of stakeholders from government, academia, industry, and civil society to develop recommendations on privacy issues encompassing biometric privacy and is pleased to share our expertise and research in the comments below.

Much of our response for this RFI reiterates critical points made in published research papers and fact sheets to supplement our ongoing work in this space. We encourage Congress to provide unique attention to high-stakes privacy issues concerning biometric information. Congress must base decisions on regulating or providing safeguards around sensitive information on a cooperative and multi-stakeholder approach.

We look forward to OSTP's continued undertaking of similar efforts to address these issues.

Overview: The purpose of this RFI is to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation. OSTP encourages input on both public and private sector use cases.

Detailed Response

1. *Descriptions of use of biometric information for recognition and inference:* Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

The collection, storage, and use of biometric information has grown over the years and will continue to grow as IT administrators seek to secure and authenticate users. Biometric information is proliferating workplaces, government agencies, and everyday life. Without regulation or guidance, companies and individuals are almost entirely determining how to deploy new technologies appropriately. We've identified a few of the uses of biometric systems by employers and government agencies.

In the workplace: Biometric authentication and identification technologies have been deployed in workplaces for many years. Many older systems in the workplace include biometric time tracking devices and authentication tools such as fingerprint or face-scanning technology to access secure work devices or clock in for a shift. In many cases, fingerprint readers have replaced the "punch card" for many hourly work environments. These technologies can be scaled up or down according to employers' surveillance preferences. For example, clocking in and out of a shift in a warehouse using your fingerprint represents a small biometric footprint. At many retailer fulfillment centers, employees are tracked using facial recognition throughout their shift, representing a large biometric footprint. This includes physical tracking to ensure that workers are following safety rules, monitoring their activities on the warehouse floor, and other applications.

More modern biometric uses in the workplace include things like tracking eye movements and facial expressions through a webcam to ensure a workers' attention is staying on task, and sentiment analysis to gauge the mood of workers. Non-traditional use of biometrics in the workplace includes data collected through health tracking devices that track things such as location, heart rate, gait, or other physical attributes. This type of data collection has only increased as remote work environments become more popular.

Government use: Biometric data collection in the government sector is prolific, and there are many examples of government agencies and law enforcement's collection and use of biometric information. Similarly to the use of biometric identifiers in the workplace, a few departments detect their employees' identities using biometric technology. The Defense Department and Air Force use biometric recognition technology for entry into secure areas.

Several government agencies are expanding their use of biometric data. The U.S. Customs and Border Protection (CBP) Agency Global Entry program, for example, uses biometric identifiers in several ways. Originally used as facial recognition technology upon EXIT, CBP's biometric scanning procedures have expanded to facial scans to verify passport and VISA images and other technology to expedite clearance for travelers arriving in the United States. Some land borders ports also use biometric devices and algorithms to verify travelers. CBP's responsibility to confirm the identity of international travelers through a facial recognition process is balanced by its commitment to privacy by limiting the amount of personally identifiable information used and the deletion of photos of U.S. citizens and non-citizens. Like any successful implementation of biometric technology, the operation of an efficient commercial travel process will require additional assessment and gradual rollout to wherein early experiences inform further deployment. The NSA deployed technology that can identify people by the sound of their voices as early as 2006. The system takes samples to make a "voiceprint" then compares other recordings to the voiceprint to identify a match. The existence of the system was revealed when Edward Snowden released classified documents to the public.

Federal law enforcement captures individuals' biometric information through fingerprints, and images and videos that capture a person's facial features such as mugshot photos and driver's license photos. According to the FBI's Privacy Impact Assessment, information collected for the biometric identity and criminal history system is protected through several measures, such as limited retention time and strong security features to lower risks to individuals' privacy.

Some local governments have also benefited from the installation of biometric identifiable technology. Cities from Atlanta to Portland installed thousands of cameras that can combine with facial recognition technology particularly for criminal investigations. This technology has come under scrutiny by other cities that have recently restricted the use of facial recognition technology in public spaces. For example, in 2019, San Francisco passed a law to ban the use of facial recognition software by the police and other agencies.

In health care: Biometric technology can substantially improve capabilities in the health care industry and improve staff and patient safety. Patients' personal health identifiers are generally protected under federal health privacy law, HIPAA, as discussed in a later section. For authentication purposes, biometric identifiers can be used to protect patients' sensitive information and reduce registration times. Biometric technology is also a promising tool for improved accuracy and efficiency of electronic medical records (EMR) and health records (EHR). Biometric technology is poised to grow in one of the largest sectors in the US, however, lawmakers should consider how to streamline transitions in the health care system and how to ensure patients' safety is protected.

Congress must learn from successful implementation as well as mismanagement and mistakes identified in this response and by other RFI responses to better protect Americans' sensitive and critical information.

2. *Procedures for and results of data-driven and scientific validation of biometric technologies*: Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

As part of OSTP's ongoing research on the validation of biometric technologies, special consideration should be made to review the work of Dr. Anil Jain and his research on relevant sample sizes and processes for authentication. Dr. Maruf Monwar and Marina Gavirlova have also produced research on multimodal biometric systems.

To gain greater expertise, we suggest the National Center for Biotechnology Information at the NIH as a valuable resource on the topic. NIST also has several resources, including a summary of a workshop conducted in 2015 to improve datasets standards for use in biometrics.

3. *Security considerations associated with a particular biometric technology.* Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.

Federal legal requirements outlined in the Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) under which individuals' biometric information is broadly protected, help to protect individuals' information. HIPAA applies safeguards for patients' sensitive health information and require covered entities to notify individuals in the event of a breach of personal health information, including biometric identifiers. FERPA similarly requires parental consent before a student's biometric records can be released.

Federal agencies are uniquely required to abide by the Privacy Act of 1974, also known as the "Code of Fair Information Practices," which intends to "balance the government's need to maintain information about individuals with the right of individuals to be protected against unwarranted invasion of their privacy and to limit the unnecessary collection of information about individuals." This is essential in address privacy violations, such as the cybersecirty incident during a 2019 biometric pilot program by CBP where thousands of traveler's Personally Identifiable Information (PII) was was improperly used.

Some state and local city regulations and corporate policies have added much needed layers of protection against security risks and privacy concerns of biometric technology. Stakeholders' sensitive information or personally identifying information is safeguarded under these laws, and incidences such as data breaches are more likely to be reported and responded to appropriately.

The Illinois Biometric Information Privacy Act (BIPA) is an example of a local state law that aims to protect individuals from potential exploitations or misuse of their biometric information. BIPA requires employers to publish their intended use of biometric information, and how it will be collected and stored and receive written consent from their employees in the state to use and collect biometric information. The law also has guidelines for permanently deleting and destroying data that is no longer in use to protect individuals from potential future data breaches. Further, the law requires businesses to provide notice in the case of a data breach. While this is

not customary, it is vital to ensure people are informed about the security of their biometric identifiers. While law intends to benefit citizens, the cost of implementing BIPA technology standards and the repercussions for non-compliance drives businesses outside of Illinois' state lines, which could ensue costs on the economy and people's welfare.

Some systems implement their own security measures such as only storing the data on the device, and never capturing that data outside of the device's operating system.

4. *Exhibited and potential harms of a particular biometric technology*: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

The negative impacts caused by leaked, stolen, or misused biometric information are far greater than harms caused by the same misuses of other data. Biometric data is unique and cannot be altered in the case of a data breach. High-stakes biometric information must be treated differently than other data, and Congress should make policy decisions particularly to protect users from harms. We've identified some of the harms caused by biometric capturing technology below. However, our response summarizes only the most serious harms we have found, and we recommend OSTP consider all harms identified by respondents to this RFI.

Data that is captured by biometric devices and systems are then processed and analyzed using AI or machine learning. The validity of information generated by AI or machine learning systems can be questioned due to cognitive biases from the AI developers that can influence the models and training data sets. This can lead to bias being hardcoded into the algorithm. We applaud NIST's recent work to provide a framework to address bias and fairness issues, but more work is necessary to specifically address bias in biometric data-enabled technology.

Disparities in effectiveness of the system negatively affect minority stakeholders. Facial recognition systems can fail when encountering individuals with dark skin, causing harm such as false identifications, bias in algorithms, or bias in error rates.

Harms can also be caused by a lack of transparency about the use of biometric data. This can happen when consent is granted for use of biometrics for

identification or access; that data is then used in addition or instead for surveillance or tracking of an individual. Other transparency concerns arise when consent is not deliberately granted, for example, when social media platforms use facial recognition technology to identify and make public identification of people in the backgrounds of pictures.

Unfortunately, Americans have also already encountered malicious actors; Russian-owned FaceApp used deceptive terms of service agreements – an application that encouraged users to upload photos of themselves so the app could manipulate an image to make the subject look older. People raised privacy concerns as they discovered the images were uploading to servers where AI algorithms ran against them. Users gave away control or rights over their images, and therefore their biometric information.

5. *Exhibited and potential benefits of a particular biometric technology*: Consider benefits including, but not limited to: Benefits arising from use in a specific domain (absolute benefit); benefits arising from using a specific modality of biometric technology (or combination thereof) compared to other modalities in a specific domain (relative benefit); and/or benefits arising from cost, consistency, and reliability improvements. Information on evidence of benefit (in the case of an exhibited benefit) or projections, research or relevant historical evidence (in the case of potential benefit) is also welcome.

There are many advantages to deploying biometric devices, such as increased security and privacy and greater efficiency for validation purposes. Voice recognition tools are also adapting to help decipher demands for speech command systems to improve user experiences.

The use of biometric systems in airports has helped to reduce the time it takes for passengers to get checked in. For example, TSA Precheck collects biometric data upon enrollment for background checks. However, biometrics are not regularly thereafter confirmed by members when encountering TSA security at airports. In addition, the U.S. Customs and Border Protection agency uses the Global Entry systems to allow expedited clearance for pre-approved, low-risk travelers upon arrival in the United States. Global Entry is a voluntary program that uses facial recognition and fingerprint data for identification and authentication. In exchange, travelers gain access to an expedited screening process when entering the United States. The TSA and CBP are also testing the use of facial recognition for a joint CBP/TSA Trusted Traveler pilot program.

Companies have deployed biometric time clocks to track employees' hours using a unique biometric identifier such as a fingerprint to allow employees to clock in and out more efficiently. These systems also cut down on employees entering fraudulent time worked information and free the employers from manually tracking and verifying employees' attendance. The use of biometric verification also prohibits coworkers from clocking in or out someone other than themselves.

6. *Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case:*

After assessing five state privacy laws pertaining to the collection and use of biometric information in Illinois, Texas, Washington, California, and New York, BPC created a white paper to understand sensitive information is collected, used, safeguarded, destroyed, and regulated in each state. We encourage OSTP to consider the benefits as well as the shortcomings of these five state laws when shaping future regulations and recommendations on biometric information. In each of the subsections of this response, we will report findings from this analysis and the application of these practices for different stakeholders.

Information regarding:

a. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;

Some states, including the five mentioned above, have introduced or passed legislation to protect people's biometric data, and many businesses have adopted their own policies to comply. The intention of each policy is to mitigate the risks of biometric technologies on consumers and other stakeholders. As some of the first laws to regulate biometric information in the United States, these laws have great influence over business practices and consumer awareness of the handling of biometric information. Using the infographic made public here on BPC's website, stakeholders can better assess requirements and how they overlap or differ from state to state.

Making this information more accessible will allow stakeholders to comply with laws and regulations more easily across the country. It will also improve informed consent of the use of biometric technologies, give consumers access to information about their rights, and facilitate the appropriate use of biometric technology.

b. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

The lack of federal guidance on policies surrounding issues raised in this RFI has left citizens inadequately protected, and corporations forced to navigate state-by-state regulations. As referenced in our papers, a good first step may be establishing a biometric data privacy framework using the NIST Privacy Framework as a guide to building standards.

c. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;

The five laws we reviewed reveal distinct practices regarding biometric data collection, use, and storage. Four of the five states require businesses or other entities to inform people of the use of biometric identifying technology. Two states even require affirmative consent prior to the collection, storage, or use of someone's biometric information. This informed use is important so consumers can make informed decisions about their sensitive data.

Despite varied practices regarding data collection, all five states oblige businesses or people to destroy or delete biometric data within a certain time frame. Restricting the retention of sensitive data limits its vulnerability to data breaches and other misuses.

d. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;

These state laws have implemented safeguards for unapproved use beyond requirements to delete or destroy data. All five laws we reviewed require entities capturing biometric information to protect biometric information in a more protective manner than other, less sensitive data.

h. Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.

In general, transparency of information is essential to further inform individuals' decisions regarding the utilization of biometric technology. In some instances, entities collecting biometric information are required by law to notify users in case of a data breach, sometimes requiring the details of the data that was breached. Some state laws we reviewed also allow a private right of action so people harmed by violations of the law have an opportunity to collect for their damages. Damages may result in anywhere from $100 to $25,000.

Conclusion

OSTP will play a vital role in defining the future of AI-enabled biometric technologies. BPC's response to the RFI provides recommendations developed from collaboration with industry, academia, government, and civil society on these topics and should be considered in combination with the other responses that have been submitted. We strongly recommend that policy considerations constantly be reviewed and modernized as the technology continues to develop. BPC looks forward to continued work with OSTP to collaborate on these concepts.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Brandon L. Garrett and
Cynthia Rudin

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

AI and Criminal Procedure Rights

Brandon L. Garrett[*] and Cynthia Rudin[**]

Introduction

Today, as data-driven technologies have been implemented across a wide range of human activities, new warnings have been issued from a wide range of sources, academic, public policy, and government, regarding the dangers posed by artificial intelligence to society, democracy, and individual rights. The Federal Trade Commission (FTC) has described more detailed views concerning unfair and deceptive practices that rely on AI and impact consumers, and the FTC has taken action against a series of corporations regarding different types of algorithms.[1] Several pieces of legislation that would regulate algorithms have been introduced in Congress, none of which has been enacted, but meanwhile, states have been active in considering and also adopting legislation regarding uses of AI. The White House Office of Science and Technology Policy (OSTP) has called for an "AI Bill of Rights."[2]

Our statement responds to the OSTP call for submissions on that topic and we focus specifically on uses of AI in the criminal system.[3] We write to reflect our own views as researchers, respectively, in law, scientific evidence, and constitutional law more broadly, and in artificial intelligence, machine learning, and computer science more broadly. We write to emphasize two basic points, that (1) artificial intelligence (AI) need not be black box and non-transparent in the ways in which it affects criminal procedure rights, and in fact, nothing will be lost by requiring such transparency through regulation; and (2) while more rights protections and regulations should be considered, far more can and should be done to apply and robustly protect the existing Bill of Rights in the U.S. Constitution as it should apply to uses by government of AI in the criminal system, particularly when AI is used to provide evidence regarding criminal defendants.

First, particularly in criminal cases in which life and liberty may be at stake, there should be a presumption that uses of AI directed towards providing evidence against criminal defendants, including by the federal government, such be fully interpretable and transparent. The burden to justify "black box" uses of AI in court should be a high one, given our commitment to public

* L. Neil Williams, Jr. Professor of Law, Duke University School of Law and Director, Wilson Center for Science and Justice.

* Professor of Computer Science, Electrical and Computer Engineering, Statistical Science, Mathematics, and Biostatistics & Bioinformatics, Duke University.

The views expressed here reflect only those of the authors and not those of any institution to which they belong, such as Duke University.

[1] Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, Federal Trade Commission, April 19, 2021, at https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (providing an overview of relevant legal rules, including the FTC Act, prior FTC approaches and noting recent enforcement actions).

[2] Eric Lander and Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, Wired, October 8, 2021.

[3] Federal Register, Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (2021), https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.

judicial proceedings and defense rights of access. There is no evidence that performance and efficiency depend on keeping the operation of AI secret from the public and unintelligible to users. That fundamental point, that AI can and should be open, for inspection, vetting, and explanation, is a simple one and it can be more forcefully insisted on at the federal level.

Second, we do not disagree that existing rights need to be at times reinterpreted for the AI era. However, we want to be sure that there is also a strong commitment to enforce existing constitutional criminal procedure rights, particularly given how difficult it is to amend the U.S. Constitution, but also given the unfortunate reality that those constitutional rights have been unevenly enforced in criminal cases, given the challenges that largely indigent defendants face in obtaining adequate discovery and the pressures to plead guilty and waive trial rights. The federal government in particular, should lead by example, it its use of AI technologies, to vigorously protect constitutional rights of criminal defendants. In some settings, the federal government has already done so, but in others, the federal government has not taken individual rights concerns sufficiently seriously. We discuss below uses of AI that do not implicate constitutional criminal procedure rights to the same degree, and also highlight how crucial it is to focus on the uses to which AI is put during criminal investigations.

I. What is AI?

"Artificial intelligence" simply means that machines perform tasks that are typically performed by humans. Machine learning is a subfield of AI, and it heavily overlaps with predictive statistics. We should think of machine learning as a kind of pattern-mining, where algorithms are looking for patterns in data that can be useful. The data is supplied to the machine, which relies on past patterns to develop methods for making recommendations for what to do next. For instance, when predicting whether someone might have a drug overdose, patterns in their medical record and twitter feed, as well as those of others, might help us predict that outcome. These patterns can help human decision makers because no human can calculate patterns from large databases in their heads. Individual people may in fact be biased or place undue weight on information that is not particularly predictive. If we want humans to make better data-driven decisions, machine learning can help with that.

Simply put, machine learning methods can extract patterns from large databases that humans cannot. However, humans have a broader systems-level way of thinking about problems that is absent in AI.

The usefulness of AI as a tool in part depends on what data we feed to it. Just like a saw may perform irregularly if we feed it rotten wood, AI will perform poorly if we supply it with incomplete or irrelevant or biased data. If in the past, police often decided to arrest people simply based on their race, then relying on that policing data, AI will predict future arrests based on those same baked-in prejudices. If wealthier people have more access to certain medical services, then AI may recommend that medical support based on their past usage, and ignore others who may be in greater need of care.

II. Black Box Models Are *Not* More Accurate Than Interpretable "Glass Box" Models

First, what is black box AI? A black box predictive model is a formula that is too complicated for any human to understand or it is deemed by the designer to be proprietary, which means no one can understand its inner workings, because those inner workings are not shared or are not designed to be share-able. These models can cause problems for high stakes decisions like criminal risk scoring, where someone could get denied parole and they and their defense lawyer, the parole officers, and the public, are not able to figure out why the person did or did not get a high-risk score.

There is a common misconception that black box AI must be more accurate than any model a human could understand. That is just not true.[4]Models that are interpretable to humans can perform just as well as models that are not. This has been shown to be true across fields, including computer vision.[5] And recidivism risk scoring.[6] The ways in which AI affects rights and interests need not be hidden or secret. AI need not be a black box to attain the accuracy of a black box.

In fact, Black Box AI tends to lead to less accurate decision-making, because such models are harder to troubleshoot and use in practice. Typographical errors in the input to black box recidivism prediction models has led to catastrophic errors in decision making, deeply affecting people's lives.[7] This type of poor decision-making is a direct result of unnecessary secrecy, weighted in favor of companies that sell black box models to the justice system, rather than weighted towards those individuals in the justice system subjected to the decisions made from these models.

III. What Constitutional Criminal Procedure Rights are Implicated?

We now have far greater appreciation for the fact that AI can affect people's lives in all sorts of important ways. These include applications in our criminal system. AI is already used in a host of criminal investigation, pretrial, and sentencing-related settings. For example, algorithms are used for risk scoring, in order to predict the risk that someone will commit a crime if they are released on bail, or given parole. Many states mandate that risk scores be used in various decisions, always to inform a judicial or other officials' discretion, to be sure (and there are real questions concerning variability with which judges and others to incorporate quantitative information into their decision-making). Another high-profile example is the use of facial recognition technology as a forensic tool and for surveillance.

We emphasize throughout that the particular use of AI is important and can greatly alter the accuracy, privacy, and fairness interests at stake, as well as the fair trial rights involved. Thus, using AI to search for a missing person feared to have been kidnapped raises far fewer questions

---

[4] Cynthia Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and use Interpretable Models Instead*, Nature Machine Intelligence, 2019.
[5] Chaofan Chen, Oscar Li, Chaofan Tao, Alina Barnett, Jonathan Su, Cynthia Rudin, *This Looks Like That: Deep Learning for Interpretable Image Recognition*, NeurIPS, 2019.
[6] Jiaming Zeng, Berk Ustun, and Cynthia Rudin, *Interpretable Classification Models for Recidivism Prediction*, Journal of the Royal Statistical Society, 2017.
[7] Cynthia Rudin, Caroline Wang and Beau Coker*, The Age of Secrecy and Unfairness in Recidivism Prediction*, Harvard Data Science Review, 2020.

than using AI to identify a culprit from a surveillance video. Any use of AI that results in evidence introduced during a criminal investigation, or in court, will generally raise far more constitutional concerns than a use of AI that is not used to prosecute a person.

A. Fair Trial Rights

A range of constitutional rights apply to protect individuals against deprivations of important interest through government action, and a range of rights are focused on the rights of individuals during criminal investigations and criminal adjudication. The most expansive constitutional provision implicated by uses of AI in criminal investigations strikes at the fundamentals of government action: the Due Process Clauses of the Fifth and Fourteenth Amendments.[8] The federal government can ensure that no federal agency uses AI in a way that arbitrarily deprives persons of the rights during criminal investigations and adjudication. Simply put, we should look more closely at uses of AI that might result in evidence used to arrest a person and that might result in evidence used in court during a criminal case. We do not focus here on Fourth Amendment privacy rights relating to searches and seizures, although similar principles should apply. We focus here on due process and related rights: on uses of AI to generate evidence that could be used in court in a criminal case, to determine bail, to convict a person, or to impose a sentence.

The due process protections in criminal cases include assurances that all material and exculpatory evidence of innocence be disclosed to criminal defendants.[9] Defendants have a right to effective assistance of counsel; defense counsel, in our view, cannot meaningfully defend a person without information about what AI evidence is bring introduced in a case.[10] The Equal Protection Clause protects against purposeful discrimination of protected groups, including based on race. The federal government can insist that AI be carefully vetted to assure against discriminatory impacts on minority groups. Further authority under civil rights legislation can assure that federal grant recipients do the same. Further, the defense cannot meaningfully defend a person without knowing whether the AI formula was calculated without error; in the case of risk scoring, there has been much evidence of typographical errors or other types of data errors influencing the scores[11]. In some cases, it has been reported that the wrong score is being computed for all defendants: in the case of COMPAS in Broward County, FL, it was reported that the wrong scoring model had been used for years: the COMPAS parole score was used to determine pretrial risk, rather than the COMPAS pretrial score that was designed for this purpose.[12,13]

---

[8] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 10-16 (2014).

[9] *Brady v. Maryland,* 373 U.S. 83 (1963). Regarding questions whether machine-generated results are themselves "testimonial" under the Sixth Amendment Confrontation Clause, *see* Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 2039 (2017).

[10] Strickland v. Washington, 466 U.S. 668 (1984).

[11] Cynthia Rudin, Caroline Wang and Beau Coker*, The Age of Secrecy and Unfairness in Recidivism Prediction*, Harvard Data Science Review, 2020.

[12] How We Analyzed the COMPAS Recidivism Algorithm, Propublica, Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, May 23, 2016

[13] Jackson, E., & Mendoza, C. (2020). Setting the Record Straight: What the COMPAS Core Risk and Need Assessment Is and Is Not. Harvard Data Science Review, 2(1). https://doi.org/10.1162/99608f92.1b3dadaa

We emphasize the importance of affirmatively adopting policies to ensure that these constitutional rights are protected, however, because in practice, many are not meaningfully enforced. Discovery in criminal cases is typically quite limited, making it difficult for defendants to be aware that there is even an issue that exculpatory evidence may not have been disclosed. A criminal defendant may not be aware that AI was used to generate leads or evidence. Nor are evidentiary rights clearly defined in pretrial settings, or in sentencing proceedings in many jurisdictions. In general, expert evidence admissibility decisions have also been quite deferential in criminal cases; the National Academy of Sciences itself has explained that scientific safeguards must be put into place by government, given the limited ability of defendants to challenge even wholly unscientific expert evidence in criminal cases.[14] That report highlighted how courts have routinely found admissible a range of forensic evidence of reliability that simply has not been established, where: "With the exception of nuclear DNA analysis, however, no forensic method has been rigorously shown to have the capacity to consistently, and with a high degree of certainty, demonstrate a connection between evidence and a specific individual or source."[15] Further, a criminal defendant, if indigent, may often be denied funds to retain an expert to examine AI technology used by a prosecution expert.[16] The defendant may have no way to independently verify the work done, using AI, by government investigators.

Courts have tended to narrowly view defense requests for discovery regarding evidentiary uses of AI, as well as forensic evidence more broadly, in criminal cases. They have tended to more expansively view discovery requests only when errors have come to light and the judges have realized that there were important reasons why that evidence could have resulted in exculpatory information. Often those revelations occur years after a conviction and when it is too late to adequately provide relief. [17] Further, typographical errors or other data errors that could occur in a defendant's record could easily influence a proprietary risk score calculation without detection, and, as we will discuss shortly, courts have upheld the rights of companies to protect such formulas.[18]

B. Examples from Criminal Law

We know that humans can be biased, too punitive, too lenient, or inconsistent, and AI has the potential, if used consistent with principles of transparency, interpretability, and fairness, to improve on existing outcomes. In some settings, AI has the potential to better protect people's rights. For example, judicial officers for decades have often followed cash-bail schedules (short cheat sheets, basically) quite robotically. If the person is arrested for a given charge, then bail is set at some cash level, say $2,000 or $10,000, if the judge mechanically follows the schedule. The person's individual situation does not matter, apart from the arrest charges. The resulting jail

[14] *See* Comm. on Identifying the Needs of the Forensic Sci. Cmty. & Nat'l Res. Council, *Strengthening Forensic Science in the United States: A Path Forward* 87 (2009) [hereinafter NAS Report]; Peter J. Neufeld, *The (Near) Irrelevance of Daubert to Criminal Justice: And Some Suggestions for Reform*, 95 AM. J. PUB. HEALTH S107, S110 (2005).
[15] NAS Report, supra, at 7.
[16] *See* Paul C. Giannelli & Sarah Antonucci, *Forensic Experts and Ineffective Assistance of Counsel,* 48 No. 6 CRIM L. BULLETIN 8 (2012).
[17] NAS Report, supra, at 44-45 (describing audits and quality control failures at labs around the country).
[18] Rebecca Wexler. *When a Computer Program Keeps You in Jail*, N.Y. Times, June 13, 2017.

detentions are often wholly unnecessary and even counterproductive regarding public safety (pretrial detention can be crimogenic).[19] We need to give judges better tools to make these decisions. So far, risk scoring has been used, although not always carefully considered by judges. AI has the potential at least, to introduce better approaches.

The black box problem in AI has become pressing in the area of risk assessment, however, as entire judicial systems have risk assessment schemes, but often without disclosing how they were created or what their basis was. While the types of information used in a risk tool may be made public, often the underlying methods, validation data, and studies are not. Most crucially, sometimes the assumptions behind how a person's a level of risk gets categorized as "high" or "low" are not explained or justified. Concerns regarding transparency, interpretability, and fairness persist in those settings.

The most prominent legal challenge to a black box risk assessment program was brought in Wisconsin, where a defendant argued that it violated his due process and equal protection rights to base his sentence on an algorithm, marketed by a private company (called Northpointe), whose operation and validating information was not disclosed to him. In the *State v. Loomis* case, the Wisconsin Supreme Court dismissed these due process claims, emphasizing that judges have discretion when they consider the risk instrument.[20] The Court did say that sentencing judges must be given written warnings about the risk tool, including cautioning judges that it relies on group data; those warnings do not open the black box in any way, however, or give judges any tools with which to judge the operation or accuracy of the AI for the individual person whose case is in front of them. Nor does it address the issue of possible typographical errors. And still, the defendant has no ability to view the formula or check its correctness or assess its applicability.

The federal government has put advance thought into ensuring more open uses of AI, when in the First Step Act, Congress legislated the use of risk assessments regarding federal prisoners. The Act called for a panel of researchers to vet the research design for this new risk assessment instrument, annual validation, and even "a requirement that [BOP staff] demonstrate competence in administering the System, including interrater reliability, on a biannual basis"[21] The legislative text was noteworthy in its embrace of a more open approach.

Unfortunately, after enactment, when First Step Act resulted in the development of the PATTERN risk assessment, the developers of the PATTERN, as well as the Department of Justice, in approving the risk instrument, did not explain the key choices: the selection of risk thresholds, or the validation data, which itself was not shared with other researchers. One problem was that the Act itself did not provide guidance on what should be deemed high, medium, low, or minimal risk. The Act provided even less information about how the dynamic or treatment related "needs" items should be operationalized, resulting in real concerns with the PATTERN instruments definitions of such items. The authors of the PATTERN have not shared annual data regarding

[19] Paul Heaton, Sandra Mayson & Megan Stevenson, *The Downstream Consequences of Misdemeanor Pretrial Detention,* 69 STAN. L. REV. 711, 747 (2017); Will Dobbie et al., *The Effects of Pre-Trial Detention on Conviction, Future Crime, and Employment: Evidence from Randomly Assigned Judges*, 108 Am. Econ. Rev. 201, 224–26 (2018).
[20] State v. Loomis, 881 N.W.2d 749, 767 (Wis. 2016).
[21] Brandon Garrett and Megan Stevenson, *Open Risk Assessment*, 38 BEHAVIORAL SCIENCES AND LAW 279 (2020), doi.org/10.1002/bsl.2455.

the performance of the risk instrument, either. Only very general information has been reported, including that errors in the design were uncovered and supposedly corrected.[22]

Second, a wide range of AI is now used in forensics, to conduct analyses on physical and biometric evidence from crime scenes. In forensics, we traditionally often had people who look at patterns and called a "match," or a source identification, whether it was fingerprints, or firearms, or bitemarks. We know that they get it wrong and innocent people have been convicted based on those mistakes. AI may be able to improve on this pattern recognition work. Replacing humans with machines may not be bad if humans are comparatively more error prone. We need to be sure, though, that the machines work better and that they work fairly - or that they work at all.

To return to facial recognition technology, across the country, driver's license photos are being fed into the federal face recognition system, along with other photos, such as images captured from airport cameras and the like.[23] None of us agreed to have our faces included. We are part of an omnipresent lineup, and it is one maintained (in one such effort) by the federal government. The Federal Bureau of Investigation (FBI) maintains the FACE system of facial recognition. Its use raises privacy implications. It also raises accuracy questions. How likely is it that we will be misidentified? If a person is charged with a crime based on a "hit" using the federal FACE database, what can we say about how good the match is?

The FBI has been unwilling to share how the FACE algorithm works, what data it was trained on, and nor has the FBI detailed how the algorithm has been tested and how accurate it is. The GAO has repeatedly issued reports, given the FACE database use of large amounts of private biometric information, calling on the FBI to conduct such testing of false and negative positive rates.[24] The FBI has responded that its policy "policy prohibits photos being provided as positive identification and photos cannot serve as the sole basis for law enforcement action," and that ongoing work is being done to improve the accuracy of the system, including based on NIST

[22] U.S. Department of Justice, Office of Justice Programs, 2020 Review and Revalidation of the First Step Act Risk Assessment Tool, at https://www.ojp.gov/pdffiles1/nij/256084.pdf.

[23] Statement of Kimberly J. Del Greco, Criminal Justice Information Services Division Federal Bureau of Investigation Before The Committee on Oversight and Reform U.S. House of Representatives at a Hearing Concerning "The Use of Facial Recognition Technology by Government Entities and the Need For Oversight Of Government Use of This Technology Upon Civilians" 4 (2019) ("The FACE Services Unit performs facial recognition searches of FBI databases (e.g., FBI's NGI-IPS), other federal databases (e.g., Department of State's Visa Photo File, Department of Defense's Automated Biometric Identification System, Department of State's Passport Photo File), and State photo repositories (e.g., select State Departments of Motor Vehicles, criminal mugshots, corrections photos, etc.)"), at https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Wstate-DelGrecoK-20190604.pdf.

[24] U.S. Government Accountability Office, *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains* (2019), at https://www.gao.gov/products/gao-19-579t ("First, GAO found that the FBI conducted limited assessments of the accuracy of face recognition searches prior to accepting and deploying its face recognition system. The face recognition system automatically generates a list of photos containing the requested number of best matched photos. The FBI assessed accuracy when users requested a list of 50 possible matches, but did not test other list sizes. GAO recommended accuracy testing on different list sizes. Second, GAO found that FBI had not assessed the accuracy of face recognition systems operated by external partners, such as state or federal agencies, and recommended it take steps to determine whether external partner systems are sufficiently accurate for FBI's use. The FBI has not taken action to address these recommendations.").

evaluations.[25] Hopefully federal and local law enforcement adhere to that restriction, and can improve the system, but it also begs the question whether such evidence should be used for preliminary criminal identification purposes, or as part (but not the sole) basis for a criminal prosecution, absent publicly-available information about its accuracy and operation.

If a facial recognition algorithm is used purely for an investigative purpose not designed to develop evidence against a suspect, such as to scan public places to search for a victim of human trafficking, then the same rights are not implicated. It is far more tolerable to use a tool that with less-clear evidence of reliability, purely as a way to generate leads to locate a missing person. The privacy rights of that missing person are not of salient concern. If a missing person is ultimately found based on those leads, then it is not relevant whether the system generated false leads or not, and nor do we typically need courtroom disclosure of how the system worked. However, the same system should not be used, without evidence of its reliability, to generate evidence linking a person to a crime. In the same way, police may rely on an anonymous tip of unknown reliability, to potentially generate leads in an investigation. If those tips help police locate a missing person or stolen property, then they reliability is corroborated, and there is little reason to inquire further into the source of the information. However, police cannot normally introduce statements by an anonymous tipster in court as evidence to support in a criminal prosecution.

There should be a strong presumption of transparency and interpretability for courtroom uses of AI. There may also be reasons to protect certain types of AI systems from disclosure, for which the presumption may be overcome. For example, if there is a strong national security justification for not making the full AI model public, at a minimum, it should be carefully vetted by independent researchers, with complete information about its strengths and limitations made available to users in law enforcement and the courts. This failure to open the black box on its FRT programs, shared with law enforcement around the country and used by federal agencies,[26] is deeply troubling. We know quite a bit now about how accurate eyewitnesses are, and courts increasingly take real pains to ensure that a criminal jury hears about the reliability of eyewitness evidence, including due to concerns regarding error rates and cross-racial biases. Further, there is evidence that depending on what data they are trained on and how they are designed, that FRT can be racially biased unless (like Clearview AI's technology that uses biometric information from Internet users that have not given permission) it uses a massive dataset. NIST itself has reported on and documented real differences between facial recognition approaches, both regarding accuracy and bias.[27] So far, courts have not ensured that the jury hears about how reliable untested FACE AI is. And that raises deep constitutional concerns as well as reliability concerns. We

[25] Grieco, *supra*, at 3-4. *See also* P. Jonathon Phillips, Amy N. Yates, Ying Hu, Carina A. Hahn, Eilidh Noyes, Kelsey Jackson, Jacqueline G. Cavazos, Géraldine Jeckeln, Rajeev Ranjan, Swami Sankaranarayanan, Jun-Cheng Chen, Carlos D. Castillo, Rama Chellappa, David White, Alice J. O'Toole, *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms*, 115 PNAS 6171 (2018), at https://www.pnas.org/content/115/24/6171.

[26] *Facial Recognition Technology: Current and Planned Uses by Federal Agencies* (2021), at https://www.gao.gov/assets/gao-21-526.pdf (noting "18 of the 24 surveyed agencies reported using an FRT system, for one or more purposes").

[27] Dr. Charles Romine, Facial Recognition Technology (FRT), Testimony, Committee on Homeland Security, U.S. House of Representatives (2020) (noting "There, false positive differentials are much larger than for false negatives and exist across many, but not all, algorithms tested. Across demographics, false positives rates often vary by factors of 10 to beyond 100 times. False negatives tend to be more algorithm-specific, and often vary by factors below 3.").

should not use AI or any other technique in order to identify suspects criminal investigations if we do not know how good it is for achieving the purpose to which it is put.

This is an area where the federal government needs to lead in showing that use of AI robustly protects constitutional rights. Instead, the federal government is showing how readily it will permit defendant rights to be sacrificed in the name of expediency and profit by companies.

We note that our comments on surveillance to identify criminal suspects does not pertain to applications such as school security, where the goal is to eliminate a possible immediate threat. This is a separate topic than identifying suspects for criminal prosecution; they should not be confused or linked. For instance, it is possible to design security systems that require only biometric information from individuals who were previously identified as possible threats.[28]

Proposed Federal Legislation

It is noteworthy that the FTC has issued business guidance and begun enforcement regarding uses of AI in private industry, regarding non-transparent and misleading uses of AI and biased uses of AI, where they implicate consumer rights, under the FTC Act mandate to prevent unfair and deceptive practices. Each of those subjects should be also, as described, be the subject of federal efforts to prevent harms to the government's own uses of AI in criminal cases. Similar efforts should be aimed at ensuring that government agencies do not violate constitutional criminal procedure rights, through non-transparent and unfair AI practices. We note that the U.S. House of Representatives has considered a "Justice in Forensic Algorithms Act" which would ensure that any algorithms used in criminal cases be unrestricted by any claim of proprietary or trade secrets protection, and vetted by NIST. Congressman Dwight Evans, D-PA, said: "Opening the secrets of these algorithms to people accused of crimes is just common sense and a matter of basic fairness and justice. People's freedom from unjust imprisonment is at stake, and that's far more important than any company's claim of 'trade secrets.'"[29] Even absent such legislation, such an approach should be adopted by the federal government. Basic transparency standards and testing requirements should be follow by law enforcement and courts if they use AI tools in criminal cases.

Conclusion

We close by emphasizing that *the burden of justification should be on those proposing to maintain non-transparent, black box use of AI*. Government secrecy should never be the norm and the federal government should lead by example, and *because due process should be understood to require it*. The existing Bill of Rights provides important protections as against arbitrary action, without notice, and action that harms defendant's fair trial and defense rights, as well as against discriminatory action in violation of the Equal Protection Clause and implementing civil rights acts. However, those protections have not proved effectual as remedies in criminal cases, given

[28] Cynthia Rudin and Shawn Bushway, *A Truth Serum for your Personal Perspective on Facial Recognition Software in Law Enforcement*, Translational Criminology (2021).

[29] Reps. Takano and Evans Reintroduce the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System (2021), https://takano.house.gov/newsroom/press-releases/reps-takano-and-evans-reintroduce-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system.

limited pretrial discovery, inadequate defense resources, and a tradition of deferential gatekeeping regarding expert evidence. We ask that Office of Science and Technology Policy attend to these basic principles of open AI and careful and robust adherence to existing constitutional criminal procedure rights, as it conducts the important work of development of a broader AI Bill of Rights.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Brian Krupp

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: Brian Krupp
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Monday, October 11, 2021 1:54:19 PM

Good Afternoon,

I am responding to the RFI on Public and Private Sector Uses of Biometric Technologies. My background is in mobile privacy where I do research primarily in how mobile applications use data that is both sensed, stored, and inferred from a smartphone. I was very pleased to see that the government is taking action when it comes to biometrics and creating a "Bill of Rights" in regards to how AI is implemented and being used.

From my research, the larger concern is how the data used in artificial intelligence is gathered. In mobile apps, users do not have a bill of rights, yet spend a considerable amount of time a day interacting with their devices. One study showed the average American spends over 4 hours a day on their smartphones. When we think about this interaction, there is quite a bit of data that can be gathered and when we think about the revenue from companies such as Facebook and Google, which do not sell most consumers a service where it is primarily driven from advertising, the more precise they are with their advertising (from the data they collect), the more profitable they become. Tangentially, these services and the algorithms that serve content to the users, whether they be advertisements or recommendations, have been found to put users in content bubbles and serve content that can be misinformation and addictive. I think if we truly want to provide a bill of rights for consumers, we need to start where the data is collected, and mobile devices seems to be a prime candidate based on the amount of time that users interact with the device and the data that is stored, sensed, and inferred from the device.

The more transparency that consumers are provided, the more their attitudes change with concerns on privacy and data collection. Past studies have shown this including our own. Also, when controls that limit data collection are made available to users and not hidden away in an application (dark patterns), more users adopt these controls. An example of this is the recent change in iOS where an application requests if they can track the user. In one study, an overwhelming majority of users chose the option not to allow tracking. This is critical because if we want the public to buy into the effort, they need greater controls and abilities to see their data. When they have this, they can then better understand the value in these efforts and be more interested in the outcomes of these efforts. The capabilities to provide great transparency and controls to users already exist and have been shown in previous research to be effective. Recently, some of these have been incorporated partially in iOS and Android where users have more fine-grained control of their data. However, the pace of implementing these controls and transparency natively have been slow. Additionally, two companies (Apple and Google), solely control 100% of the smartphone operating system market in how these controls are implemented.

I believe we need to start with the source of the data first, which is why I'm advocating for greater transparency and controls on mobile device, and perhaps even a Bill of Rights on the intrusive data collection that is performed on the devices we interact with the most.

Thank You,
Brian Krupp

Dr. Brian Krupp
Associate Professor of Computer Science
MOPS & CS+ Faculty Advisor
Baldwin Wallace University

>https://mops.bw.edu<

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Brooklyn Defender Services

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

[redacted]

January 14, 2022

Via Electronic Mail
Office of Science and Technology Policy
Executive Office of the President
1600 Pennsylvania Ave NW
Washington, DC 20500
[redacted]

Re: Comments in Response to Request for Information on Public and Private Sector Uses of Biometric Technologies
86 Fed. Reg. 56300 (October 8, 2021)

To Whom It May Concern:

Brooklyn Defender Services ("BDS") submits these comments in response to the Office of Science and Technology Policy ("OSTP")'s Request for Information on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56300, issued on October 8, 2021.

Brooklyn Defender Services (BDS) is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. For over 25 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality.

We represent approximately 25,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or deportation. Our staff consists of specialized attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

We thank President Biden and the OSTP for the opportunity to provide information and feedback about the uses of biometric technologies within the many systems our clients and communities are forced to navigate. This comment will address topics #1 and 4.

Criminal Defense: Our criminal defense legal teams encounter biometric technologies routinely across cases and contexts. The NYPD frequently deploys facial recognition systems, latent prints, and DNA analysis, for example. This comment will focus on two recent troubling deployments in the criminal legal system context: unlawful local DNA databasing and voice printing.

[redacted]

I. Unlawful local DNA databasing

In 1997, the New York City Office of Chief Medical Examiner (OCME) implemented a system for collecting previously-typed DNA profiles into a searchable local database. Originally, the OCME's local database was called LINKAGE. In 2014, the lab absorbed the LINKAGE database into the local level of the CODIS database,[1] called the Local DNA Index System ("LDIS").

At a state level, the New York State legislature created the State DNA Databank in 1994 with the passage of Executive Law § 995. The database became operational in 1996. By law, when it comes to known contributors, the New York database can only house DNA collected from people convicted of a crime. While the list of crimes for which a conviction permits DNA sample collection has grown five times since 1996, the New York State legislature has repeatedly rebuffed efforts to expand DNA collection to people who are arrested but never convicted of a crime.[2]

Despite New York State's careful balance between the individual's rights to genetic and basic privacy, as well as due process, and the State's interest in crime solving, the City of New York's agencies—the NYPD and the OCME—have chosen to operate a rogue DNA database that reaches samples taken from persons not authorized for collection. In other words, the OCME's "LDIS" does an end run around New York State's carefully prescribed scheme. Over the last five years, the OCME's rogue database has been growing.[3]

[1] By way of brief background, CODIS (Combined DNA Index System) is actually the software databasing package developed and provided by the Federal Bureau of Investigation to DNA laboratories around the country. The CODIS database system consists of three levels: the National DNA Index System (NDIS); the State DNA Index System (SDIS); and the Local DNA Index System (LDIS). As the administrator of the CODIS database system, the FBI promulgates detailed regulations governing the types of samples that can be uploaded to NDIS, as well as quality assurance standards for labs conducting testing that feeds into NDIS.

[2] It is worth noting that, in 1999, the legislative record reflects that then-Mayor Rudy Giuliani even specifically requested that the legislature expand collection to arrestees. Mayor Giuliani asserted: "While the City enthusiastically supports this legislation and acknowledges the positive effect it will have on solving crime, it should be noted that the City of New York believes DNA testing upon arrest would allow for even greater efficiency and effectiveness in law enforcement. Examining DNA samples at the time of arrest would dramatically increase the ability of police to accurately identify or negate one's potential culpability while under arrest." The New York State Legislature refused to expand the database to arrestees.

[3] Ann Givens and Robert Lewis, "Push to solve gun cases fuels rapid growth of New York's DNA database," New York Daily News (Sept. 25, 2017), at https://www.nydailynews.com/new-york/nyc-crime/push-solve-gun-cases-fuels-growth-new-york-dna-database-article-1.3516711.

[redacted]

a. Growth of the OCME's Rogue Database

This unauthorized database has been fed in part by the surreptitious collection of individuals' saliva samples by the NYPD. Self-regulation is not the answer here. What started as a self-regulated, unauthorized database has emerged into a vast invasion of the genetic privacy of thousands of New Yorkers, many if not most of whom, are impoverished people of color.

We have watched videos where our clients have asserted their right to counsel as they drink from a water bottle or smoke a cigarette offered to them by the police. NYPD has even been observed offering teenagers cigarettes in addition to juice bottles or water bottles for DNA collection. No person, let alone a child, would envision that accepting a cigarette to smoke in the middle of a public building with the blessing of the police would mean that their DNA profile would end up in perpetuity in a database. Then they are led out of the interrogation room, the cigarette butts and juice bottles are left in an intentionally placed ashtray or garbage bin. The police then collect the cigarette butts and bottles for evidence. This same little game plays out with water cups and juice or water bottles, and DNA profiles are collected by the thousands.

The local database is in contravention to Executive Law § 995-d, which dictates that the results of DNA testing are confidential, and which specifically protects the right of a defendant to nondisclosure of his or her DNA information.

As Dr. Howard Baum, former Technical Leader of the OCME and creator of the local database, has stated: he never envisioned that the database would become the repository of profiles that the NYPD dragnetted from Black and brown communities. Our clients have been directly impacted by dragnets – the systematic search for someone such as "a Black male in Brownsville" — practices that target our clients particularly because they are Black or because they are male or because they reside in a particular neighborhood.

Dr. Baum never envisioned that the database would include thousands of profiles from people who were tricked into handing over their DNA without consent or court-order. Even our clients who consented to have their DNA taken have told us that they had no real understanding that their cooperation meant that their DNA would stay in a government database forever.

Dr. Baum never envisioned that the local database would include people who were merely detained – sometimes never even arrested, and many never convicted of any crimes.

The local database was also set up long before the NYPD's Domain Awareness System was created. The Domain Awareness System ("DAS") is a software program created by the NYPD and Microsoft that aggregates data collected by the NYPD across the city. While the DAS's role in aggregating surveillance camera video is well known, another DAS function is

its ability to inform officers whether or not an individual detainee's DNA profile is in the database – thus making the detainee a target for DNA collection by individual police officers.

b. The OCME and NYPD DNA Collection and Storage Practice's Threat to our Community's Liberty is Growing.

The current practices of the NYPD mean that it is not only the countless numerical profiles of mainly people of color that are warehoused in an electronic database. For each of those warehoused profiles, the OCME maintains extracts of the DNA in tiny vials. As technologies emerge, law enforcement and the lab can go back to that vial and effectively interrogate the DNA to invade the genetic privacy of the individual's genetic code in even deeper and more disturbing ways.

Genetic genealogy, which has been much reported-on in the news recently, is only the latest incarnation. This technique uses DNA analysis methods that mine more of the human genome for sensitive information than a traditional forensic DNA test and surveil not just the individuals' DNA but also the DNA of that individual's entire family line.

The DNA technique employed in genetic genealogy—Single Nucleotide Polymorphism (SNPs) testing or Next Generation Sequencing—is being considered for widespread forensic uses by the law enforcement community as we speak. Whereas traditional DNA testing—Short Tandem Repeat (STR) testing—only measures the lengths of certain segments of non-coding regions on our genome, SNPs and NextGen testing actually code the genome (revealing the specific As, Gs, Ts, and Cs we all learned about in high school) and potentially reveal deeply intimate details including things like predisposition to disease and susceptibility to addiction. And where STR testing only looks at a very small percentage of the overall genome, SNPs testing looks at huge percentages of the overall genome, revealing the most private elements of our selves.

In the face of this brave new world of genetic testing and the overall threat to privacy, as well as our First Amendment associational freedoms, we need to think about historically targeted communities when considering emerging technologies. The OCME and the NYPD, without oversight or regulation are effectively building a warehoused library of entire communities' genetic extracts. With emerging technologies like genetic genealogy and so-called Next Generation Sequencing, the genetic privacy of not only the individual but the individual's family will come under surveillance by law enforcement.

We now know that 'Junk DNA' is not really "junk" at all: it can by tied by inference to other areas on the human genome, that in turn can reveal sensitive information like susceptibility to disease.[4] As technologies emerge and forensic profiles become even more

[4] *See* "Statistical Detection of Relatives Typed with Disjoint Forensic and Biomedical Loci," Cell 175, 848–858, October 18, 2018, and "Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets," PNAS | May 30, 2017 | vol. 114 | no. 22 | 5671–5.

revealing of a person's biological status, it is incumbent upon our elected officials to protect the genetic privacy of all people.

II. Voice printing

While the communities we represent are routinely having their genetic information collected and aggregated by law enforcement, its members often face the long-lasting and community-draining impact of periods of incarceration. Family and friends coordinate visits and phone calls, attempting to tend the connection between their incarcerated loved ones and the community they were torn from. On the other end of that tether, those incarcerated view access to outside phone calls to their family members, loved ones, counselors, and friends as a much-needed lifeline. But access to communication comes at a very real biometric cost.

Here, in New York City, the Department of Correction has contracted with the private company Securus Technologies to provide phone services within the City's jails. Far from a basic phone company, however, Securus is more aptly described as a surveillance-tech-company-turned-phone-service-provider. One piece of Securus's phone surveillance apparatus relies on the universal use of voice printing.

a. The Technology.

Securus Technologies' phone system in an institution like those on Rikers Island audio records *every* phone call made. The call recordings are housed in an investigational database and are accessible to Corrections' law enforcement officers. To sort this vast amount of unstructured data, Securus offers several products. One offering relies on the collection of a voiceprint database to identify the participants in audio-recorded calls.

In 2014, the City's Department of Correction entered into its first contract with Securus. Under that agreement, every person brought to a city jail and anyone on the outside who receives a call from DOC phones has their voiceprint taken. The voiceprint is merely a visual representation of an individual's speech pattern. But available reporting indicates that the voice print database maintained by Securus includes speech patterns for all of those incarcerated, as well as those who have been incarcerated at any point in the past. It also houses voice prints from everyone who received a call from a Securus phone, including mothers, children, spouses, loved ones, siblings, friends, counselors, lawyers, spiritual advisors, and social workers.

The voiceprint database is run in conjunction with the audio recording database to analytically determine who participants are in recorded calls. The data aggregation and analytics tools allow law enforcement to identify recordings by voice print. For example, an investigator could search the recording database with my voice print and return all files that record my phone conversations, regardless of who originally placed the call or what number originally received it.

Other uses for the compiled voice print databases have not been publicly disclosed.

b. The Impact.

Just as the City's local DNA database results in a community dragnet, housing the biometric intimacies of entire communities' lives and identities, the voice print database results in a community dragnet of vocal identity, relationship, and intimate communication.

The repeated targeting of specific communities for such programs of mass surveillance reemphasizes the need for lawmakers to take seriously the task of legislative protection. If our lawmakers do not act soon, the rise of biometrics, big data analytics, and machine-driven surveillance will fundamentally destroy our bedrock First and Fourth Amendment principles.

Unemployment Insurance Benefits: Outside of the criminal legal system, our clients are encountering biometric surveillance in diverse arenas. Our family defense, immigration, and civil legal services teams encounter biometric technology use in a number of different contexts and use cases. This comment will focus on a recent troubling deployment in the employment benefits context.

BDS's employment practice assists BDS clients by removing barriers to employment created by court-involvement. Our interdisciplinary team helps to fight employment discrimination, ensure clients are paid a fair wage, receive employment benefits, like time-off, and are free from workplace abuses. Our staff also provide legal representation and informal advocacy to clients seeking Unemployment Insurance Benefits.

Over the past year, BDS has seen a dramatic increase in need for those seeking assistance with accessing unemployment insurance benefits. Specifically, our clients have encountered two recurring problems. First, we have received countless calls from unemployed New Yorkers whose unemployment insurance payments had suddenly stopped without them understanding why they had stopped or what to do about it. Second, we also heard from newly unemployed New Yorkers that although they had filed applications and were claiming every week, they were not receiving benefits and did not understand why.

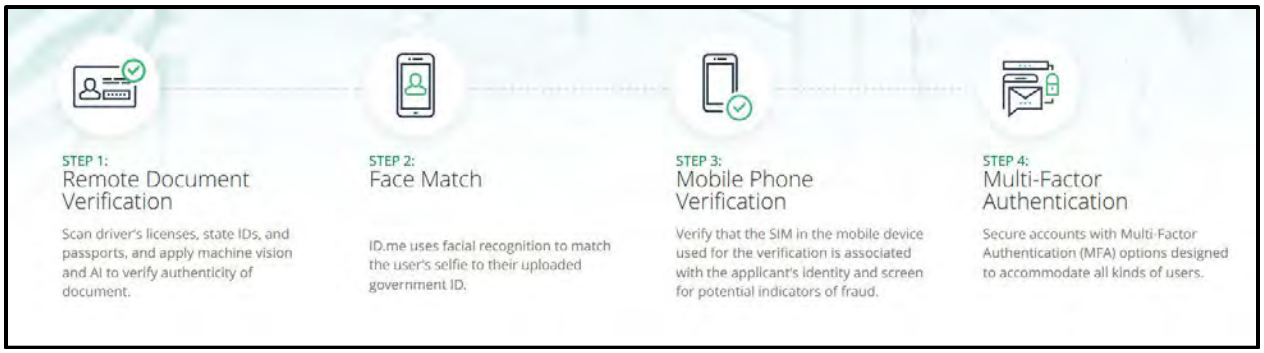
Through our work with those clients, BDS has come to understand that these claimants have run headlong into the deployment of a new technological solution for identity verification. In response to concerns around fraudulent unemployment claims, a near majority of states onboarded the web-based identity verification program ID.me beginning in the spring of 2020. New York State was one of several states that bypassed the traditional RFP process and contracted for ID.me's services in that time period.

The web-based product deploys "machine vision" and AI, as well as facial recognition technology, to provide identity verification services to the New York State Department of Labor ("NYSDOL").

[redacted]

I. The Technology.

ID.me self-reports that they implement a four-step process to verify identity:[5]



The company publicly touts that it is in compliance with NIST 800-63-3's identity proofing and authentication standards. The company has not publicly verified what facial recognition algorithm it is using for its 1:1 face matching, and has not publicly provided verification and validation data supporting either its document verification function or its facial recognition program.

Additionally, when a person is instructed to use ID.me to verify their identity, they are faced with a potential security risk. A google search for "ID.me" returns the company's generic website. Through this website, New Yorkers are able to enter all of the required personal information—including identity documents and faceprints—into the generic ID.me website. The site does not warn visitors that it will not interface with that visitor's relevant state agency.

In fact, numerous New Yorkers we work with, who proactively attempted to comply with the ID.me verification requirement, later learned that the generic site is not linked in any way with NYSDOL. Despite having submitted large amounts of private and biometric information to the government-designated private corporation, those New Yorkers experienced significant delays in identity verification, waited weeks or months to receive benefits they were owed, and were ultimately required to resubmit their information to a specific NYSDOL ID.me. Where all of that originally-submitted private and biometric information went has not been answered.

II. The Impact.

Unfortunately, the use of ID.me for identity verification has resulted in delays and denials causing New Yorkers serious financial and personal harm.

[5] https://www.id.me/business/government

[redacted]

Document verification failures. ID.me's process appears to apply an overly restrictive list of acceptable identity documents, but also fails to publicly provide the list of identity documents it will accept. Two examples:

a. ID.me provides no submission opportunity for name change orders. The failure to do so prevents transgender and gender-nonconforming claimants from verifying their identities.

b. ID.me rejects validly-issued but expired passports or identification documents, despite barriers to renewal posed by the COVID pandemic. This rejection has been specifically detrimental for claimants with foreign identity documents. Nothing in state or federal law prevents the acceptance of a validly-issued, but expired identity document as proof of identity.

Facial recognition failures. ID.me's 1:1 facial recognition process appears to disproportionately reject the identity of women, transgender or gender-nonconforming, and BIPOC claimants. Two examples:

a. We have had to work with a number of claimants with darker skin tones to lighten their identity documents in order for ID.me's algorithms to accept those documents. Similarly, we have had to work with claimants to ensure high levels of light in their spaces when attempting to interface with ID.me's face scanning function. This failure of ID.me's face recognition suite is not specific to ID.me, but a known risk for facial recognition projects.[6] Despite this, ID.me has not publicly released any information about the actual performance of its face recognition suite.

b. We have heard from a number of claimants that they have been rejected by the face match scan with no explanation or instruction for correction. The vast majority of claimants experiencing these rejections have been Black women, transgender and nonconforming claimaints, and people with darker skin tones. Without providing any data, verification/validation, or other studies, ID.me claims its algorithms are 99.9% efficacious. This kind of bald statistical salesmanship is both offensive and misleading to those who are being rejected by the system.

Error correction failures. ID.me allegedly provides access to a "Trusted Referee" via a mobile app to address any technical failures encountered in interfacing with the algorithms. The wait times for reaching these Trusted Referees have been days-to-weeks long.

[6] *See, e.g.*, Patrick Grother, et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[redacted]

Outright exclusionary barriers. ID.me's process imposes exclusionary barriers to those in need of accommodation due to disability, language and literacy, or technology access and age.

a. Disability barriers: ID.me's technological process does not provide appropriate accommodations for those with physical or mental disabilities. Reliant on text-based instructions, visual interaction, and technological literacy, ID.me's identity verification becomes an insurmountable barrier for those requiring accommodation.

b. Language and literacy barriers: New York law and the NYSDOL's own Language Access Plan require agencies to offer adequate translation and interpretation services for limited English proficiency ("LEP") claimants.[7] Although various languages are purportedly supported by ID.me, the available list is quite restrictive and many claimants who speak even the most common non-English languages in New York await an ID.me representative in their language for weeks.

   Similarly, ID.me provides detailed written instructions, but those instructions are inaccessible for those who are illiterate, as well as for those whose English is limited. The only other available instructions available are a very brief outline in Spanish alone. As a result, LEP claimants and those with literacy barriers are more likely to experience wrongful delays or terminations of their benefits.

c. Technology access and age barriers: ID.me's web-based process relies on a level of technological access and literacy that is inaccessible for many New Yorkers, particularly lower income New Yorkers and older individuals. State and federal law and administrative guidance consistently require public programs and services to be meaningfully accessible. We have repeatedly worked with claimants for whom the technological navigation of the system was a real and, at times insurmountable, struggle. As a result, lower income

[7] N.Y. Executive Order 26.1, available at: https://www.governor.ny.gov/sites/default/files/atoms/files/EO_26.1.pdf; NYSDOL Language Access Plan available at: https://dhr.ny.gov/sites/default/files/pdf/lep/DOL-LAP-2021.pdf. Federal guidelines also outline alternatives states should use to create access for LEP claimants: https://wdr.doleta.gov/directives/corr_doc.cfm?docn=9141; and https://wdr.doleta.gov/directives/attach/UIPL/UIPL_02-16_Change-1.pdf

and older claimants are more likely to experience wrongful delays or terminations of their benefits.

We have repeatedly seen claimants struggle to complete the ID.me process. The requirement to verify ID through a web-based platform without offering reasonable alternatives excludes these individuals from receiving benefits in a timely manner.

Please do not hesitate to contact us if you have questions regarding our comments. Thank you for your attention and considering our concerns.

Sincerely,

/s/ *Elizabeth Daniel Vasquez*
Elizabeth Daniel Vasquez
Director, Science & Surveillance Project

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

BSA | The Software Alliance

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 13, 2022

The Honorable Eric Lander
Director, US Office of Science Technology Policy
Science Advisor to the President
1650 Pennsylvania Ave., NW
Washington, DC 20502

The Honorable Alondra Nelson
Deputy Director, US Office of Science Technology Policy
1650 Pennsylvania Ave., NW
Washington, DC 20502

Dear Director Lander and Deputy Director Nelson,

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to provide feedback on the Office of Science and Technology Policy's (OSTP) effort to create a "Bill of Rights for an Automated Society" and engage the public in "National Policymaking about AI and Equity."[2] We commend OSTP for launching this initiative to examine policy options for ensuring AI systems are designed and deployed responsibly and safeguarding the public from the risks of unintended bias. Recognizing that industry has a key role to play in addressing these issues, we recently published *Confronting Bias: BSA's Framework to Build Trust in AI*, which sets out a comprehensive impact assessment process for identifying and mitigating the risks of AI bias.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members are at the forefront of software-enabled innovation that is fueling economic growth in every industry sector. As

[1] BSA's members include: Adobe, Atlassian, Alteryx, Autodesk, Bentley Systems, Box, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.
[2] Join the Effort to Create A Bill of Rights for an Automated Society | The White House

global leaders in the development of data-driven enterprise software solutions, BSA's members have a keen interest in working with policymakers to establish a legal environment that can support the public's trust and confidence in the technologies that are driving today's digital economy.

Tremendous advances in artificial intelligence are quickly transforming expectations about how the technology may reshape the world. Every day, companies now leverage AI-powered tools to enhance their product offerings, solve complex business challenges, and accomplish previously unimaginable tasks. For instance, AI is now enabling graphic designers to automate elements of their workflows that used to constitute tedious distractions; it is spurring American manufacturers to improve the performance of their products while reducing costs to consumers and environmental impacts; and it is helping small businesses serve their global customers through the use of real-time translation functionality.

However, the rapid pace of AI innovation is also prompting important conversations about equity. While AI can undoubtedly be a force for good, there is a growing recognition that it can also perpetuate (or even exacerbate) existing social biases in ways that may systematically disadvantage members of historically marginalized communities. BSA therefore applauds the Office of Science and Technology Policy's recent launch of an initiative to develop a "Bill of Rights for an Automated Society" (AI Bill of Rights).[3] By articulating baseline expectations for responsible AI development and deployment practices, an AI Bill of Rights can foster greater public trust in technologies that are playing an increasingly important role in our daily lives.

In addition to enumerating the "rights and freedoms we expect data-driven technologies to respect," we agree that the AI Bill of Rights should also contemplate how those rights will be protected.[4] To that end, we offer below two recommendations that the Administration should consider as it develops a workplan for the AI Bill of Rights. First, to ensure that companies are implementing responsible AI practices to prevent civil rights abuses, the AI Bill of Rights initiative should encourage organizations to perform comprehensive impact assessments prior to the deployment of any high-risk AI system. Second, the Administration should use this opportunity to ensure that all agencies responsible for the oversight of civil rights protections have the legal authorities and resources they need to

[3] Americans Need a Bill of Rights for an AI-Powered World | WIRED
[4] Id.

robustly enforce violations regardless of whether AI is being used. Unlawful discrimination should be just as unlawful when AI is being used as when it happens in the physical world.

By articulating a clear policy vision that maximizes the benefits of AI while addressing its key risks, the AI Bill of Rights initiative can also serve as a foundation for international engagement. The global nature of today's technology ecosystem makes international cooperation on shared regulatory challenges more important than ever. A robust AI Bill of Rights initiative can help foster common agreement in transatlantic and transpacific dialogues on regulatory harmonization.

Encouraging the Adoption of AI Impact Assessments

When AI is used in ways that could adversely impact civil rights or access to important life opportunities, the public should be assured that such systems have been thoroughly vetted and will be continuously monitored to account for the risks associated with unintended bias by the companies that develop and/or deploy them. For BSA members, earning trust and confidence in the AI they develop is crucial, so identifying ways to reduce the risk of bias is a top priority. BSA therefore set out to develop real, credible, and actionable steps to guard against the potential of AI systems producing unintended disparate impacts. The resulting framework – *Confronting Bias: BSA's Framework to Build Trust in AI*[5] – was released in June of 2021 and is built on a vast body of research and informed by the experience of leading AI developers. BSA has been pleased to testify about the Framework before the US Congress and the European Parliament, and BSA presented about the Framework as part of the National Institute of Standards and Technology's AI Risk Management Framework workshop in October.

The BSA Framework outlines a lifecycle-based approach for performing impact assessments to identify risks of AI bias and corresponding best practices for mitigating those risks. Impact assessments are widely used in a range of other fields—from environmental protection to data protection—as an accountability mechanism that promotes trust by demonstrating that a system has been designed in a manner that accounts for the potential risks it may pose to the public.

[5] Confronting Bias: BSA's Framework to Build Trust in AI

The purpose of an AI impact assessment is to establish organizational processes to guide the development and use of high-risk systems by requiring internal stakeholders to identify the risks that a system may pose, quantify the degree of harm the system could generate, and document any steps that have been taken to mitigate those risks to an acceptable level. By establishing a process for personnel to document key design choices and their underlying rationale, impact assessments are a crucial mechanism for advancing trust. Given the nascent state of AI technical standards, impact assessments performed by organizations that develop and/or deploy AI are the most effective tool for promoting transparency and accountability of AI systems.

The foundation of the BSA Framework is a detailed methodology for performing impact assessments that help ensure that key decisions are documented and that an organization's product development team, its compliance personnel, and senior leadership are aligned on the appropriate steps for mitigating risks of bias when they are identified. A key attribute of the BSA Framework is a recognition that impact assessment processes must span throughout the lifecycle of an AI system. The impact assessment methodology in the BSA Framework therefore includes more than 50 diagnostic statements that should be documented throughout an AI system's lifecycle. Among its key recommendations is for organizations to maintain documentation about:

- The objectives and assumptions of the system, including its intended use cases and its target variable;
- The metrics that will be used as a baseline for evaluating bias in the system;
- The provenance of the data used to train the system, an evaluation of its appropriateness for the intended use case, and the steps that were taken to scrutinize the data for biases;
- The rationale for selecting data attributes and their impact on model performance; and
- The lines of responsibility for monitoring the system following deployment and plans for responding to potential incidents or system errors.

The BSA Framework is ultimately a playbook that organizations can use to enhance trust in their AI systems through risk management processes that promote fairness, transparency, and accountability. Consistent with the practices set out in the BSA Framework, we urge OSTP to consider options for encouraging organizations to perform comprehensive impact assessments on AI systems that pose a potential risk to civil rights. Crafting an effective and workable impact

assessment policy that can address both the broad range of AI uses that may implicate civil rights and the multiple stakeholders that may have responsibility for managing the risks associated with any particular system (e.g., system developers, service providers, and entities that deploy AI systems) will require careful consideration. We would welcome the opportunity to work with you to resolve those challenges.

Ensuring Civil Rights Protections Remain Fit for Purpose in the Digital Age

While the responsibility for managing the risks of AI falls squarely on the organizations that develop and use AI systems, civil rights protections should be updated as needed to protect from discrimination. As digital technologies are deployed in ways that impact the most important aspects of life in America, from hiring decisions to housing and lending policies, the government should ensure that the law will continue to afford the same level of protection irrespective of whether a decision is made by a person or an automated system.

A key element of the AI Bill of Rights initiative should therefore be a comprehensive review of existing consumer and civil rights protections to determine whether they remain fit for purpose. For instance, agencies that are responsible for enforcing civil rights protections should be directed to audit their existing enforcement authorities to evaluate whether they need to be updated to account for changes in technology. As part of such an audit, agencies should assess whether there are gaps in the current framework of civil and consumer protection law or whether resource constraints currently impede enforcement agencies from diligently pursuing violations. Because the enforcement of civil rights laws is dispersed among multiple executive and independent agencies, OSTP leadership is needed to coordinate an all-of-government approach to analyzing the current state of the law. To the extent gaps are identified, the Administration should seek to fill them in through appropriate resource allocations, providing additional regulatory guidance, and where necessary working with Congress to update the underlying legislative frameworks to ensure that civil rights protections remain both technologically neutral and robustly enforceable. Moreover, there is a growing recognition of the linkage between data privacy, AI, and civil rights, so we would encourage OSTP to coordinate with other agencies – such as NTIA – that have expressed an interest in these issues.

* * * * *

BSA looks forward to collaborating with the Administration as the AI Bill of Rights initiative moves forward and applauds your commitment to ensuring that US leadership in the development of AI is supported by a robust and coherent framework of consumer protections. With countries around the world beginning to grapple with the challenges of updating their policy and regulatory environments to account for both the unique opportunities and the potential risks implicated by AI, the Bill of Rights initiative is an opportunity for the US to play a leading role in establishing legal norms for the regulation of AI. It is our hope that the AI Bill of Rights – in conjunction with the Administration's other AI-related work, such as NIST's development of an AI Risk Management Framework – will help lay the groundwork for a comprehensive and forward-leaning AI policy framework. With the European Union in the midst of developing its own approach to AI regulation, we urge you to think boldly and ambitiously about how the AI Bill of Rights initiative can be harnessed to keep the United States in synch with the EU and other key markets that are contemplating reforms. A cohesive US policy on AI, along with your sustained leadership, can create interoperability on core AI regulatory issues that can protect both consumers and the competitiveness of American companies.

Sincerely,

Christian Troncoso
Senior Director, Policy

The Software Alliance

BSA

Confronting Bias:
BSA's Framework to Build Trust in AI

CONTENTS

Introduction

Tremendous advances in artificial intelligence (AI) research and development are quickly transforming expectations about how the technology may shape the world. The promise that AI may one day impact every industry is quickly turning into a commercial reality. From financial services to healthcare, AI is increasingly leveraged to improve customer experiences, enhance competitiveness, and solve previously intractable problems. For instance, AI is enabling medical researchers to diagnose early-stage Alzheimer's Disease years before debilitating symptoms arise,[1] and it is helping ecologists analyze impossibly large datasets to better track the impact of their efforts to preserve critical habitat and prevent illegal elephant poaching in Malawi.[2]

As used in this report, the term "artificial intelligence" refers to systems that use machine learning algorithms that can analyze large volumes of training data to identify correlations, patterns, and other metadata that can be used to develop a model that can make predictions or recommendations based on future data inputs. For example, developers used machine learning to create "Seeing AI," an app that helps people who are blind or visually impaired navigate the world by providing auditory descriptions of objects in photographs.[3] Users of the app can use their smartphone to take pictures, and Seeing AI describes what appears in the photograph. To develop the computer vision model capable of identifying the objects in a picture, the system was trained using data from millions of publicly available images depicting common objects, such as trees, street signs, landscapes, and animals. When a user inputs a new image, Seeing AI in effect predicts what objects are in the photo by comparing it to the patterns and correlations that it derived from the training data.

The proliferation of AI across industries is also prompting questions about the design and use of the technology and what steps can be taken to ensure it is operating in a manner that accounts for any potential risks it may pose to the public.

The use of advanced technologies in connection with high-stakes decisions presents both opportunities and risks. On the one hand, the adoption of AI by financial institutions has the potential to reduce discrimination and promote fairness by facilitating a data-driven approach to decision-making that is less vulnerable to human biases.[4] For instance, the use of AI can improve access to credit and housing to historically marginalized communities by enabling lenders to evaluate a greater array of data than is ordinarily accounted for in traditional credit reports. At the same time, researchers caution that flaws in the design, development, and/or deployment of AI systems have the potential to perpetuate (or even exacerbate) existing societal biases.[5]

Developing mechanisms for identifying and mitigating the risks of AI bias has therefore emerged as an area of intense focus for experts in industry, academia, and government. In just the past few years, a vast body of research has identified a range of organizational best practices, governance safeguards, and technical tools that can help manage the risks of bias throughout the AI lifecycle. Static evaluations of AI models cannot account for all potential issues that may arise when AI systems are deployed in the field, so experts agree that mitigating risks of AI bias requires a lifecycle approach that includes ongoing monitoring by end-users to ensure that the system is operating as intended.

This document sets forth an *AI Bias Risk Management Framework* that organizations can use to perform impact assessments to identify and mitigate potential risks of bias that may emerge throughout an AI system's lifecycle. Similar to impact assessments for data privacy, AI impact assessments can serve as an important assurance mechanism that promotes accountability and enhances trust that high-risk AI systems have been designed, developed, tested, and deployed with sufficient protections in place to mitigate the risk of harm. AI impact assessments are also an important transparency mechanism that enables the many potential stakeholders involved in the design, development, and deployment of an AI system to communicate about its risks and ensure that responsibilities for mitigating those risks are clearly understood.

In addition to setting forth a process for performing an AI impact assessment, the Bias Risk Management Framework:

- Sets out the key corporate governance structures, processes, and safeguards that are needed to implement and support an effective AI risk management program; and
- Identifies existing best practices, technical tools, and resources that stakeholders can use to mitigate specific AI bias risks that can emerge throughout an AI system's lifecycle.

This Framework is intended to be a flexible tool that organizations can use to enhance trust in their AI systems through risk management processes that promote fairness, transparency, and accountability.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Carnegie Mellon University

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 18, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW
Washington, DC 20504

RE: RFI Response: Biometric Technologies

Carnegie Mellon University (CMU) welcomes this opportunity to provide comments in response to the White House Office of Science and Technology Policy (OSTP) Request for Information (RFI) on the use of biometric technologies for identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.[1] We'd like to recognize that this RFI is a part of a broader strategy that OSTP has taken to help ensure that artificial intelligence (AI) technology is deployed safely and effectively balancing the privacy and safety of citizens with the advancement of society as a whole. CMU appreciates the leadership that OSTP is providing to ensure the ethical and inclusive development of emerging technologies through such initiatives as the development of an AI Bill of Rights.

CMU conducts a broad range of societal research that is enabled through the use of biometric data. Some examples include research in accessibility, manufacturing, and autonomous vehicles - these all utilize human-robot and human-computer interaction and rely on the use of massive data sets that use biometrics in order to continue to develop technologies to improve society. CMU faculty are also leaders in AI research and policy development. For example, CMU faculty contributed to the development of the Department of Defense ethical principles for artificial intelligence and the university has acted to develop and deploy a comprehensive AI curricula, including strong attention throughout on AI ethics..

CyLab is CMU's security and privacy research institute where experts from schools across the university, encompassing the fields of engineering, computer science, public policy, information systems, business, humanities, and social sciences work together to address some of society's largest research problems. CyLab researchers are often called upon by government leaders to provide expertise on security and privacy issues. Their work in helping shape public policy related to security and privacy spans several decades.

CMU's comments focus on three key points. First, "biometric technologies" refer to systems that use biometric information for a broader range of uses than just recognition (identity verification

[1] 86 Fed. Reg. 56300 (Oct. 8, 2021).

or authentication). OSTP recognizes that biometric technologies have increasingly been used for identification or inference of emotion, disposition, character, or intent. We provide a number of examples of such biometric technologies.

Second, CMU researchers believe that technologies that use biometric information for non-recognition purposes have the potential to greatly improve lives, in particular the lives of individuals with certain disabilities. However, a significant obstacle to effectively developing these technologies is a lack of varied and robust data. For example, an assistive device designed to aid an individual with speech-affecting disabilities must be trained using audio recordings that include recordings of individuals with such disabilities. The datasets available to researchers typically do not represent such individuals.

Finally and relatedly, CMU recognizes the challenge in balancing the privacy expectations of individuals with the needs of research and development in order to create an effective governance model.

Examples of Use of Biometric Information for Recognition and Inference

Broadly speaking, we use "biometric technology" to refer to a system that uses biometric information (*i.e.*, measurements or derived data of an individual's physical or behavioral characteristics) for any number of purposes. Many people are aware that biometric technology can be used in the context of identity verification, for example, using a fingerprint to unlock a device or voice recognition to confirm identity. CyLab researchers are working on improving the accuracy of biometric systems used for identity authentication with robust development and testing and keeping in mind ways adversaries may try to spoof these systems. In addition, one goal of CyLab's biometric researchers is making biometric identification an effortless, foolproof, and fair task.

Beyond traditional matching of biometric information to a specific individual for identity verification or authentication, biometric technologies can be used for such purposes as gauging employee effectiveness (*e.g.*, through keystroke monitoring), recording attendance (*e.g.*, through facial recognition), or in marketing scenarios (*e.g.*, use of facial recognition to detect unhappy in-store shoppers). Biometric technologies can also be used to identify individuals at a categorical level without identifying a human as a specific individual.

Biometric information can also be used to enhance understanding of commands and intent. Examples include, but are not limited to, speech recognition systems that use raw speech data to convert speech to text or robot systems that observe human motion in video data to determine safe, efficient, or appropriate trajectories (e.g., bring the next part for a manufacturing task to the human at the right time and in the right way).Developing techniques that understand commands and intent requires collecting data that contains human faces, gaits, and other identifying features in order to properly train and evaluate new robot systems. There are numerous multi-camera

datasets used for these purposes and they are the foundation for advances in modern robot systems.

Another important potential application of biometric technologies that involves the classification of emotion for speech has been of great interest to different constituencies. For example, call centers would like to make use of this information to guide agent behaviors (both humans and artificial). However, emotion information is also of use in other contexts, for example for 911 call evaluation. Other public-facing services would benefit from such information. Companion agents (*e.g.*, for the elderly) can also benefit, by supporting the development of systems that can react to emotional states and that need to develop empathetic relationships with humans. Research in this area has been hampered by lack of data. Relatively small amounts have been created for research. But progress in this area requires significant amounts of data. Current data, *e.g.*, audio recordings of podcasts, can be used but it needs to organized for such research. Moreover, additional categories of data (linked to potential use cases) need to be identified and used to improve the technology.

Benefits and Harms Associated with Biometric Technologies

One area where biometric technologies have the potential to greatly improve lives is in the improvement of assistive devices. Carnegie Mellon University (CMU) researchers use biometric information extracted from raw data such as video and audio recordings and images to train ambient artificial intelligence and improve the ability of such devices to respond to the particular needs of individuals. For example, information about how people speak (which may be considered biometric information) can be extracted from audio recordings and used to train AI models to better respond to questions and commands. However, in order for AI to be trained in a fair an equitable way that benefits all members of society, the raw data from which biometric information is extracted must be varied and robust. In the context of the example above, an audio dataset must include recordings of a wide range of individuals in order to train the AI to understand commands from individuals who may have accents or speech impediments, One potential hurdle in creating the types of datasets that are needed is that individuals may not expect that information about them, such as footage from a surveillance camera, to be used for biometric technologies. This creates a challenge to researchers who seek to balance the privacy expectations of individuals with the needs of research and development.

The benefits of biometric technologies in the realm of assistive devices are significant. For example, Professor Henny Admoni conducts research to understand and develop autonomous, intelligent robots that help people live better. An example of the lab's research involves developing devices to assist humans that may have an upper body mobility limitation. Such limitations can prevent people from performing everyday tasks such as picking up a cup or opening a door. The U.S. Census Bureau has indicated that more than 8.2% of the U.S. population, or 19.9 million Americans, suffer from upper body limitations. Assistive robots offer a way for people with severe mobility impairment to complete daily tasks. However, current assistive robots primarily operate

through teleoperation, *i.e.,* the remote operation of devices through a user's hand and body movements, which requires significant cognitive and physical effort from the user. Professor Admoni's research relates to understanding human verbal and nonverbal behaviors (like speech and eye gaze) during robot teleoperation. The research ultimately aims to develop technology to decrease operator fatigue and task duration when using assistive robots by employing human-sensitive shared autonomy.

The analysis of biometric information in video, audio, and image datasets is essential to the development of the ambient AI systems designed to provide real-time assistance to humans. For example, developing a virtual kitchen coach that helps people with dementia safely prepare their own food at home would require the AI to have an understanding of how humans move. Biometric data about physical and physiological characteristics of humans, such as their gait, can be extracted from video datasets. Other examples of assistive devices include, but are not limited to, an AI-equipped manufacturing space that uses video information to support just-in-time delivery of materials and an AI-equipped sports training program that watches the user and provides feedback.

While biometric technologies have the potential for great benefits, there is also a risk of harm if these technologies are not developed with sufficiently broad datasets. New datasets are needed to ensure equity since existing datasets may have widespread population biases. This limits the value and safety of AI systems. For example, most speech datasets lack the necessary training data to understand disability-affected speech (*e.g.*, ALS, multiple sclerosis, etc.). Likewise, video datasets often lack enough training data for AI systems to identify and behave properly around people with disabilities. Without robustly diverse data from which to extract biometric information to train AI, an autonomous vehicle may not detect or act properly when encountering a pedestrian who is using a wheelchair or cane.

One potential challenge to creating the types of datasets that are required to develop biometric technologies is balancing the needs of research and development with the privacy expectations of the people about whom the data may relate. While there may be mainstream acceptance of video recording in public places for surveillance purposes, for example, most individuals may not expect information about their physical characteristics to be extracted from the recording for product development. CMU researchers have done extensive research on how people feel about a wide range of video analytics/facial recognition scenarios representative of the current state of practice. The main article detailing our research, which involved asking 123 people to answer questions about a variety of video analytics deployments they could realistically encounter as they went about their regular daily lives over the course of 10 days, resulted in detailed responses about 2,328 video analytics scenarios.[2]

These results provide a uniquely rich picture of how people feel towards different deployment scenarios and how their perceptions of these scenarios vary from one individual to another.

[2] S Zhang, Y Feng, L Bauer, LF Cranor, A Das, and N Sadeh, ""Did you know this camera tracks your mood?": Understanding Privacy Expectations and Preferences in the Age of Video Analytics", Proceedings on Privacy Enhancing Technologies, 2, 1, Apr 2021 [pdf].

Overall, while many (though not all) people seem to have grown accustomed to the deployment of some video surveillance technologies, many express surprise and a desire to be informed about and exercise some control over more recent types of deployments such as deployments in the workplace, deployments geared towards marketing or attendance tracking purposes, or video analytics capable of making inferences about someone's health, including mental health.

Governance Programs

Carnegie Mellon University (CMU) recognizes the challenge of developing policy that sufficiently mitigates potential harms to consumers arising from the collection and use of biometric information without hampering critical research and innovation.

As mentioned above CMU's study confirms that people have diverse attitudes towards different scenarios involving the collection of biometric data. Current biometric privacy laws at the state level, such as the Illinois Biometric Information Privacy Act, focus on a notice and consent model under which organizations must provide notice to individuals in order to collect and process their biometric information, and in some cases, obtain consent.

Organizations deploying biometric technologies often rely, for example, on signs that read "this area under camera surveillance" or some equivalent language. These signs themselves often do not inform people about how their data will be processed (*e.g.*, what type of analysis will be run on the footage), for what purpose, with whom results will be shared, or for how long they will be retained. They do not provide mechanisms for people to opt-in or opt-out of these practices and do not enable them to access the results (*e.g.*, discovering what was possibly inferred about someone's mood or productivity).

In response to the challenge of providing adequate notice and obtaining consent, CMU researchers have developed and deployed a privacy infrastructure for the Internet of Things (IoT) that can be used to inform people about the collection and use of their biometric data as they go about their activities. This infrastructure is accessible at: https://iotprivacy.io. It already hosts close to 150,000 entries for Internet of Things resources that collect data about individuals. These entries are accessible via an "IoT Assistant" mobile app available on both iPhones and Android phones. Using their IoT Assistants, users can be informed via customizable notifications about biometric/IoT data collection scenarios they care about as they go about their regular activities. The infrastructure includes a portal that allows entities deploying IoT/biometric data collection technologies to disclose the presence of their technologies and make them discoverable. It allows entities to provide users with privacy controls, for example in order to comply with privacy laws such as the EU's General Data Protection Regulation.

While the notice-and-consent model seeks to alleviate some of the privacy concerns associated with the collection and use of biometric information, it is important to note that the model may be unduly burdensome in the research context and thus impede the ability to realize the important societal benefits of the responsible use of biometric technologies.

As an alternative, future policies could reflect current governance models used for research. Traditionally, best practices for collection, storage, sharing, and other processing of data, including sensitive health and personal data, have been managed through Institutional Review Boards (IRBs). These remain the best situated, trained, and suited to balance risk to participants against benefits to both the participants and society as a whole.

The IRB is a diverse group of scientific and non‐scientific individuals who conduct the initial and ongoing review of research studies in order to ensure the protection of the rights, safety, and well‐being of human subjects participating in those studies. The federal code of regulations (Title 45) governs the composition and conduct of the IRB.

Current IRB best practices reflect that in certain situations, providing notice and obtaining consent before collecting information about individuals is appropriate. Moreover, IRB best practices recommend participants in private settings be offered an option for requesting deletion of collected video or audio data. This option is often not required for public settings where there is no expectation of privacy (*e.g.*, a location that also has security cameras or is heavily populated by other people).

CMU also recognizes that recent bipartisan measures by Congress[3] and the science agencies to integrate a focus on ethics and increased awareness of the potential impact of technologies such as biometrics will enhance effective governance programs and policies.

[3] These measures include provisions in the National Artificial Intelligence Initiative Act of 2020 that advances the development of ethics or risk statements as a part of or subset of all applications for research to the National Science Foundation. The Act, Division E of Public Law No: 116-92, also advances the integration of ethics education into STEM curricula from K-12 to higher education.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Center for Democracy & Technology

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

To: Suresh Venkatasubramanian
White House Office of Science and Technology
Executive Office of the President
1650 Pennsylvania Avenue NW
Washington, DC 20504

Re: RFI Response: Biometric Technologies, Document Number 2021-21975

I. Introduction

The Center for Democracy & Technology (CDT) welcomes the opportunity to submit comments to the White House Office of Science and Technology (OSTP) on public and private sector uses of biometric technologies. CDT is a nonprofit, nonpartisan 501(c)(3) organization that advocates for civil rights and civil liberties in the digital age. CDT works on many issues involving the use of biometric data in a range of contexts from law enforcement to hiring. In these comments, we focus on the impact of the use of biometric data on disabled people.

Like other forms of marginalization, ableism is systemic.[1] Most social spheres have historically been structured to primarily, if not exclusively, serve people who appear, communicate, move, think, and behave in certain ways, and who share similar baseline needs that must be met in order for them to fully participate in society. Many health conditions become disabilities because they affect people's needs, ability to conform to these norms, and interactions with existing social structures. The technologies utilized in these social spheres can reflect this ableism for multiple reasons, including: flawed and unrepresentative training data can result in inaccurate and biased outcomes; the technologies' purpose, use, and design may be based on implicit or explicit judgments about the inherent value of disabled people; or disability issues may simply be overlooked when designing and deploying the technologies.[2]

[1] HENRY CLAYPOOL ET AL., AM. ASS'N OF PEOPLE WITH DISABILITIES AND CTR. FOR DEMOCRACY & TECH., CENTERING DISABILITY IN TECHNOLOGY POLICY: ISSUE LANDSCAPE AND POTENTIAL OPPORTUNITIES FOR ACTION 30 (2021), https://cdt.org/wp-content/uploads/2021/12/centering-disability-120821-1326-final.pdf.

[2] Ctr. for Democracy & Tech. et al., Comments to the United Nations Special Rapporteur on the Rights of Persons with Disabilities' Report on Artificial Intelligence, https://cdt.org/wp-content/uploads/2021/11/Comments-to-UN-SR-for-Disability-Report-on-Artificial-Intelligence.pdf.

When biometric technologies are poorly trained and unsuitable for the services for which they are utilized, they make disabled people, especially multiply-marginalized disabled people, more vulnerable to algorithmic discrimination. As with other AI systems, biometrics are developed using datasets that are supposed to train them to accurately evaluate people in the real world. Training datasets can be derived from various sources, including historic data, voluntary survey responses and research participation, and publicly available data. If training data misrepresents or excludes marginalized groups or intersections of these groups, this can skew the outcomes of technologies trained on this data. Even when biometrics are trained and designed to improve accuracy, they may rely on stereotypes about marginalized groups that correlate with seemingly neutral decision-making criteria. To make matters worse, data collected through these technologies may be shared with third parties or otherwise utilized for purposes unrelated to a person's intended engagement with the technologies, creating privacy risks for affected people.

In the remainder of these comments, we discuss several examples that illustrate how biometric technologies used to verify identity and to infer cognitive, physical, and emotional states can reproduce and further entrench disparities for disabled people.

II. Diagnostics and health care management

Biometric data analysis can be helpful in health care because without documented diagnosis, healthcare providers, insurers, employers, academic institutions, and other entities limit or deny access to accommodations and supports that help disabled people meet their needs. However, biases in health care technologies can limit access to accommodations and supports, and ultimately to critical life opportunities and better quality of life.

For example, medical professionals use facial analysis to diagnose a range of conditions, including in people who are nonverbal and have difficulty articulating pain.[3] Automated facial analysis can be an unreliable diagnostic tool for multiply-marginalized disabled people as it has been shown to produce higher rates of error for darker skin tones and along gender lines.[4] One study also found that image-based diagnostic algorithms are disproportionately trained on data from only three states – California, New York, and Massachusetts – which all report lower rates

[3] Kristina Grifantini, *Detecting Faces, Saving Lives: How Facial Recognition Software is Changing Health Care*, IEEE PULSE (May 13, 2020), https://www.embs.org/pulse/articles/detecting-faces-saving-lives/.

[4] *See* JOY BUOLAMWINI & TIMNIT GEBRU, GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

of disability than the national average.[5] Recognizing these sources of bias, researchers have developed facial analysis tools that are trained to work on more diverse populations, but they caution that these technologies should be only part of the clinical evaluation process.[6]

Biometric and other data-driven technologies also apply traditional diagnostic standards, without accounting for additional information and context that might better inform human-driven evaluation. Diagnostic standards are based on presumptions about how and among whom certain medical conditions present, influencing datasets derived from people who have had access to diagnosis and treatment.[7] For example, facial analysis has been used to diagnose autism by analyzing facial expressions and repetitive behaviors, but these attributes tend to be evaluated relative to how they present in a white autistic person assigned male at birth and identifying as masculine.[8] Attributes related to neurodivergence vary considerably because racial and gender norms cause other forms of marginalization to affect how the same disabilities present, are perceived, and are masked. Therefore, people of color, transgender and gender nonconforming people, and girls and women are less likely to receive accurate diagnoses particularly for cognitive and mental health disabilities, and that would also be true of biometric technologies trained on data that embeds these biases. Accurate facial and behavioral analysis of one type and presentation of disability may also vary due to other disabilities – disabilities that affect facial features, bone structure, or mobility might impact whether a cognitive or mental health disability is accurately diagnosed.[9]

The use of biometric data in health also presents privacy risks. On the one hand, such data can help people manage their health independent of health care providers, and it is increasingly being used for that purpose. Consumers have turned to commercial sleep and fitness trackers that analyze heart rate, body temperature, movement, voice tone and talking during sleep.[10]

[5] AMIT KAUSHAL ET AL., GEORGRAPHIC DISTRIBUTION OF US COHORTS USED TO TRAIN DEEP LEARNING ALGORITHMS, 324 J. AM. MED. ASS'N 1212 (2020), https://jamanetwork.com/journals/jama/fullarticle/2770833; WILLIAM ERICKSON ET AL., CORNELL U. YANG-TAN INST. ON EMP. & DISABILITY, 2018 DISABILITY STATUS REPORT: UNITED STATES 7-8 (2020), https://www.disabilitystatistics.org/StatusReports/2018-PDF/2018-StatusReport_US.pdf.

[6] Grifantini, *supra* note 3.

[7] *See* CYNTHIA BENNETT AND OS KEYES, WHAT IS THE POINT OF FAIRNESS? DISABILITY, AI, AND THE COMPLEXITY OF JUSTICE, 27 ACM SIGACCESS ACCESSIBILITY AND COMPUTING 2-3 (2019), https://arxiv.org/pdf/1908.01024.pdf; Daniel Young, *Black, Disabled, and Uncounted*, NAT'L HEALTH LAW PROGRAM (Aug. 7, 2020), https://healthlaw.org/black-disabled-and-uncounted/.

[8] BENNETT, *supra* note 7.

[9] *See* Sheri Byrne-Haber, *Disability and AI Bias*, MEDIUM (July 11, 2019), https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533.

[10] Victoria Song, *Amazon Halo View Review: The Fitbit Clone No One Asked For*, THE VERGE (Dec. 15, 2021, 8:00 AM), https://www.theverge.com/22834452/amazon-halo-view-review-fitness-trackers.

People are also relying on mental health apps that collect users' self-reported entries.[11] But much of the biometric data collected and processed by these trackers, apps, and other products is highly sensitive and can allow cognitive or mental health disabilities to be inferred. In many cases HIPAA does not apply to these products, and in the absence of applicable privacy rules, such data may be used for unrelated purposes or shared with third parties who can repurpose this data for marketing or combine it with other data to re-identify users.[12]

III. Public benefits, assistive technology, and IoT devices

Benefits. Biometric data is used to verify identity information for fraud detection for unemployment insurance and other types of public benefits. Systems that rely on facial recognition to verify applicants' identities have proven challenging to use,[13] a problem which can be exacerbated for disabled users. For instance, facial recognition systems often employ a "liveness test" to ensure that the system is not matching against a photo or a mask. Liveness tests that rely on nodding at or making "eye contact" with the camera can be impossible for blind users to complete without assistance, further raising the barriers to critical social supports for disabled people.[14]

Other algorithmic systems calculate the hours of home- and community-based services (HCBS) a disabled person needs or the budget to cover that care,[15] which can then be subject to biometrics. Electronic visit verification (EVV) is used to detect fraud, waste, and abuse in the provision of HCBS benefits.[16] In many EVV systems, the home care worker or the benefits recipient must call into the system within a set window of time to verify through facial recognition or biometric voice authentication that the approved worker is providing the hours

[11] Andrew Crawford, *Protecting Health Data – CDT and eHI Release Consumer Privacy Framework for Health Data*, CTR. FOR DEMOCRACY & TECH. (Feb. 9, 2021), https://cdt.org/insights/protecting-health-data-cdt-and-ehi-release-consumer-privacy-framework-for-health-data/.

[12] *Id.*

[13] *See* Hannah Quay-de la Vallee, *Combatting Identify Fraud in Government Benefits Programs: Government Agencies Tackling Identity Fraud Should Look to Cybersecurity Methods, Avoid AI-Driven Approaches that Can Penalize Real Applicants*, CTR. FOR DEMOCRACY & TECH. (Jan. 7, 2022), https://cdt.org/insights/combatting-identify-fraud-in-government-benefits-programs-government-agencies-tackling-identity-fraud-should-look-to-cybersecurity-methods-avoid-ai-driven-approaches-that-can-penalize-real-applicant/.

[14] Jonathan Keane, *Facial Recognition Apps Are Leaving Blind People Behind,* VICE (March 22, 2016), https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind

[15] LYDIA X.Z. BROWN ET AL, CTR. FOR DEMOCRACY & TECH., CHALLENGING THE USE OF ALGORITHM-DRIVEN DECISION-MAKING IN BENEFITS DETERMINATIONS AFFECTING PEOPLE WITH DISABILITIES (2020), https://cdt.org/insights/report-challenging-the-use-of-algorithm-driven-decision-making-in-benefits-determinations-affecting-people-with-disabilities/.

[16] ALEXANDRA MATEESCU, DATA & SOCIETY, ELECTRONIC VISIT VERIFICATION: THE WEIGHT OF SURVEILLANCE AND THE FRACTURING OF CARE 15-16 (2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf.

of approved services to the approved recipient.[17] People whose disabilities affect their verbal communication and ability to make calls or stay still to capture a facial image may not be able to successfully use this system, requiring workers to turn to an alternate web-based system that can be burdensome to navigate.[18] If home care visits cannot be verified, home care workers are underpaid for their labor.[19] All the while, EVV systems are collecting and storing voice and other data beyond what is legally mandated.[20] By undermining access to public benefits, these systems can affect disabled people's ability to live independently.

Assistive Tech/Internet of Things (IoT). Systemic barriers to independent living make it all the more necessary for disabled people to be able to use assistive technology and IoT devices, many of which use biometric data that can enable inferences about cognitive or emotional states. Assistive technologies include automated captioning and speech-to-text services that use voice data, and video chat platforms that capture facial imagery. IoT devices are used in homes and automobiles to control lights and other personal devices, appliances, and security systems through voice recognition and iris and fingerprint scans.[21] These technologies can allow disabled people to depend less on others to live in, manage, and navigate their environments.[22]

However, greater reliance and integration of these biometric technologies into disabled people's day-to-day lives comes with greater risk of data exposure and misuse. Several commercial products involve access for other authorized users, data sharing between interconnected devices subject to different companies' data policies, cloud data storage that might be vulnerable to data breaches, and data sharing with advertising partners.[23] Disabled consumers' biometric data can be further misappropriated due to security lapses: hackers accessed Amazon Ring's smart cameras – ironically, used for home security – in multiple incidents of harassment and abuse that have left people afraid to live alone.[24]

[17] *Id.* at 54; JACQUELINE MILLER, ET AL., UNIVERSITY OF CAL. SAN FRANCISCO HEALTH WORKFORCE RESEARCH CTR. ON LONG-TERM CARE, IMPACT OF ELECTRONIC VISIT VERIFICATION (EVV) ON PERSONAL CARE SERVICES WORKERS AND CONSUMERS IN THE UNITED STATES 5 (2021), https://healthworkforce.ucsf.edu/sites/healthworkforce.ucsf.edu/files/EVV_Report_210722.pdf.
[18] *See* MILLER, *supra* note 15, at 11; MATEESCU, *supra* note 14, at 54.
[19] MILLER, *supra* note 15, at 15; MATEESCU, *supra* note 14, at 17.
[20] MILLER, *supra* note 15, at 6; MATEESCU, *supra* note 14, at 8.
[21] CLAYPOOL, *supra* note 1, at 41.
[22] *Id*. at 40.
[23] LAUREN SMITH, ET AL., FUTURE OF PRIVACY FORUM, THE INTERNET OF THINGS (IOT) AND PEOPLE WITH DISABILITIES: EXPLORING THE BENEFITS, CHALLENGES, AND PRIVACY TENSIONS 10-14 (2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.
[24] Kari Paul, *Dozens Sue Amazon's Ring After Camera Hack Leads to Threats and Racial Slurs*, THE GUARDIAN (Dec. 3, 2020, 4:40 pm),

When forced to choose between getting the benefits of these technologies or avoiding privacy risks, disabled people and other marginalized communities cannot afford to prioritize privacy protection over the benefits they need.[25] They should not have to choose – policy reforms must prevent privacy harms and educate disabled consumers and commercial entities about these risks, while ensuring that policies do not undermine disabled people's access to these benefits.

IV. Hiring technologies

Today's hiring processes incorporate biometric data that can directly indicate cognitive and emotional states, which particularly disadvantage disabled workers already subject to employment barriers. Hiring technologies evaluate this data purportedly to gauge a candidate's suitability for the job position in question, but the inferences drawn are often less relevant to job success and instead relevant to disability.[26] Certain tools analyze candidates' responses to questions about how they feel, or their selection of images with which they identify, to measure personality traits such as optimism, conscientiousness, or "emotional stability."[27] Recorded video interview tools use facial and voice analysis that captures a candidate's speech patterns and tone, gestures and limb movements, facial expressions, and eye contact to assess their enthusiasm, assertiveness, extroversion, trustworthiness, and other traits.[28] Gamified testing analyzes candidates' keystrokes and clicks while they play a set of games, purportedly measuring personality traits as well as cognitive skills and aptitudes such as response time, ability to adapt and learn from mistakes, attention span, and performance under pressure.[29]

Personality traits measured with these tools are not always relevant to essential job functions, and they are often subject to interpretation. For instance, whether a candidate is perceived as "optimistic" depends on how the trait is depicted and labeled as such in the tool's training data. The training data might only reflect stereotypes about the facial expressions or vocal tone

https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.

[25] *See* CLAYPOOL, *supra* note 1, at 40.

[26] CTR. FOR DEMOCRACY & TECH., ALGORITHM-DRIVEN HIRING TOOLS: INNOVATIVE RECRUITMENT OR EXPEDITED DISABILITY DISCRIMINATION? 11-12 (2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf [hereinafter "ALGORITHM-DRIVEN HIRING TOOLS"].

[27] *Id.* at 6, 8; *Hearing on Algorithms and Bias Before the Cal. Dep't of Fair Employment and Hous.*, (Apr. 30, 2021) (testimony of Lydia X.Z. Brown), https://cdt.org/wp-content/uploads/2021/04/California-Fair-Employment-Housing-Council-Public-Hearing-Lydia-X.-Z.-Brown-statement-30.Apr_.2021.pdf [hereinafter "Testimony of Lydia X.Z. Brown"].

[28] *Id.*

[29] ALGORITHM-DRIVEN HIRING TOOLS, *supra* note 27, at 6, 8-9.

associated with that trait, and candidates might not conform to these stereotypes due to their disability.[30] Personality traits do not present similarly for every candidate, especially those with cognitive and mental health disabilities or disabilities that affect their facial appearance, voice, and speech.[31] Further, even when certain tested traits and aptitudes are relevant to essential job functions, the tools' methods of analyzing the collected data may not accurately demonstrate how disabled candidates would exhibit the necessary skills, aptitudes, or ability when performing essential job functions.[32] As a result, the processing of biometric and other data might contribute to the hiring disparities that disabled candidates already experience.

V. Surveillance technology

In addition to misuse of biometric technologies in deciding whether to affirmatively provide opportunities to disabled people across the areas discussed above, biometric data has also allowed entities to monitor disabled people in ways that effectively punish disabled people for their disability status. Such harmful uses of biometric data are especially prevalent in the education system and the workplace, and they have served to criminalize disabled people.

School and work environments. Academic institutions utilize facial recognition systems, as well as "aggression detectors" that are supposed to infer stress and anger from loud, high-pitched, and strained voices without analyzing the meaning of what is said.[33] These tools aim to promote student safety by monitoring students' behavior, detecting screams or other audible signs of stress, or verifying whether people captured on camera are authorized to be on campus.[34] During the pandemic, academic institutions began using remote proctoring software that monitors movements, sounds, keystrokes, and eye contact to flag suspicious behavior.[35]

[30] *See* Lydia X.Z. Brown, *How Opaque Personality Tests Can Stop Disabled People*, CTR. FOR DEMOCRACY & TECH. (Jan. 6, 2021), https://cdt.org/insights/how-opaque-personality-tests-can-stop-disabled-people-from-getting-hired/.
[31] *See* ALGORITHM-DRIVEN HIRING TOOLS, *supra* note 27, at 14.
[32] *See* Ctr. for Democracy & Tech., *CDT Leads Letter to New York City Council on Pending Automated Employment Tools Bill* (Feb. 25, 2021), https://cdt.org/insights/cdt-leads-letter-to-new-york-city-council-on-pending-automated-employment-tools-bill/.
[33] Alfred Ng, *Facial Recognition in Schools: Even Supporters Say It Won't Stop Shootings*, CNET (Jan. 24, 2020), https://www.cnet.com/features/facial-recognition-in-schools-even-supporters-say-it-wont-stop-shootings; Jack Gillum and Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, PROPUBLICA (Jun. 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.
[34] *Id.*
[35] Lydia X.Z. Brown, *How Automated Test Proctoring Software Discriminates Against Students with Disabilities*, CTR. FOR DEMOCRACY & TECH. (2020), https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/.

Because facial analysis has proven inaccurate particularly for dark-skinned women, and the tracked behaviors are often affected by disability rather than mal-intent, these technologies will target students of color, disabled students, and transgender and gender nonconforming students most frequently.[36]

Some of these biometric data practices also occur in the workplace through what is commonly referred to as bossware, used to gauge workers' performance and productivity.[37] Some bossware tools use speech analysis of workers' interactions with customers to measure workers' perceived empathy and other emotional characteristics.[38] Other tools track workers' movement data and keyboard and mouse interactions (which may not seem obviously biometric but which can vary substantially in speed and pattern based on physical or cognitive disability) to determine their productivity, and certain applications also collect health data to administer wellness programs.[39] Similar to the hiring context, these tools are trained on and function on the premise that only workers who behave, work, and communicate a certain way can perform their job functions as employers require. By using measures of performance or productivity that vary based on disability, these tools may make disabled people more prone to adverse decisions related to compensation, promotion, and disciplinary actions.[40]

Criminalization. As OSTP and advocates alike recognize, the harms stemming from the inaccuracies in and improper uses of facial recognition can be most acute in the law enforcement context. Law enforcement use of facial recognition has enabled targeting of Black and brown people, leading to wrongful arrests and detention.[41] Such use of facial analysis

[36] *See* Ctr. for Democracy & Tech., Comments to Office of Civil Rights, Dept. of Ed. on Protecting Privacy Rights and Ensuring Equitable Algorithmic Systems for Students of Color and Students with Disabilities, at 3 (Jul. 23, 2021), https://cdt.org/wp-content/uploads/2021/07/2021-07-23-CDT-Title-VI-Comments.pdf; Ctr. for Democracy & Tech., Comments to the U.S. Department of Education, Office of Civil Rights, Protecting Privacy Rights and Ensuring Equitable Algorithmic Systems for Transgender and Gender Non-Conforming Students, at 4 (Jun. 11, 2021), https://cdt.org/wp-content/uploads/2021/06/CDT-Title-IX-Comments-Protecting-Privacy-Rights-and-Ensuring-Equitable-Algorithmic-Systems.pdf.

[37] MATT SCHERER, CTR. FOR DEMOCRACY & TECH., WARNING: BOSSWARE MAY BE HAZARDOUS TO YOUR HEALTH 4 (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/.

[38] *Id.* at 11-12.

[39] *See* IFEOMA AJUNWA ET AL., LIMITLESS WORKER SURVEILLANCE, 105 CAL. L. REV. 735, 742-55 (2017), https://www.californialawreview.org/print/3-limitless-worker-surveillance/.

[40] *See* ANNETTE BERNHARDT ET AL., U. CAL. LABOR CTR., DATA AND ALGORITHMS AT WORK: THE CASE FOR WORKER TECHNOLOGY RIGHTS (2021), https://laborcenter.berkeley.edu/data-algorithms-at-work/.

[41] Ctr. for Democracy & Tech., *CDT Joins EFF, Algorithmic Justice League, Others in Demanding Congress Prevent Continued Use and Investment in Facial Recognition Tech*, (Jul. 1, 2020), https://cdt.org/insights/cdt-joins-eff-algorithmic-justice-league-aclu-others-in-demanding-congress-prevent-continued-use-and-investment-in-facial-recognition-tech/.

violates due process rights, chills free speech, and invades privacy.[42] These risks extend to situations where private entities collect biometric data and turn it over to law enforcement or use it as a basis for seeking police involvement. Landlords have used facial recognition to identify tenants and detect unauthorized presence on their properties, often providing this data to law enforcement to forcibly remove even tenants who are legally entitled to remain on the properties.[43] Retail establishments have also turned to behavioral AI that purports to detect shoplifting by tracking gait and classifying actions such as looking around and moving quickly as suspicious, leading to potential police involvement.[44] These systems can flag disabled people whose gait diverges from data on which the systems were trained, and the systems may also retain data about a returning shoppers' physical appearance to identify people who were previously flagged.[45]

Disabled people of color, especially disabled Black people, are at even greater risk. In addition to biases in their treatment of Black and brown communities, law enforcement tends to respond to behaviors related to deafness or to mental health or developmental disabilities with use of force, even when the behaviors do not pose an imminent threat and when the encounter was intended to be a wellness check.[46]

OSTP should encourage research to address some of these issues. For example, facial imagery and movement data recorded from police encounters should be analyzed to determine how frequently law enforcement responds with force to a disabled person's nonverbal cues, signs of

[42] SHARON BRADFORD FRANKLIN, CTR. FOR DEMOCRACY & TECH, RECOGNIZING THE THREATS: CONGRESS MUST IMPOSE A MORATORIUM ON LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECH (Oct. 14, 2021), https://cdt.org/wp-content/uploads/2021/10/Recognizing-the-Threats-Congress-Must-Impose-a-Moratorium-on-Law-Enforcement-Use-of-Facial-Recognition-Tech.pdf.

[43] Anti-Eviction Mapping Project, *Landlord Tech Watch*, https://antievictionmappingproject.github.io/landlordtech/. *See also* Lydia X.Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale and Contribute to Broader Patterns of Injustice*, CTR. FOR DEMOCRACY & TECH. (Jul. 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/.

[44] Kyle Wiggers, *Cashierless Tech Could Detect Shoplifting But Bias Concerns Abound*, VENTUREBEAT (Jan. 23, 2021, 8:45 AM), https://venturebeat.com/2021/01/23/cashierless-tech-could-detect-shoplifting-but-bias-concerns-abound/.

[45] *Id.*

[46] Lydia X.Z. Brown and Ridhi Shetty, *Critical Scrutiny of Predictive Policing is a Step to Reducing Disability Discrimination*, CTR. FOR DEMOCRACY & TECH. (Jul. 23, 2020), https://cdt.org/insights/critical-scrutiny-of-predictive-policing-is-a-step-to-reducing-disability-discrimination/; Sarah Jones, *33-50 Percent of Police Use-of-Force Incidents Involve a Person Who is Disabled*, WTHR (Jun. 19, 2020, 9:42 PM), https://www.wthr.com/article/news/33-50-percent-of-police-use-of-force-incidents-involve-a-person-who-is-disabled-has-disability/531-011bddff-a5f0-4d2a-9ad2-6964623bc32d.

stress, or inability to hear or understand what law enforcement officers are communicating. Review of this data may help assess patterns of improper and excessive law enforcement practices and lead to training or other mitigation measures to prevent dangerous outcomes.

Caretakers have sought community-driven alternatives to seeking police assistance for aggressive behavior to which police often respond with force. Now, researchers are pursuing algorithm-driven alternatives, developing wearables that monitor heart rate, voice, skin temperature, and movements to detect stress that may lead to outbursts.[47] On the one hand, this could supplement other therapeutic tools by prompting preemptive use of coping strategies.[48] On the other hand, while this technology might avoid the need for wellness checks or other law enforcement interactions, it might cause caregivers or legal guardians to intervene unnecessarily, limit disabled people's autonomy, and potentially enable abuse by caretakers.

VI. Conclusion

Although biometric technologies can provide important benefits to disabled individuals, they also present significant risks. They can perpetuate or exacerbate biases, particularly for multiply-marginalized individuals. And they can present significant privacy issues. While some of those privacy risks apply to everyone, disabled individuals are at greater risk for the reasons outlined above. The onus must be on public and private sector entities to proactively avoid reinforcing systemic ableism through exploitative biometric data practices, while ensuring that disabled people can access the benefits that biometric technologies promise.

Respectfully submitted,

Center for Democracy & Technology

[47] Emily Arntsen, *This Wearable Device Can Predict Aggressive Outbursts in People with Autism a Minute in Advance*, NEWS@NORTHEASTERN (Aug. 21, 2019), https://news.northeastern.edu/2019/08/21/this-wearable-device-predicts-aggressive-outbursts-in-people-with-autism-a-minute-in-advance/; Vanderbilt School of Engineering, *Researchers to Test Wearable Tech to Detect Problem Behaviors in Children with Disabilities and Offer Intervention Strategies* (Oct. 27, 2021), https://engineering.vanderbilt.edu/news/2021/researchers-to-test-wearable-tech-to-detect-problem-behaviors-in-children-with-disabilities-and-offer-intervention-strategies/.

[48] Will Coldwell, *What Happens When AI Knows How You Feel?*, WIRED (Dec. 29, 2021, 12:00 pm), https://www.wired.co.uk/article/artificial-emotional-intelligence.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Center for New Democratic Processes

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Center for New Democratic Processes

Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Document Citation: 86 FR 56300
Document Number: 2021-21975

The Center for New Democratic Processes (CNDP) commends the Office of Science and Technology Policy (OSTP) for seeking public comment and stakeholder input on the critical issues surrounding the development and deployment of biometric technologies by public and private sector entities. We are pleased to respond to this Notice of Request For Information (RFI) on Public and Private Sector Uses of Biometric Technologies by outlining potential benefits of deliberative civic engagement processes to support the development of policies and guidance related to the topics identified in this Request.

For the purposes of this response, we focus our comments most specifically on Section 6 of the Supplementary Information included in the Notice of Request For Information (RFI):

"Section 6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case"

The work of the Office of Science and Technology Policy could be strengthened by the utilization of deliberative civic engagement methods (such as Citizens' Juries) to engage the public (constituents, consumers, and residents) in the development of policies and guidance on the public and private sector uses of biometric technologies, key information governance and data privacy issues, and the application of artificial intelligence, automated decision-making, and machine learning technologies. The use of purposefully designed deliberative civic engagement processes could also bolster the Office's work to establish a "Bill of Rights for an Automated Society" that works for all.

Deliberative engagement on the public and private sector uses of biometric technologies, data privacy and information governance, and artificial intelligence application issues can promote diversity and equity in shaping data collection, data storage and management practices, developing regulatory oversight and guidance, and creating robust, equitable policy solutions. This can be achieved by meaningfully involving those who are directly impacted by policies and who have been historically excluded from decision-making processes and policy development - both as subject matter experts and as participants in deliberative events.

Center for New Democratic Processes

We encourage the OSTP to pursue the use of deliberative civic engagement methods as the Office undertakes efforts to gather information and inform guidance and policy development regarding (from Section 6 of the Supplementary Information in the Notice of Request For Information):

A. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;
B. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;
C. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;
D. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;
H. Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.

The Center for New Democratic Processes has demonstrated the potential impact and contributions of deliberative civic engagement to support the development of guidance and regulatory frameworks in partnership with government bodies on a range of emerging technology issues including (but not limited to) artificial intelligence and secondary uses of personal data among public and private sector entities.

In 2021 CNDP conducted a series of deliberative projects to shape national policy regarding COVID-19 data sharing initiatives on behalf of the National Health Service (England), the National Data Guardian for Health and Social Care, and NIHR-ARC Greater Manchester.

The following documents present the findings from this project.

- The Full Report from the Pandemic Data Sharing Citizens' Juries (three citizens' juries) which were conducted in early to mid-2021.
- The Executive Summary from the Pandemic Data Sharing Citizens' Juries (three citizens' juries) which were conducted in early to mid-2021.

In 2019 CNDP conducted a pair of Citizens' Juries on behalf of The National Institute for Health Research (NIHR) Greater Manchester Patient Safety Translational Research Centre (PSTRC) and the Information Commissioner's Office in the United Kingdom which focused on the tradeoffs between explainability and performance when AI-powered automated decision making systems make decisions impacting individuals. This pair of citizens' juries assessed a range of scenarios including healthcare diagnosis, organ transplant matching, employment screening, and criminal justice sentencing practices.

Center for New Democratic Processes

The following document presents the findings from this project.

- The Full Report from the AI (explainability and performance) Citizens' Juries (two citizens' juries) conducted in 2019.

The following articles, documents, and posts from project sponsors with whom we've worked demonstrate how they have incorporated and/or responded to Jury outcomes on emerging technology policy, data privacy, artificial intelligence, and information governance issues.

- From the National Data Guardian (Dr. Nicola Byrne) (project sponsor) re: Pandemic Data Sharing Juries (2021).
- From Greater Manchester National Institute of Health Research and NHSX (project sponsors) re: Pandemic Data Sharing Juries (2021).
- From the Information Commissioner's Office (project sponsor) re: AI Citizens' Juries and Interim Report from ICO on use of Jury Findings (2019).
- From the Greater Manchester Patient Safety Translational Research Centre (project sponsor) re: AI Citizens' Juries (2019).
- From the National Data Guardian (project sponsor) re: Reasonable Expectations for Data Sharing Citizens' Jury (2018).

As outlined previously on the Brookings Institution blog, "Citizens' Juries are valuable, we believe, as tools for improved policymaking. But their value may go beyond any specific use, in part because their use would demonstrate greater trust in and respect for the people. Adopting a more open version of democracy — such as one in which Citizens' Juries are positioned to purposefully shape policymaking — provides the public with a structured opportunity to directly voice their opinions and influence decision-making… An approach which purposefully situates Citizens' Juries in policy development communicates to community members and constituents that their viewpoints matter and are trusted enough to be included in the decision-making process. This could be accomplished by developing clear channels for the incorporation or adoption of jury findings and results by policymakers and decision-making bodies.

We provide this comment in response to the Request For Information on Public and Private Sector Uses of Biometric Technologies to encourage the OSTP to supplement their ongoing information gathering, stakeholder input, and policy development efforts through the use of deliberative civic engagement processes.

The Center for New Democratic Processes welcomes the opportunity to collaborate with the OSTP on efforts to utilize deliberative civic engagement on emerging technology issues.

Organizational Contact

Please contact Kyle Bozentko, Executive Director of the Center for New Democratic Processes, (email: [redacted]) for further information or with any questions.

Center for New Democratic Processes

About Us

The Center for New Democratic Processes is a nonpartisan, nonprofit civic engagement organization based in St. Paul, MN with global partners and clients. Our mission is to strengthen democracy by partnering with individuals, communities, and institutions to design and implement informed, innovative, and democratic processes to address today's toughest challenges. We provide an interdisciplinary, customized approach to the design and implementation of each deliberative process and engagement project we undertake.

Since 2012 CNDP has conducted over 150 multi-day deliberative events (Citizens' Jury, Citizens' Assembly, Community Panel, Policy Juries, etc.,) and deliberative forums (single day events) on a broad range of complex policy issues and research programs. We've advised governments and teams in Argentina, Australia, Canada, Japan, Portugal, Scotland, Singapore, South Korea, and the UK on the effective design and implementation of civic engagement strategies and public participation projects. Our recent projects have informed data privacy and governance, technology policy and artificial intelligence (AI) regulatory guidance, and shaped national policy regarding data sharing initiatives that emerged in response to the COVID-19 pandemic on behalf of the NIHR-ARC Greater Manchester, the National Health Service (England) and the National Data Guardian for Health and Social Care. We've supported rural communities responding to local impacts of climate change and extreme weather through the Rural Climate and Energy Dialogues. We worked with stakeholders to guide significant infrastructure and planning decisions with the City of Vancouver (British Columbia) through the Flats Arterial Community Panel. We designed and delivered the first Citizens' Assembly in the United States through the MN Community Assembly Project. We are currently working with the University of Liverpool and Pfizer Inc. who've commissioned the Liverpool Citizens' Jury on Antimicrobial Resistance to explore attitudes and perspectives about relationships among public and private entities collaborating to monitor and develop responses to antimicrobial resistance.

Our History

For nearly fifty years we've been expanding the boundaries of democracy through ongoing experimentation and implementation of groundbreaking deliberative processes. We were the first to employ the Citizens' Jury, invented by our founder (Ned Crosby), as a method for participatory deliberative engagement in the United States. Since its introduction, we have supported the global proliferation of this method. Throughout the 1970s, 80s and 90s our work focused on refining the use of the citizens' jury on issues ranging from Ag Impacts on Water Quality, Organ Transplants, and School-based Clinics to the Federal Budget and evaluating the positions of candidates for US Senate. In the early 2000s we covered topics such as global climate change, piloting the Citizens' Initiative Review in the state of Washington, advancing the use of deliberative democracy in Australia, and improving Electoral Recounts.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Center for Research and Education on Accessible Technology and Experiences at University of Washington, Devva Kasnitz, L Jean Camp, Jonathan Lazar, Harry Hochheiser

Areas of Strategic Visibility: Disability Bias in Biometrics

Position Statement, Submitted to EFC, January 2021.
Signatories[1]: Jennifer Mankoff, representing the Center for Research and Education on Accessible Technology and Experiences (U. Washington); Devva Kasnitz, Disability Studies (City University of New York); L Jean Camp (Indiana U.); Jonathan Lazar (U. of Maryland, HCIL, Trace Center); Harry Hochheiser (U. of Pittsburgh)

Overview. This response to the RFI considers the potential for biometrics to help or harm disabled people[2]. Biometrics are already integrated into many aspects of daily life, from airport travel to mobile phone use. Yet many of these systems are not accessible to people who experience different kinds of disability exclusion . Different personal characteristics may impact any or all of the physical (DNA, fingerprints, face or retina) and behavioral (gesture, gait, voice) characteristics listed in the RFI as examples of biometric signals.

We define disability here in terms of the discriminatory and often systemic problems with available infrastructure's ability to meet the needs of all people [UN 2017, Oliver, 2013). Using this definition, *"[biometrics] could either mitigate or amplify disability depending on how they are designed."* (Guo, 2019). As Whittaker and colleauges (2019) state, this is not simply a matter of algorithmic accuracy: *"...discrimination against people of color, women, and other historically marginalized groups has often been justified by representing these groups as disabled…. Thus disability is entwined with, and serves to justify, practices of marginalization."* (p. 11). It is critical that we look beyond inclusion to full and fully accommodated participation. Just being in the room is not enough, or just, when power, understanding and action are in the hands of computer scientists, business people and the many other stakeholders implementing biometric systems . This report adopts the philosophy of a recent report from the AI Now institute authored by multiple disabled disability scholars (*ibid.*), which asks *"How do we move from "inclusion" to 'agency and control,' given the increasingly proprietary nature of the technologies being created, and the centralization inherent in the current form of AI?"* Further, as Bennett and Keyes (2020) argue, we must look beyond **fairness**, which can only *"reproduce the discrimination it seeks to remedy,"* to disability **justice**, a term used by activist scholars steeped in the Black Lives Matter movement (Wong, 2020). Below we address each of the six categories discussed in the RFI, noting risks and opportunities. Ultimately, the concerns raised in this report can only be fully addressed with the addition of structural changes that will require regulation and control to exist within the for-profit system. Without the right guardrails, **both**

[1] The authors of this response include people with personal disability experience and people with experience in biometric and AI technology creation. This response also reflects the words of thought leaders in the field as represented in numerous cited existing reports and commentary.
[2] The language for describing people and disability is as diverse as the experience of disability itself. We reject the oversimplified binary of "identity-first" and "person-first" language. We use both, and other alternatives, based on context and goals, reflecting and respecting where modern dialogue on these issues stands.

primary categories of use raised in the RFI (recognition and inference) can actively harm or exclude disabled people.

1. Uses of Biometric Information for Recognition and Inference

The RFI points out two primary categories of use: *Recognition* and *Inference*. The benefits of such technologies are similar for people with and without impairments, however *access to such technologies is important for equitable use*. Thus, **it is critical that basic accessibility barriers with biometric technologies are addressed** (Guo, 2019). Even, if a biometric algorithm is unbiased, the interface to that algorithm, its configuration (Kane 2020), or the explanation of how it works (Wolf, 2019), may all be inaccessible. Ableist assumptions built into an application can make it inaccessible even if it meets legal standards. An example from a recent survey of disabled users of biometric systems is system timeouts that *"do not account for the slower movement speeds of people with physical disabilities"* (*ibid.*), including doors closing too fast or locking before a person can get to them; as well as timeouts in voice menus; bathroom lights; and vending machines/ATMs. The simple inability to hold still enough for biometrics to register is also often overlooked. Similarly, Kane (2020) describes how systems may not address differences in height (*e.g.,* for wheelchair users) or other physical factors such as strength, stamina, or range of motion. We note that while "Universal Design" of biometric systems is not feasible, just as one toilet height serves "most" but not all wheelchair riders, the *flexibility to adapt* can ensure accessibility to all. Such an approach avoids creating separate systems for a subset of people, which risks inequitable outcomes over time as one system is updated and others are not (Lazar, 2015).

A second and related concern in any data-driven biometric system is the fact that **data sets used to train biometric systems are biased:** they rarely if ever have a comprehensive representation of the range of people they might encounter. A person might have unusual or missing limbs and not have a fingerprint, or walk differently, or speak differently than the system expects, and thus be unable to access services tied to recognition of fingerprints, gait, or voice. Further, the oversimplification of disability experience into single diagnoses or symptoms often excludes people with multiple impairments.

2. Procedures for and results of data-driven and scientific validation of biometric technologies

The RFI asks for *"procedures data-driven and scientific validation of biometric technologies."* It is critical for such procedures to reflect the full range of persons who may be impacted by such technologies. *Measures*, and their *validity*, are important, but *what is measured* is equally important. Bias in biometric data, such as overlooking multiple co-occurring impairments, or using a voice print for identification when voices are missing, machine-produced, or unusual enough to not be recognized as human, can take several forms that all must be considered if we are to rectify the errors that result.

- **Human or Machine Bias:** Biased human perceptions of disability can accidentally be captured during data entry (Trewin, 2018). For example, suppose crowd workers are asked to label affect in images of disabled people without proper training. Similarly,

outlier detection represents a form of machine bias. Algorithms that flag or remove outliers, either at training time or at inference/detection time, may erroneously exclude people who are under-represented in the data (Guo, 2019).

- **Unrepresentative and Overly Simplified Data** When groups are historically marginalized and underrepresented, this is *"imprinted in the data that shapes AI systems… Those who have borne discrimination in the past are most at risk of harm from biased and exclusionary AI in the present."* (Whittaker, 2019, p. 8). **Addressing bias is not a simple task of increasing the number of categories represented** *(ibid.)***.** Impairment is not static, homogenous, nor do people only have one impairment. One person may have many impairments with synergistic effects. For example, facial recognition is less successful for older adults with dementia (Taati, 2019) and gait recognition accuracy differs based on age and gender (the study did not include disability). Yet, older adults are significantly under-represented in AI data sets (Park, 2021b). Other intersecting non-disability characteristics, such as accented speech, or technology fluency, can further impact data (Whittaker, 2019; Trewin, 2018). Additionally, the same impairment may vary across individuals or change based on age of onset, or over time (Kasnitz, 2012). It is critical to collect data about people from multiple contexts with multiple impairments over multiple timescales, rather than assuming a single fixed experience of disability.
- **Measurement Error** Measurement error can further exacerbate bias (Trewin, 2018). For example, a Fitbit may not recognize wheelchair activity as exercise, a bias in its measure of activity. Guo *et al*. (2019) provide an extensive list of examples for each major class of biometric sensing. Guo *et al. (*2019*)* discuss how facial mobility, emotion expression, and facial structure impact *detection*, *identification*, *verification*, and *analysis* (*e.g.,* emotion analysis)); how body motion and shape impact "body recognition" (*e.g.,* activity detection); handwriting analysis; and speaker analysis.

Addressing bias in biometric data requires assessment methods that can uncover bias. Aggregate metrics can hide performance problems in under-represented groups (Besmira, 2018). Many algorithms maximize these metrics and thus not only fail to recognize bias, but also to address it (Guo, 2019). For example, algorithms that eliminate, or reduce the influence, of outliers are more likely to eliminate disabled people because of the heterogeneity of disability data. Trewin (2018) covers several alternative options for assessment, and highlights *"individual fairness,"* defined as comparing performance (outcomes) between people who are similar, where similarity is defined using metrics that are chosen not to encode bias. For example, movement speed might favor a wheelchair user and exercise variety might favor people who do not have chronic illness; while measures of exertion time might be a similarity metric that covers a wide variety of different types of people. Defining such unbiased metrics requires careful thought and domain knowledge, and scientific research will be essential to defining appropriate procedures for this.

3. Security considerations in making biometric technologies accessible

Biometric systems used by people with disability have all of the same risks as anyone faces regarding data breaches and other aspects of privacy and security [Ritter, 2021]. However, ableism and other biases embedded in society raise additional disability-specific risks.

Privacy and Security. The risk to disabled people of data disclosure can include direct harms such as denial of insurance and medical care, or threaten employment (Whittaker, 2019, p. 21). Any system that can detect disability can also track its progression over time, possibly disclosing disability even before a person knows themselves that they have a diagnosis (or incorrectly labeling someone). Yet this is an uneven flow of information -- the person being labeled may not even know it is happening, or even if they do it may not be voluntary, as suggested by Whittaker et al (*ibid.*). Further, small sample sizes for people with rare disabilities may make data security more difficult. For example, an algorithm may learn to recognize the disability, rather than the individual, reducing security when used for access control, allowing multiple people with similar impairments to access the same data.

Diagnosing, or pathologizing disability or illness. From DNA to voice to gesture and gait, the data biometric systems collect can easily be used to learn about disability. This is not just theory -- for example, Whittaker et al (2019) document how HireVue, an AI based video interviewing company has a patent on file to detect disability (Larsen, 2018), despite the fact that Title I of the Americans with Disabilities Act (ADA) forbids asking about disability status in a hiring process (42 U.S.C. § 12112(a)) and also forbids *"using qualification standards, employment tests or other selection criteria that screen out or tend to screen out an individual with a disability"* (42 U.S.C. § 12112(b)(6)). HireVue's intent is to reduce algorithmic discrimination, however, such information could easily be used, without consent, to deny access to housing, jobs, or education. Disability identification is spreading, including detecting Parkinsons from gait (Das, 2012), and mouse movement (Youngmann, 2019), and detecting autism from home videos (Leblanc, 2020). While disability detection may have value, **the potential for abuse of these tools makes regulation a necessity.**

Further, as Whittaker et al (2019, p. 21) point out, algorithms often define disability entirely in historical medical terms, potentially replicating biases (Bennett, 2020), that then cause a person to go unrecognized and thus to be gatekept out of support systems. This is inconsistent with U.S. Federal law, since the ADA does not require a diagnosis for disability protections, simply that a person be regarded as having a disability (42 U.S.C. § 12101 (a)(1)). The underlying idea is brilliantly progressive, albeit often under attack: **Legally, if you are treated as disabled, you are disabled. Yet biometrics cannot detect how people are treated. Biometrics must never be considered sufficient, nor required as mandatory, for disability identification or service eligibility,** but it will be proposed for both in systems seeking easy answers to complex phenomena.

4. Exhibited and potential harms of a particular biometric technology

Even if accessibility concerns with interfaces to biometrics are addressed, there are numerous additional disability-related risks, including incorrect recognition of faces, fingerprints, and speech; and incorrect inferences about activity and gender (Kane, 2020), raising several severe areas of concern and potential risk which have been laid out in detail in the literature (*e.g.,* Whittaker, 2019).

Defining, or enforcing "normality" based on a biased data set. As Whittaker (2019) argue, norms are baked deeply into algorithms which are designed to learn about the most common cases. As human judgment is increasingly replaced by biometrics, "norms" become

more strictly enforced. There will always be outliers, these outliers will face higher error rates, and they will disproportionately represent and misrepresent people with disability. Resulting errors can impact **allocation of a resource** (Guo, 2019). Biometrics already are being used to track the use and allocation of assistive technologies, from CPAP machines for people with sleep apnea (Araujo 2018) to prosthetic legs (as described by Jullian Wiese in Granta and uncovered in Whittaker et al 2019), deciding who is "compliant enough" to deserve them. Recent changes in California's automating billing procedures for In Home Supported Services require navigating inaccessible phone or online AI verification procedures, further impacting resource access.

Defining, or enforcing what it means to be "human". From government services to education, healthcare, finances (including ATM use) and even basic computer security, access to services today often depends on passing biometric tests. Yet, many biometric systems gatekeep access based on either individual identity, identity as a human, or class of human, such as "old enough to buy cigarettes." When biometric systems are not accessible, they are essentially defining a disabled person as non-human, or not enough of something with respect to the service being denied. Kane (2020) give examples, such as a participant having to falsify data because *"some apps [don't allow] my height/weight combo for my age."* Often, the only solution is to accept reduced digital security, such as the person who must ask a stranger to 'forge' a signature at the grocery store *".. because I can't reach [the tablet]"* (*ibid.*). This is not only inaccessible, it is illegal: kiosks and other technologies such as point-of-sale terminals used in public accommodations are covered under Title III of the ADA, as clearly stated by the U.S. Department of Justice (2014). At work, activity tracking may define "success" in terms that exclude disabled workers. Further, technology may simply fail to recognize that a disabled person is even present (Kane, 2020), a phenomenon they term *invisibility*, because it others and erases people. Such systems amplify existing biases internal to and across othering societal categories (Guo, 2019), reflecting and even enforcing normative categories, thus *"demarcating what it means to be a legible human and whose bodies, actions, and lives fall outside... [and] remapping and calcifying the boundaries of inclusion and marginalization (*Whittaker, 2019). The calcification of such decisions in code risks harm not only in each decision but also through **obscuring the processes for improvement** of such problematic decision making.

Exacerbating or Causing Disability. Whittaker et al (2019) raise concerns about how activity tracking systems may push workers to limits that increase the likelihood of work-related disability, by forcing workers to work at maximal efficiency. Even where accommodations are provided they may have unrecognized time or contextual limitations. Further, biometrics may limit access to critical care resources such as human assistance, resulting in increased risk of hospitalization or institutionalization (Lecher, 2018). These harms are exacerbated when biometric systems, by **removing the human, remove the humane nature of decision making and replace open systems with closed systems**. Such closed systems remove control over the reasons behind decisions and obscure concerns such as whether data is representative or algorithms are erroneous or fair.

5. Exhibited and potential benefits of biometric technology

There are also some disability-specific benefits of biometric technology. For example, biometric technologies can provide opportunities for improved access by replacing a less accessible option. An example is that face recognition may be an easier way to handle phone security than passcode entry for someone who lacks physical dexterity. However, many of the potential benefits of biometrics for disabled domains are dependent upon input from the communities being served. Overlooking disabled peoples' expertise in their own needs risks creating systems that exacerbate harm rather than improving lives.

Behavioral training/support for independence. For example, biometrics have been used in commercial products to recognize affect, gaze, and other behaviors in support of autistic individuals. While marketed for their therapeutic and other benefits, the result can be highly problematic and contribute to contentious, debated practices, rather than contributing to the agency and independence of the target audience [Demo, 2017]. The stakeholders targeted, underlying beliefs guiding the app design and marketing of these apps are all sources of potential harm.

Public safety. People with visible disability can easily be misunderstood and even targeted by both criminals and law enforcement (Trewin, 2019). Biometrics could help to classify behaviors, or re-interpret facial cues, as non-threatening (*ibid.*). However this must be weighed against the potential of increased risk of *misinterpretation* with biased data for training, and the overall risk to society of using biometrics systems for public safety (*ibid.*)

Diagnosis. The potential for biometric technologies to flag a situation that may require medical intervention is well established (Trewin, 2019). However, as stated earlier in the discussion of privacy and security, this brings severe risks as well. For example, Bennett and Keys (2020) provide a case study of a system that uses biometric information to "diagnose" autism, highlighting a number of risks that a naive approach to fairness, which simply examines "*the immediate algorithmic inputs and outputs of the computer vision system,*" cannot rectify. They describe how gender bias in diagnostic methods may be replicated in a diagnostic tool; how diagnosis reinforces the medicalization of the autism; the removal of power from patients; and the lack of consideration of potential harms of diagnosis including financial cost, murder, and social consequences. They conclude by stating: *"we need a model that considers holistic, societal implications, and the way that technologies alter the life chances of those they are used by or on."*

These examples demonstrate the potential for biometrics to contribute positively to the lives of people with disabilities. However this possibility can only be realized through careful application of appropriate and inclusive design methods.

6. Governance programs, practices or procedures

As eloquently stated by Bennett and Keys (2019), rectifying bias through fairness is necessarily an incomplete solution. Fairness cannot rectify structural differences with its reliance on well defined traits and focus on individual identities and goals rather than holistic improvements. Instead, fair biometric systems require a nuanced understanding of

issues surrounding disability justice and the lived experience of disability (Wong, 2020). Further, strong ethical standards have a profound effect on professional work, as evidenced when comparing medicine to fields like AI (Mittlestadt, 2019). Such standards go beyond policy, and developing them must be a priority going forward.

a. Stakeholder Engagement Practices: Changing who builds biometric systems

Appropriate expertise, meaning direct input from the inception to evaluation of a project from the disability community (with appropriate compensation), is critical to successfully addressing bias without introducing new risks and errors into biometric systems. There are *"significant power asymmetries between those with the resources to design and deploy AI systems, and those who are classified, ranked, and assessed by these systems"* (Whittaker, et al, 2019, p. 9). This can improve--but only if we take steps to **ensure that disabled people are included in the design of biometric systems.** Participatory design is a critical way to include people with personal disability expertise (Quintero, 2020). However, true equity will require that people with disabilities can enter the technology workforce so that they can directly build and innovate such systems. This requires access to higher education programs; access to conferences and events where research and products are discussed, presented and shared; and accessible toolkits and development environments including for user interface development, data analysis, and general programming.

In addition, the disability community needs to form a broad coalition and organize itself to impact regulation of biometric systems; prioritization regarding where biometrics would add value; and decisions about data collection. Community representation can not only improve the range and quality of participation in data collection, but may guide the design of data collection systems and prioritization of what data to collect.

b. Best practices for pilots or trials to inform further policy developments

As a general policy rule, algorithms that put a subset of the population at risk should not be deployed. This requires both regulatory intervention and research, at the algorithmic level (*e.g.,* developing better algorithms for handling outliers) and the application level (*e.g.*, studying the risks of harm applications might create for disabled people). Both studies and regulation must take an holistic approach that, rather than being exclusively about technology *"accounts for the context in which such technology is produced and situated, the politics of classification, and the ways in which fluid identities are (mis)reflected and calcified through such technology"* (Whittaker, 2019, p. 11). Regulatory decisions must be informed by analyses that consider all of these factors, to strongly guide industry practice.

Further, accessibility solutions must be directly implemented in existing products: It is well established in the literature that "separate but equal" technological solutions are not equitable, because there is no economic incentive to ensure equality is maintained over time (Lazar, 2015). Accessible options must also be complete and easy to use. Further, both research and regulation must look at biometrics in combinations with each other and with the non-biometric systems they are designed to replace to assess what constitutes an equitable, accessible system. Just as accessible ramps or elevators that are hidden or far away are not considered acceptable for accessibility in physical spaces, truly accessible biometric systems must not create undue burdens in digital spaces nor segregate disabled

users. While a single interface may not be accessible to all people, a single, flexible *system of solutions* with appropriate accessibility support can be.

c. Practices regarding data collection, review, management, storage and monitoring

Park *et al*. (2021a) lay out design guidelines for data collection including how to motivate participants and appropriate pay; what to communicate at data collection time, and how to make sure that data collection infrastructure is accessible. They argue for the need to ethically compensate people for their data; accurately inform people about the estimated time and effort required to provide data (based on trials with people of the targeted group); and to be upfront about risks to privacy (also see [Ritter, 2021]). They also discuss the importance of collecting metadata that does not over simplify disability; and ensuring that disabled peoples' data is not unfairly rejected when minor mistakes occur or due to stringent time limits. Standard methods of data labeling, such as leveraging crowdworkers, have the potential to bake in biases about who is disabled, or what the meaning of disabled biometric data is. Whittaker (2019) discusses the example of clickworkers who label people as disabled "based on a hunch". Badly labeled data has many downstream implications for the quality, and potential negative impact, of biometric systems.

Park et al. (2021a) also advocate for the importance of *accessible data collection processes.* A basic requirement to improve data representation is making sure that data collection systems are accessible to everyone, and ensuring privacy and security of disability information in the specifics of how data is collected (*ibid.*). Similar expectations should be placed on each stage of data review, management, storage and monitoring.

Finally, it is important to ensure proper documentation. Abbott et al (2019) lay out guidelines for documentation and data security. Data management is a complex domain with many risks. While these concerns are universal, taking disability into account means ensuring that solutions to each of these challenges are accessible and open.

d-f. Safeguards or limitations regarding approved use and mechanisms for preventing unapproved use; Performance auditing and post-deployment impact assessment; and Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);

At a basic level, just as websites are required to be accessible, so should algorithms. The W3C guidelines provide insight into website accessibility, but a similar set of expectations does not currently exist for biometrics. It is critical that we establish a basic set of expectations around how such algorithms are assessed for their accessibility. This should help to address **basic access constraints**, reduce the types of errors that **enforce "normality"** rather than honoring heterogeneity, and eliminate errors that gatekeep who is **"human".**

Finally, as Ritter [2021] argues, consumer consent, and oversight around best practices, are both essential to fair use. Further, biometric systems should be interpretable and correctable, meaning that they can be overridden by a person based on their human judgment about a situation. There should be particularly strong consequences when algorithms which are used to detect disability, or make decisions about access to services

on the basis of disability, lack these properties. The potential consequences of errors made by these algorithms to health, safety, and participation in society are too severe to ignore.

g-h. Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems and Practices for public transparency regarding: use, impacts, opportunities for contestation and for redress, as appropriate.

From how data is collected to how it is labeled to how it is used, it is critical that all stakeholders can participate in and understand their representation in biometric data. This requires that the data collection process be accessible, and that there is transparency about and documentation of what is collected and how it is used (Trewin, 2018). Transparency is critical to ensuring that all people can make safe and informed decisions about what services to use and when to take care or explore alternatives. It also incentivizes improvements in service quality. Further, transparency is critical to ensure that the rights of disabled people are enforceable in the court system (Whittaker, 2019, p. 17). Finally, as stakeholders with the same range of intelligence and commitment as anyone else, people considered and identifying themselves as disabled need to be in leadership positions. The slogan "Nothing about us without us" is not just memorable, but is how a just society works (Charlton, 1998).

References

[ADA] U.S. Department of Justice, Civil Rights Division. The Americans with Disabilities Act (ADA).

[Abbott, 2019] Abbott, Jacob, et al. Local standards for anonymization practices in health, wellness, accessibility, and aging research at CHI. ACM *CHI* 2019.

[Araujo 2018] Araujo, M., et al. MI approach for early detection of sleep apnea treatment abandonment: A case study. In the International Conference on Digital Health (pp. 75-79).

[Bennett 2020] Bennett, C., & Keyes, O. What is the point of fairness?. Interactions, 27(3), 35-39.

[Besmira, 2018] Nushi, B., et al. Towards accountable ai: Hybrid human-machine analyses for characterizing system failure. In *AAAI CHCC* 2018.

[Charlton, 1998] Charlton, James I. *Nothing about us without us*. University of California Press.

[DOJ 2014] United States Department of Justice, Statement of Interest in the New v. Lucky Brand Jeans (Apr. 10, 2014).

[Das 2012] Das, S., et al. Detecting Parkinsons' symptoms in uncontrolled home environments: A multiple instance learning approach. In IEEE Engineering in Medicine and Biology Society (pp. 3688-3691). IEEE.

[Demo, 2017] Demo, A. T. Hacking agency: Apps, autism, and neurodiversity. *Quarterly Journal of Speech*, *103*(3), 277-300.

[Guo, 2019] Guo, A., et al. Toward fairness in AI for people with disabilities: A research roadmap. ACM SIGACCESS Accessibility and Computing, (125), 1-1.

[Iwama, 2012] Iwama, Haruyuki, et al. The ou-isir gait database comprising the large population dataset and performance evaluation of gait recognition. In IEEE Transactions on Information Forensics and Security 7.5 (2012): 1511-1521.

[Kane, 2020] Kane, S. K., et al. Sense and accessibility: Understanding people with physical disabilities' experiences with sensing systems. In *ACM ASSETS*. 2020.

[Kasnitz, 2012] Kasnitz, D., & Block, P. (2012). Participation, time, effort and speech disability justice. Chapter 14, *Politics of occupation-centred practice: Reflections on occupational engagement across cultures*, Nick Pollard and Dikaios Sakellariou, Ed.John Wiley & Sons, Ltd.

[Larsen 2018] Loren Larsen, Keith Warnick, Lindsey Zuloaga, and Caleb Rottman, "Detecting Disability and Ensuring Fairness in Automated Scoring of Video Interviews," United States Patent Application Publication, August 20, 2018. Unearthed by AI Now Tech Fellow Genevieve Fried.

[Lazar, 2015] Lazar, J., et al. The discriminatory impact of digital inaccessibility. Chapter 3, *Ensuring Digital Accessibility Through Process and Policy.* Waltham, MA: Elsevier/Morgan Kaufmann Publishers.

[Leblanc 2020] Leblanc, E., et al. Feature replacement methods enable reliable home video analysis for machine learning detection of autism. Scientific reports, 10(1), 1-11.

[Lecher, 2018] Lecher, C. What happens when an algorithm cuts your health care, The Verge, 3/21/18

[Mittelstadt, 2019] Mittelstadt, B. Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 501-507.

[Oliver, 2013] Mike Oliver. The social model of disability: Thirty years on. *Disability & society* 28(7):1024–1026.

[Park, 2021a] Park, J. S., et al. Designing an Online Infrastructure for Collecting AI Data From People With Disabilities. In the *ACM Conference on Fairness, Accountability, and Transparency* (pp. 52-63).

[Park, 2021b] Park, Joon Sung, et al. Understanding the Representation and Representativeness of Age in AI Data Sets. *arXiv preprint arXiv:2103.09058* (2021).

[Quintero, 2020] Quintero, Christian. A review: accessible technology through participatory design. *Disability and Rehabilitation: Assistive Technology* (2020): 1-7.

[Ritter, 2021] Ritter, E. Your Voice Gave You Away: the Privacy Risks of Voice-Inferred Information. Duke Law Journal, 71(3), 735-771.

[Taati, 2019] Taati, Babak, et al. Algorithmic bias in clinical populations—evaluating and improving facial analysis technology in older adults with dementia. IEEE Access 7 (2019): 25527-25534.

[Trewin 2018] Trewin, S. (2018). AI fairness for people with disabilities: Point of view. *arXiv preprint arXiv:1811.10670*. Also a blog post.

[Trewin, 2019] Trewin, S., et al. Considerations for AI fairness for people with disabilities. *AI Matters*, *5*(3), 40-63.

[UN 2007] UN General Assembly. (2007). Convention on the Rights of Persons with Disabilities: resolution / adopted by the General Assembly, 24 January 2007, A/RES/61/106. Retrieved Dec 2021.

[Whittaker 2019] Whittaker, M. et al. (2019). Disability, bias, and AI. *AI Now Institute*.

[Wolf, 2019] Wolf, Christine T., and Ringland, K. E. Designing accessible, explainable AI (XAI) experiences. *ACM SIGACCESS Accessibility and Computing* 125 (2019): 1-1.

[Wong, 2020] Wong, Alice, ed. *Disability visibility: First-person stories from the twenty-first century*. Vintage, 2020.

[Youngmann 2019] Youngmann, B., et al. A machine learning algorithm successfully screens for Parkinson's in web users. *Annals of clinical and translational neurology*, 6(12), 2503-2509.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Center on Privacy &
Technology at Georgetown Law

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

GEORGETOWN LAW
Center on Privacy & Technology

January 15, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

VIA EMAIL
BiometricRFI@ostp.eop.gov

Re: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies — Comments of Center on Privacy & Technology at Georgetown Law

The Center on Privacy & Technology at Georgetown Law (the "Center") welcomes this Office of Science and Technology Policy (OSTP) proceeding on public and private sector uses of biometric technologies. The Center is a law and research think tank that focuses on the privacy rights and surveillance of historically marginalized communities. Our track record includes rigorous, long-term research and groundbreaking legal and policy analysis and advocacy, resulting in state and federal legal reforms to protect privacy and civil rights.[1]

This submission focuses on the use of biometric surveillance technologies by private sector employers on low-wage workers across the United States.[2] Part I responds to Topic 1 of the RFI ("Descriptions of use of biometric information for recognition and inference"), with an overview and examples of biometric worker surveillance in various industries.

Part II responds to Topic 4 ("Exhibited and potential harms of a particular biometric technology"), by situating biometric worker surveillance in critical historical context to inform harms analysis. This section traces biometric surveillance technologies back to 20th-century Taylorism and Fordism, and connects them to surveillance of Black bodies as originating in the transatlantic slave trade and plantation slavery, drawing on the scholarship of Simone Browne.

Part III responds to Topic 6 ("Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case"), by setting out the implications of Part II for legal and policy reform to address biometric surveillance technologies as used on low-wage workers and intersecting marginalized groups.

---

1 "Our Work," Center on Privacy & Technology, Georgetown Law, https://www.law.georgetown.edu/privacy-technology-center/our-work/.

2 For use of biometric technologies in the public sector, we refer the OSTP to the Center's previous work on use of facial recognition technologies by law enforcement in the contexts of the criminal legal system and national security. See e.g., Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology at Georgetown Law (October 18, 2016), https://www.perpetuallineup.org/; Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Center on Privacy & Technology at Georgetown Law (May 16, 2019), https://www.flawedfacedata.com/; Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Center on Privacy & Technology at Georgetown Law (May 16, 2019), https://www.americaunderwatch.com/; and Harrison Rudolph, Laura M. Moy & Alvaro M. Bedoya, *Not Ready for Takeoff: Face Scans at Airport Departure Gates*, Center on Privacy & Technology at Georgetown Law (December 21, 2017), https://www.airportfacescans.com/.

I. Biometric Surveillance of Low-Wage Workers Is Proliferating (*RFI Topic 1*)

Biometric worker surveillance technologies make up a rapidly proliferating industry, as a subset of thousands of little known commercial vendors, business intelligence firms, start-ups, and apps that "are used in all aspects of labor, hiring, workplace and workforce management, gig economy, benefits, and more."[3] Coworker.org has deemed this group of workplace technology products and services "Little Tech"—in contrast to their household-name counterparts—and in a recent study of over 550 such products,[4] nearly one-third "emerged between 2020-2021; the rest were developed between 2018 and 2020."[5]

Biometric surveillance of workers while they are on the job is often used for generating inferences about their physical, physiological, mental, emotional, and social or relational states at any given moment, with a view to extracting as much efficiency and productivity from the monitored workers as possible.[6] Examples include:

- Ford workers donning "skin-tight bodysuits" that contain 15 motion-tracking wireless sensors to monitor the wearer's body as a posture and productivity aid;[7]
- Oracle and Thomson Reuters developing "intrusive and sophisticated workplace monitoring systems that are expanding the collection of vulnerable worker data such as sentiment, heart rate, blood pressure, and mental health status";[8]
- Microsoft Wellness Insights collecting workers' biometric data such as heart rate and blood pressure as part of providing "wellness recommendations";[9]
- Humanyze's "Sociometric Badge", which places on workers two microphones, an infrared sensor, and an accelerometer, to "determine when employees are interacting, … analyze the tones of employees' voices, [and] determine which employees are interacting, where, for how long, and with what general type of emotional valence";[10]
- Focus UX, by SAP and EMOTIV (a provider of "mobile neuroinformatics solutions"), which purports to detect a worker's "cognitive state and then adapt the user experience… to best fit what [the worker] can handle at that moment," while providing "personalized feedback on their cognitive performance and needs";[11] and
- Amazon's biometric surveillance of its warehouse workers and delivery drivers, including installing in all delivery vehicles four-lens "AI-powered" cameras by

---

3 Wilneida Negrón, *Little Tech Is Coming for Workers: A Framework for Reclaiming and Building Worker Power*, Coworker.org (2021), https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf at 19, 21.

4 See generally *Ibid.* and "Bossware and Employment Tech Database," Coworker.org (November 2021), https://home.coworker.org/worktech/.

5 Negrón, *supra* note 3 at 24.

6 This submission will focus on the use of biometric surveillance technologies for the purpose of generating inferences about workers, as opposed to for identification or recognition purposes.

7 "Ford looks to motion tracking bodysuits to aid factory workers," Internet of Business (August 6, 2018), https://internetofbusiness.com/ford-motion-tracking-bodysuits/.

8 Negrón, *supra* note 3 at 20.

9 *Ibid*., at 67.

10 Matthew T Bodie et al, *The Law and Policy of People Analytics*, 88 University of Colorado Law Review 961 (2017) at 971; and Katherine Noyes, "Startup Humanyze's 'people analytics' wants to transform your workplace," *Computer World* (November 20, 2015), https://www.computerworld.com/article/3006631/startup-humanyzes-people-analytics-wants-to-transform-your-workplace.html. See also Ivan Manokha, *The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace*, 18:4 Surveillance & Society 540 (2020) at 545 for a similar product from "Boston-based analytics firm Sociometric Solutions."

11 Maricel Cabahug, "Adaptive Assistance for Improved Well-Being and Productivity at Work," SAP (October 12, 2018), https://news.sap.com/2018/10/sap-emotiv-adaptive-assistance-well-being-productivity-work/.

> Netradyne, which reportedly can "sense when a driver yawns, appears distracted, or isn't wearing a seatbelt … and monitor drivers' body and facial movements."[12]

Researchers and reporters have also identified potential future applications of biometric surveillance of workers through technology companies' patent filings, including:

- an Uber patent for predictive risk assessment algorithms to determine if a driver is "safe", which involves generating a "safety score based on how carefully they drive ('vehicle operation') and how they interact with passengers ('interpersonal behavior')";[13]
- a Walmart patent for "sound sensors" that would record and analyze conversations between workers and customers, including "how employees greet customers," and evaluate workers based on generated "performance metrics";[14]
- an Amazon patent representing the "automation of relational labor", which uses "imaging and spatial sensors" to "capture [a worker's] position in space, movements, or facial expressions" as they walk through a warehouse to "detect frustration rather than boredom" and potentially alert a supervisor or trigger automated assistance;[15] and
- another Amazon patent for "a wristband that can precisely track where warehouse employees are placing their hands and use vibrations to nudge them in a different direction", using ultrasonic tracking and a haptic feedback system."[16]

As the above examples demonstrate, emerging workplace technologies are a "key driver in the commodification of low-wage workers' data" and worker surveillance,[17] with "next generation" productivity tools "expand[ing] employment and labor organizing surveillance in order to mine more data from low-wage workers."[18] Such tools increasingly include biometric surveillance capabilities, such as "facial recognition technology,… more intrusive data collection inside and outside the workplace, increasingly more sensitive data collected about workers (medical, sentiment, stress levels, cognitive functioning, etc.), and real-time monitoring of workers."[19]

In addition, the growing availability and accessibility of biometric worker surveillance tools means that granular worker monitoring and algorithmic management capabilities are no longer necessarily limited to large corporations or deep-pocketed employers. A prominent proponent of so-called "people analytics," Humanyze's co-founder Ben Waber, called this type of technology "'management in a box' for small business."[20] In fact, Coworker.org's *Little Tech* study found "an ongoing digitization of small business and working class industries such as auto repair (ShopMonkey), plumbing and electricians (ServiceTitan), beauty salons

---

12 Lauren Kaori Gurley, "Amazon Delivery Drivers Forced to Sign 'Biometric Consent' Form or Lose Job," *Vice Motherboard* (March 23, 2021), https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job.

13 Belle Lin, "Uber Patents Reveal Experiments with Predictive Algorithms to Identify Risky Drivers," *Intercept* (October 30, 2021), https://theintercept.com/2021/10/30/uber-patent-driver-risk-algorithms. Given the myriad known harms of algorithmic discrimination, it is already concerning that one patent involving machine learning and rider feedback "suggests a driver's 'heavy accent' corresponds to 'low quality' service."

14 Jason Silverstein, "Walmart patents audio surveillance technology to record customers and employees," *CBS News* (July 13, 2018), https://www.cbsnews.com/news/walmart-patents-audio-surveillance-technology-to-record-customers-and-employees/.

15 Alessandro Delfanti & Bronwyn Frey, *Humanly Extended Automation or the Future of Work Seen through Amazon Patents*, 46:3 Science, Technology, & Human Values 655 (2020) at 671.

16 Olivia Solon, "Amazon patents wristband that tracks warehouse workers' movements," *Guardian* (January 31, 2018), https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking.

17 Negrón, *supra* note 3 at 32.

18 *Ibid*., at 61.

19 *Ibid*.

20 Jeremias Addams-Prassl, *What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, 41 Comparative Labor Law & Policy Journal 123 (2019) at 131.

(GlossGenius) and barbershops (Squire) … which will bring the data collection and processing to the hyperlocal level and to more sectors of the job markets."[21] What this means for lawmakers and policymakers is that typical legislative exemptions for small and medium enterprises in previous bills aimed at "Big Tech"-related issues may be less appropriate when it comes to protecting workers from invasive surveillance and detrimental uses of their data.[22]

Biometric worker surveillance, as a type of data-driven workplace technology, disproportionately impacts and harms low-wage workers who are also members of other historically marginalized groups, such as Black, Brown, and Indigenous workers; female and gender-diverse workers; workers with disabilities; and migrant workers.[23] This may be due to the demographics of the workforce in industries that are more likely to deploy biometric surveillance and automated management technologies on their workers, such as call centers, warehouses, home care, and hospitality.[24] The consequences for these workers, where surveillance feeds into algorithmic management systems, are compounded by the independently existing set of civil rights harms associated with data bias, algorithmic discrimination, and algorithmic decision systems across the board.[25] Thus, workers' rights are intertwined with civil rights, a dynamic on which Part II will elaborate.

II. Situating Biometric Worker Surveillance in Historical Context (*RFI Topic 4*)

The harms of biometric worker surveillance, and related technologies such as algorithmic management and other forms of worker surveillance, have been and continue to be well documented.[26] Instead of repeating them here, the following subsections provide a historical lens that lawmakers, regulators, employers, and technology vendors should apply when it

---

21 Negrón, *supra* note 3 at 62.

22 *Ibid*., at 43.

23 Annette Bernhardt, Lisa Kresge & Reem Suleiman, *Data and Algorithms at Work: The Case for Worker Technology Rights*, UC Berkeley Labor Center (November 2021), https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf, at 15.

24 See e.g., *Ibid*., at 6-14; Katherine Anne Long, "New Amazon data shows Black, Latino and female employees are underrepresented in best-paid jobs," *Seattle Times* (April 14, 2021), https://www.seattletimes.com/business/amazon/new-amazon-data-shows-black-latino-and-female-employees-are-underrepresented-in-best-paid-jobs; and Alexandra Mateescu, *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, Data & Society (November 2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf at 31.

25 See e.g., Ian Weiner, "Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce," Lawyers' Committee for Civil Rights Under Law (August 4, 2021), https://www.lawyerscommittee.org/federal-trade-commission-must-protect-civil-rights-privacy-in-online-commerce/.

26 See e.g., generally, Negrón, *supra* note 3; Bernhardt, Kresge & Suleiman, *supra* note 23; Alexandra Mateescu & Aiha Nguyen, *Explainer: Workplace Monitoring & Surveillance*, Data & Society (February 2019), https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf; Matt Scherer, *Warning: Bossware May Be Hazardous to Your Health*, Center for Democracy & Technology (July 2021), https://cdt.org/wp-content/uploads/2021/07/2021-07-29-Warning-Bossware-May-Be-Hazardous-To-Your-Health-Final.pdf; Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 California Law Review 735; Athena, "Put Workers over Profits: End Worker Surveillance," Open Letter (October 14, 2020), https://athenaforall.medium.com/end-worker-surveillance-d99aa7cd3850; Irene Tung, Maya Pinto & Debbie Berkowitz, *Injuries, Dead-End Jobs, and Racial Inequity in Amazon's Minnesota Operations*, National Employment Law Project (December 2021), https://s27147.pcdn.co/wp-content/uploads/Report-Injuries-Dead-End-Jobs-and-Racial-Inequity-in-Amazons-Minnesota-Operations-.pdf; Daniel A Hanley & Sally Hubbard, *Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power*, Open Markets Institute (September 2020), https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf; and Kathryn Zickuhr, *Workplace surveillance is becoming the new normal for U.S. workers*, Washington Center for Equitable Growth (August 2021), https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers.

comes to assessing the demonstrated and potential harms of biometric surveillance, to ensure that such harms are placed in their full historical context and given appropriate weight.

II.A. Taylorism, Fordism, and Foucauldian Biopower

Today's biometric worker surveillance technologies are not new or innovative, but are a more powerful iteration of long existing ideologies and systems implemented to manage and control workers—specifically, the 20th-century strategies of Taylorism and Fordism.[27] This section will discuss how biometric worker surveillance facilitates contemporary and more thorough executions of these two management systems, further enabling mass transfer of political power away from already largely disenfranchised workers,[28] in part through the phenomenon of "biopower" as conceptualized by Michel Foucault.

Many scholars and experts at the intersection of worker rights and technology studies have pointed out that present-day systems of worker surveillance and algorithmic management amount to a continuation and further fulfillment of Frederick Taylor's tenets for organizing a workplace, as set out in his *Principles of Scientific Management*.[29] This can be seen in examples such as Amazon's scanners and biometric cameras; UPSs' telematics; rideshare and food delivery apps' worker algorithmic route and price management; and all of their respective ongoing data collection from and granular directives to workers. As Laura Nurski points out, Taylor's treatise "reads like a twenty-first century guide to data-driven management: data collection and process analysis, efficiency and standardisation, and knowledge transfer from workers into tools, processes and documentation. … With the rise of workplace AI, Taylor's dream of perfectly optimised work processes might finally become a reality."[30]

In fact, reality may be on track to overshoot Taylor's dream. One study that analyzed Amazon's patent filings concluded that the future logical endpoint of their proposed technologies is a "workplace in which human operators serve machines rather than vice versa."[31] Not only that, but the machines would be subjected to their own form of Taylorism, where their processes and any corrective aid provided by human workers would be continually monitored, and both the biometric and cybernetic data is "fed back to digital machinery to improve its performance."[32] In this ultimate scenario, deemed "humanly extended automation," data is harnessed to

---

27 "The surveillance of workers is not a new phenomenon in the United States. In the 1800s, 'the Pinkertons' worked on behalf of employers, infiltrating and busting unions, enforcing company rules, and monitoring workers deemed to be a threat. … [T]he advent of Taylorism in the early twentieth century inspired Henry Ford to surveil the factory floor with a stop watch and to institute the Sociological Department, which was a team of detectives hired to monitor the private lives of his workers. In recent years, technological innovations, both digital and otherwise, have become the primary tools of employee monitoring." Ifeoma Ajunwa, *Protecting Workers' Civil Rights In The Digital Age*, 21 North Carolina Journal of Law & Technology 1 (2020) at 22-23.

28 "Scientific management, for all its pretensions, was less about determining ideal working methods and more about shattering this tremendous source of worker power… The modernizing terminology of 'science' and "efficiency" masked the prerogatives of discipline and control of workers." GAVIN MUELLER, BREAKING THINGS AT WORK: THE LUDDITES WERE RIGHT ABOUT WHY YOU HATE YOUR JOB (2021) at 33.

29 See e.g., Delfanti & Frey, *supra* note 15 at 659, 665-66; Manokha, *supra* note 10 at 543; Bodie et al, *supra* note 10 at 964; Erica Pedersen, *People Analytics and Individual Autonomy: Employing Predictive Algorithms as Omniscient Gatekeepers in the Digital Age Workplace*, Columbia Business Law Review 1122 (2020) at 1129-30; Alex Rosenblat, Tamara Kneese & danah boyd, "Workplace Surveillance," Data & Society Working Paper, Data & Society (October 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2536605; and Katherine C Kellogg, Melissa A Valentine & Angèle Christin, *Algorithms at Work: The New Contested Terrain of Control*, 14:1 Academy of Management Annals 366 (2020).

30 Laura Nurski, "Algorithmic management is the past, not the future of work," *Bruegel* (May 6, 2021), https://www.bruegel.org/2021/05/algorithmic-management-is-the-past-not-the-future-of-work/.

31 Delfanti & Frey, *supra* note 15 at 675.

32 *Ibid*., at 660.

optimize the *machines'* performance,[33] as workplace technologies have by then relegated humans to little more than "living labor operat[ing] as a new kind of appendage of machinery, making up for its shortages."[34] Such a potential outcome, even if Amazon and other employers end up falling short of it, highlights more starkly the need to ensure a "just transition"[35] for workers in the event of their workplaces, duties, or managers becoming automated.

Fordism, emerging from the mass production factories of Henry Ford, built on and extended Taylorism and included the additional element of worker surveillance for adherence to behavioral and lifestyle dictates even outside of work.[36] This too is mirrored in present-day biometric surveillance of workers, only instead of Sociology Department inspectors knocking on doors, human resources departments hand out wearable fitness devices and enroll workers in digitally monitored "wellness programs", some of which are mandatory or include penalties for non-compliance.[37] As a result, employers now "combine Taylorism's workers-as-inputs mindset with Fordism's pervasive intrusion into employees personal lives, and wield this data to algorithmically maximize organizational profit."[38]

Furthermore, this web of demands, pressures, and incentives, all of which are tied to workers' bodies in one or more ways, gives rise to what some scholars have noted is a 21st-century privatization and enactment of Foucauldian "biopower."[39] Biopower refers to the process by which the individual's body, through norms, standards, and implicit or explicit requirements placed upon it (for instance, what is considered "healthy"), becomes a tool of social ordering and political control, "mark[ing] the inscription of the biological into the political."[40] "Privatization" has occurred because biopower is now in the hands of private sector employers—especially where biometric surveillance is in use—whereas in Foucault's original formulation, it was primarily a tool of the state.[41] One core aspect of biopower is that, like Jeremy Bentham's Panopticon,[42] it instils a "disciplinary power",[43] including self-discipline in

---

33 *Ibid*., at 661.

34 *Ibid*., at 675.

35 The term "just transition" is taken from the climate justice context, where the term means "greening the economy in a way that is as fair and inclusive as possible to everyone concerned, creating decent work opportunities and leaving no one behind" (such as workers whose livelihoods currently depend on the fossil fuel industries). "Frequently Asked Questions on Just Transition," International Labour Organization (2022), https://www.ilo.org/global/topics/green-jobs/WCMS_824102/lang--en/index.htm.

36 "Ford … endeavored to shape his employees' lives by managing off-duty habits that might affect their performance. He created a 'Sociological Department' to address the problems of boredom, absenteeism, and turnover amongst Ford workers. The Department deployed a team of 150 to investigate the lifestyle of each Ford employee and their personal vices…" Bodie et al, *supra* note 10 at 966 (citations omitted).

37 Ifeoma Ajunwa, Kate Crawford & Joel S Ford, *Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs*, 44 Journal of Law, Medicine & Ethics 474 (2016).

38 Pedersen, *supra* note 29 at 1132.

39 Manokha, *supra* note 10 at 548.

40 François-Xavier de Vaujany et al, *Control and Surveillance in Work Practice: Cultivating Paradox in 'New' Modes of Organizing*, 42:5 Organization Studies 675 (2021) at 683.

41 In this respect, it is important to note Simone Browne's observation here on Foucault and biopower: "While Foucault argued that the decline of the spectacle of public torture as punishment might have marked 'a slackening of the hold on the body,' this chapter contends that when that body is black, the grip hardly loosened during slavery and continued post-Emancipation with, for example, the mob violence of lynching and other acts of racial terrorism." SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015) at 37.

42 "[F]or workers placed under digital surveillance, the three main assumptions behind the panopticon are now increasingly fulfilled: the omnipresence of the employer is ensured by the digital gathering and storage of all information concerning productivity; their universal visibility is guaranteed by the fact that everything that they do, including the organization of their lunch or toilet breaks, may be monitored; and, as a result, workers must assume that they are constantly observed." Manokha, *supra* note 10 at 547.

43 *Ibid*., at 547.

particular.[44] Under this self-disciplinary power, workers feel constant pressure, regardless of formal work requirements or official policies, "to perform better, to beat the targets, to outperform team members,"[45]—or to skip legally required breaks, pee in water bottles, run into traffic, sustain chronic injuries, or forego legally protected accommodations.[46] Legislation or regulation to address biometric surveillance of workers should take these forms of overt and tacit control into account, so that employers creating technology-facilitated Taylorist or Fordist workplaces cannot circumvent fair labor standards or other labor and employment laws.

Lawmakers and regulators should also recognize that intervention to protect workers' rights and well-being from employers' adoption of surveillance and algorithmic technologies is urgently needed now. This recommendation arises from noting some of the key forces that led to the eventual undermining of Taylorism and to Ford shutting down his Sociological Department: high costs of worker surveillance at and outside of work;[47] the company head (Ford) considering that "prying into employees' private concerns is out of date";[48] Congressional willingness and ability to act in favor of impacted workers at the expense of large employers;[49] and workers' ability to organize away from the technologically enhanced eyes and ears of their employers. These circumstances mostly do not exist today. Thus, workers are being subjected to a strengthened version of Taylorism and Fordism combined, using biometric and other forms of surveillance and algorithmic technologies, while thanks to these same technologies, workers are simultaneously restricted in their ability to resist or oppose such developments, relative to their historical counterparts. The law must step in.

II.B. Slavery, Biometric Surveillance, and Racial Capitalism

Biometric worker surveillance is inherently a racial justice issue. This intrinsic connection is demonstrated in the foundational work of Black feminist surveillance studies scholar Simone Browne, who locates the origins of biometric surveillance not in Ford's factories, nor in Bentham's Panopticon,[50] but on transatlantic slave ships and colonial plantations.[51] To be clear at the outset: 21st-century workers are not slaves, and suggesting any equivalency would

---

44 See also: "People who are subject to such monitoring are also tasked with actively participating in their own confinement by partnering, in a way, with the overseeing body or agency in the check for violations and infractions." BROWNE, *supra* note 41 at 16.

45 Manokha, *supra* note 10 at 548.

46 See e.g., Lauren Kaori Gurley, "Amazon Denies Workers Pee in Bottles. Here Are the Pee Bottles," *Vice Motherboard* (March 25, 2021), https://www.vice.com/en/article/k7amyn/amazon-denies-workers-pee-in-bottles-here-are-the-pee-bottles; Jodi Kantor, Karen Weise & Grace Ashford, "Inside Amazon's Worst Human Resources Problem," *New York Times* (October 24, 2021), https://www.nytimes.com/2021/10/24/technology/amazon-employee-leave-errors.html; Lauren Kaori Gurley, "Amazon's Cost Saving Routing Algorithm Makes Drivers Walk Into Traffic," *Vice Motherboard* (June 2, 2021), https://www.vice.com/en/article/5db95k/amazons-cost-saving-routing-algorithm-makes-drivers-walk-into-traffic; and Will Evans, "Ruthless Quotas at Amazon are Maiming Employees," *Atlantic* (November 25, 2019), https://www.theatlantic.com/technology/archive/2019/11/amazon-warehouse-reports-show-worker-injuries/602530/.

47 Addams-Prassl, *supra* note 20 at 130 & 146 ("One of the reasons why Taylorism failed was the high transaction cost involved in monitoring and measuring each individual worker's performance. With algorithmic management, the marginal monitoring costs for additional employees are minimal.")

48 Bodie et al, *supra* note 10 at 966.

49 MUELLER, *supra* note 28 at 35.

50 "It turns out Bentham travelled on a ship transporting slaves during the trip where he sketched out the Panopticon… [Browne] asks how 'the view from "under the hatches"' of Bentham's Turkish ship … might change our narrative about the emergence of disciplinary power and the modern management of life as a resource." Daniel Greene, "Digital Dark Matters," *b2o* (December 14, 2016), https://www.boundary2.org/2016/12/digital-dark-matters/.

51 "The historical formation of surveillance is not outside of the historical formation of slavery. Using narratives of ex-slaves, runaway slave advertisements, the census, and a set of plantation rules as primary source data, what follows is a historicizing of [key surveillance studies concepts and issues]." BROWNE, *supra* note 41 at 50.

constitute reprehensible co-optation and trivialization. The purpose of this section is to demonstrate how surveillance of labor is historically tied to surveillance of Blackness.[52]

To start, Browne's historical research and analysis establishes early examples of surveillance technologies used to categorize, control, commodify, and dehumanize Black bodies, such as:[53]

- the plan of the slave ship as the precursor of prisons, displacing and complicating the Panopticon's central role in surveillance studies,[54] and which Browne asserts should equally be "understood as an operation of the power of modernity, and as part of the violent regulation of blackness";[55]
- lantern laws in 18th-century New York City, which required Black, Indigenous, and mixed-race slaves "to carry small lamps, if in the streets after dark and unescorted by a white person"[56] — under such laws, the lantern became "a technology that made it possible for the black body to be constantly illuminated from dusk to dawn, made knowable, locatable, and contained … a supervisory device that sought to render those who could be, or were always and already, criminalized by this legal framework as outside of the category of the human and as un-visible";[57]
- the physical branding of slaves, which according to Browne "played a key role in the historical formation of surveillance"[58] and was a "biometric technology, as it was a measure of slavery's making, marking, and marketing of the black subject as commodity"[59]; and
- public advertisements for runaway slaves, which "were not only about ascribing physical details to the runaway, but also offered the slave owner's assessment of the fugitive's character"[60]—bringing to mind so-called predictive algorithms that purport to use biometrics to infer someone's likelihood of "criminality,"[61] or to determine and assess a job candidate's or employee's character for likelihood of "success" within the company, or for predisposition to unionization or collective organizing.[62]

Thus, "rather than seeing surveillance as something inaugurated by new technologies, … to see it as ongoing is to insist that we factor in how racism and antiblackness undergird and sustain the intersecting surveillances of our present order"[63]—including the present order of low-wage employment, gig work, and other types of labor increasingly governed by "Little Tech."

Surveillance of slaves as a function of anti-Black racism marks the beginning of racial justice and socioeconomic justice being inseparable, including in the context of biometric worker

---

52 "Surveillance is nothing new to black folks. It is the fact of antiblackness." *Ibid.*, at 10.

53 "[B]iometric information technology—as a measure of the black body—has a long history in the technologies of slavery that sought to govern black people on the move, notably those technologies concerned with escape." *Ibid.*, at 25.

54 *Ibid.*, at 42.

55 *Ibid.*, at 22.

56 *Ibid.*, at 24.

57 *Ibid.*, at 79.

58 *Ibid.*, at 91.

59 *Ibid.* "Current biometric technologies and slave branding, of course, are not one and the same; however, when we think of our contemporary moment when 'suspect' citizens, trusted travelers, prisoners, welfare recipients, and others are having their bodies informationalized by way of biometric surveillance, … we can find histories of these accountings of the body in [primary sources associated with slavery, as detailed in the book]." *Ibid.*, at 128.

60 *Ibid.*, at 54.

61 Coalition for Critical Technology, "Abolish the #TechToPrisonPipeline," Open Letter (June 22, 2020), https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16.

62 See e.g., Jay Peters, "Whole Foods is reportedly using a heat map to track stores at risk of unionization," *Verge* (April 20, 2020), https://www.theverge.com/2020/4/20/21228324/amazon-whole-foods-unionization-heat-map-union.

63 BROWNE, *supra* note 41 at 8.

surveillance. In other words, "[c]apitalism has always, as Browne's notes on plantation surveillance make clear, been racial capitalism."[64] Tracing biometric worker surveillance and algorithmic management back to Taylor and Ford only reveals half the picture,[65] when they were long pre-empted by "a set of rules from the 1800s for the management of slaves on an East Texas plantation,"[66] and slave management methods on plantations in general.[67] Such methods included—with clear present-day echoes—data collection (such as tracking missing tools or weapons) "to anticipate rebellion"; regulating "slave diets and clothing"; and enforcing quotas of how much cotton to pick per day, with missed quotas resulting in physical punishment, while exceeding one's quota could result in a permanently raised "picking rate."[68]

To reiterate, drawing the parallels above is not to equate present-day low-wage employment with chattel slavery.[69] The point is to situate technology-related workers' rights issues in their full historical context, [70] which includes the history of slavery and racial injustice, and how such a national legacy impacts intersecting forms of injustice (such as socioeconomic) to this day.[71]

III. Protecting Workers by Centering Racial and Socioeconomic Justice (*RFI Topic 6*)

The historical legacies outlined above in Part II raise at least two overarching implications for lawmaking and regulation of biometric surveillance technologies and their use on low-wage workers, alongside related data-driven systems such as algorithmic management tools.

First, accurately assessing and weighing the harms of biometric surveillance technologies, particularly in the case of historically marginalized groups, must integrate "a critical biometric consciousness." This requires "acknowledg[ing] the connections between contemporary biometric information technologies and their historical antecedents,"[72] and "understand[ing] the histories and the social relations that form part of the very conditions that enable these technologies."[73] Biometric surveillance comes with historical and "racial baggage,"[74] and that is a weight that should not be (further) placed on the lives of historically marginalized people.

Second, "[w]hen designing policy and regulatory interventions, we must center America's legacy of racial capitalism."[75] In part, this involves recognizing that for Black, Brown, and Indigenous workers, as well as migrant workers, it is not only private sector employers who

---

64 Greene, *supra* note 50.

65 "It's a more comforting origin story, one that protects the idea that America's economic ascendancy developed not because of, but in spite of, millions of black people toiling on plantations. But management techniques used by 19th-century corporations were implemented during the previous century by plantation owners." Matthew Desmond, "In order to understand the brutality of American capitalism, you have to start on the plantation," *New York Times Magazine* (August 14, 2019), https://www.nytimes.com/interactive/2019/08/14/magazine/slavery-capitalism.html.

66 BROWNE, *supra* note 41 at 32.

67 Desmond, *supra* note 65.

68 *Ibid*.

69 Similarly, "it is crucial to note that the panopticon is a metaphor and that the workplace is not a panoptic prison— workers are not inmates, they have rights and legal protections, and they may organize to resist or limit the use of new surveillance technologies by employers." Manokha, *supra* note 10 at 550.

70 "Whether through slavery, sharecropping, the prison-industrial complex, overpolicing, or the overrepresentation of Black and brown workers in low-wage work, the exploitation and subjugation of Black and brown people has also consistently underpinned the norms, values, and practices that shape American society and the economy. The tech political economy and the tech products that come out of it are not only recipients of this legacy, but are exacerbating and extending it into the 21st century." Negrón, *supra* note 3 at 51.

71 *Ibid*., at 41.

72 BROWNE, *supra* note 41 at 119.

73 *Ibid*., at 128.

74 BROWNE, *supra* note 41 at 131-32 (generalizing from Browne's concept used in the airport security context).

75 Negrón, *supra* note 3 at 43.

pose a threat to fundamental human rights and mental and physical well-being. The state itself is a threat, through institutions such as policing, immigration laws, and the criminal legal system, which are similarly rooted in the above-mentioned histories of slavery and colonialism. Therefore, "tech and labor policy design processes need to not only address tangible concerns brought forth by technology companies and the tech industry [and by their clients, employers which buy and use these technologies on their workers] but at the same time reimagine and strengthen a strong, accountable, and inclusive administrative state."[76]

More broadly, workers deserve a bill of rights with guaranteed protections in the face of harms resulting from employer adoption of biometric surveillance and other forms of data-driven or algorithmic technologies in the workplace.[77] This includes principles such as restoring and promoting worker dignity; protecting worker voice and collective organizing; restricting electronic monitoring and algorithmic decision-making; more meaningful protection of civil rights and freedom from discrimination; and establishing robust oversight, accountability, and enforcement mechanisms, including building interdisciplinary expertise and capacity within all relevant federal agencies.[78]

The combination of new technological capabilities with old systems of sociopolitical ordering threatens to do away with workers' human rights and dignity in addition to their livelihoods and economic security. If current employer practices such as biometric worker surveillance and algorithmic management are left unchecked, the future of workers as little more than "appendage[s] of machinery" may become the norm (to an even greater extent than it already is in some sectors[79]). However, workers do not stop being people at the doors to their workplace (or work vehicles), nor should they be expected to cede their fundamental human rights and freedoms in exchange for employment. U.S. labor, employment, technology, and privacy laws should reflect this basic principle.

Thank you for the opportunity to comment.

Respectfully submitted,

/s/_____
Cynthia Khoo, Associate
Center on Privacy & Technology
Georgetown Law
600 New Jersey Avenue, NW
Washington, DC 20001
[redacted]

---

76 *Ibid.*, at 43.

77 For a broad principles-based framework with specific recommendations, see Bernhardt, Kresge & Suleiman, *supra* note 23 at 18-26.

78 For recommendations that address building federal agency capacity in the technology and civil rights context, see Laura Moy & Gabrielle Rejouis, "Addressing Challenges at the Intersection of Civil Rights and Technology," Day One Project (December 2020), https://www.dayoneproject.org/post/addressing-challenges-at-the-intersection-of-civil-rights-and-technology.

79 Jathan Sadowski, "Potemkin AI," *Real Life* (August 6, 2018), https://reallifemag.com/potemkin-ai; and Astra Taylor, "The Automation Charade," *Logic* (August 1, 2018), https://logicmag.io/failure/the-automation-charade/.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Cisco Systems

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Cisco Systems, Inc. Response to White House Office of Science and Technology Policy Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

January 13, 2022

Introduction

Cisco Systems, Inc. ("Cisco") appreciates the opportunity to provide comments in response to the Office of Science and Technology Policy's Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies. We welcome OSTP's attention to the role of data-driven technologies in society and we look forward to ongoing engagement with OSTP regarding the use of these technologies in business settings.

Cisco is the worldwide leader in technology that powers the Internet. We deliver innovative software-defined networking, cloud, collaboration, applications, and security solutions across the globe. Our customer base spans large and small organizations across the public and private sectors, including 95% of Fortune 500 companies. Our corporate mission is to empower an inclusive future for all.

Cisco uses artificial intelligence (AI) and machine learning (ML) across our portfolio to deliver high-value capabilities that satisfy our customers' needs. Cisco is committed to responsible development and use of AI/ML and to upholding industry-leading privacy, security, and human rights standards.

In this submission we provide some general observations about the questions raised in the RFI, describe how we use (and do not use) biometric technologies in our product portfolio, address security considerations, and describe the governance frameworks that we have in place.

General observations

Biometric technologies are currently used across a very wide range of settings and contexts, from private use on a personal device to employee use on corporate systems to broad scale use in public settings. Understanding the potential for benefits and harms arising from the use of these technologies requires evaluating the specifics on a case-by-case basis. There are valid and salient concerns about the potential for harm when biometric information is used in certain settings or without appropriate safeguards for efficacy, privacy, security, human rights, and fairness.

We believe that with meaningful safeguards in place, biometric information can be leveraged for certain business use cases to deliver value to individuals and organizations that cannot easily be obtained by other means. Our experience has been that by being thoughtful about the unique properties of technologies like facial recognition, our products can become more inclusive and provide individuals with greater flexibility in how they work, learn, and carry out daily activities.

We also believe that the evolution and uptake of machine learning presents an opportunity to be more explicit and transparent about potential unintended biases that exist in data and algorithms than was previously possible with traditional software systems and business processes. Human judgement carries its own biases that, in traditional systems, were not typically quantified or even revealed. Advances in machine learning present an opportunity to make these biases known and to be deliberate and transparent in choosing bias mitigation measures.

Biometric technologies are not a proper fit for every use case. The decision to leverage biometric information within a particular product or service needs to be taken with diligent attention to the overall system design and with an understanding of the trade-offs between the risks and benefits that biometric information brings.

Responsible uses of biometric technologies

At Cisco, we build our products to be secure by design and private by default. In general, we minimize the amount of personal or sensitive data we collect and retain from our customers and end users to what is strictly required to offer our services,

and we seek alternative product designs that avoid data collection where possible. We believe that privacy is a fundamental human right.

In this section we describe three Cisco product suites - Webex, Duo, and Meraki Video – to illustrate the range of approaches we have taken to the collection and use of biometric information. This section is responsive to questions 1, 2, 3, and 5 of the RFI.

Webex

Webex is a purpose-built collaboration suite for hybrid work that supports calling, meetings, messaging, devices, and more. Cisco makes use of facial recognition within our Webex suite to recognize individuals participating in Webex meetings and display their name labels, to provide background blur and background replacement, and to optimize visual layouts on screen. These features are designed to make Webex meetings more inclusive, secure, and personalized, and to power the future of hybrid work.

We use a layered set of techniques and mitigations to ensure privacy, security, and accuracy in our use of facial recognition.[1]

We require customer organizations and their end users to opt in to use facial recognition before it is turned on. Users must follow an intentional, multi-step process that involves approving a face image for upload to our secure Webex cloud. If an organization administrator later disables facial recognition, all associated data for that organization's users is deleted in a timely fashion. If an enrolled user leaves the organization, the user's face images and associated data are deleted.

We never use facial recognition outside of the controlled environment of a Webex meeting, and we never use facial recognition to identify individuals who have not enrolled their facial images. While doing otherwise is technically feasible, we have deliberately chosen to constrain our use of facial recognition only to those users who affirmatively choose to use it to improve their meeting experiences.

The neural network models we use for facial recognition are pre-trained by Cisco without using customer data. We manage our training data sets to ensure that they are

[1] More details about data handling and privacy related to facial recognition in Webex are available in our white paper.

balanced across visual features, reducing data bias. We improve accuracy by using labeled training data where we can associate a training image to a verifiable identity (e.g., where a Cisco employee volunteers to help with training).

Users' enrollment images are never used outside their own organizations. Other than enrollment images, images of users are not stored in the Webex cloud.

Images are not used in real time for facial recognition. Instead, a vector is calculated at enrollment time. This approach is reliable because the computed vector is based on multiple views of the user's face from different angles and with different accessories (e.g., with eyeglasses and without eyeglasses). This vector is used to match the vector of a user constructed when a face is detected during a meeting. This approach reduces algorithmic bias by relying on the enrollment vector, which provides a more accurate match than would be obtainable by doing real-time image matching. It also removes any dependency on the user's image in the operation of Webex meetings.

For some features, we make use of face detection rather than facial recognition. Face detection uses a trained model to detect that a human face is present (or to count the number of faces present) in a video frame without attempting to recognize an individual human. This technology is used in features such as background segmentation to determine which user in a video frame is in the foreground and for features that track the active speaker in a meeting to provide the best view of a speaker, which requires being able to detect heads in 3D rather than 2D face images. Similarly, when we train models to support other video features like the recognition of hand gestures (e.g., to show a "thumbs up" emoji on screen when a meeting attendee gives a thumbs up sign with their hand), we never do facial recognition or link the faces in the video data to identity.

Duo

Duo is a user-friendly, zero trust platform used by organizations of all sizes to secure their users' access to devices and applications.

Duo supports certain biometric authentication factors that are widely available and easy to use. These include Apple's Touch ID and Face ID and Android's fingerprint feature. These features are built into device operating systems and provide both a high level of security as well as privacy protection that prevent larger scale abuse. Biometric information is stored in a secure manner on the device by the native

operating system, and the use of WebAuthn[2] technology allows the operating system to confirm with Duo systems that the individual user has authenticated biometrically, confirming their identity, while not conveying any other potentially identifiable information to Duo. When users choose to use these methods of authentication, their biometric data is never shared with Cisco. This combines strong privacy protection for Duo users with the strong security benefits of biometric identification.

Meraki Video

Meraki Video provides enterprise video security with a suite of cloud-managed smart cameras. Schools, retail establishments, and businesses of all kinds use Meraki Video to secure their premises.

Meraki cameras use computer vision to detect people and vehicles, but the cameras never determine individual identity. This allows enterprises to track activity on-location without learning the identities of patrons, employees, students, or visitors. The cameras report when a person appears in a video frame, but not who the person is. Meraki Video does not use facial recognition, gait recognition, or any other kind of biometric identification.

This design was a deliberate choice and is one that bucks the much more common trend in the video surveillance industry of using biometric technologies to identify individuals. Many of our customers consistently request that we add identification capability, but we refuse to do so because we believe that biometric identification in video security solutions has a high probability of misuse, and the difficulties of doing it accurately can prevent it from being used safely. For example, available research demonstrates that identification of individuals via facial recognition in public spaces is extremely difficult to do accurately without significant control over the physical environment or cooperation from the individuals to be identified.[3]

Even without doing biometric identification, we know that recorded video is sensitive data. For that reason, we store all recorded video encrypted on the cameras themselves rather than in the cloud. Processing of video for the purpose of object

[2] See WebAuthn.
[3] See NISTIR 8173, Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects.

recognition takes place exclusively on the cameras. We were the first in the industry to bring this innovative, privacy-preserving design to market.

Cisco has no access to stored customer video unless the customer explicitly authorizes access. When these accesses are authorized, for example during a customer support call, they are logged in a customer-viewable log so that the customer has a record of each access event.

This authorization scheme extends to customer video provided to selected teams within Cisco to train the object classification model we use in the cameras. Our customers have an option of contributing their video data to help us improve object classification (including detecting the presence of a person but not the person's identity in a video frame). Customers have complete control over which of their cameras contribute video to our training data. By default, no customer video data is shared with Cisco. If they opt in to contribute training data, customers can review which video clips we use for training. They can delete any of their data or opt out at any time. This is yet another way in which Cisco differentiates from the rest of the industry: by providing a robust set of privacy controls around customer-provided training data, rather than simply using all customer data for training as a condition of using our cameras.

Summary

As these three products demonstrate, we are deliberate in our decision-making about when the use of biometric technologies is appropriate to meet customer needs. In the case of Meraki Video, we have chosen not to use biometric identification – and foregone potential additional revenue - because it is neither safe nor accurate. In the controlled environments of Webex meetings and Duo authentication, we enable biometrics-based features when our customers and users choose them. In all cases, we use layered safeguards to mitigate inaccuracy, bias, and privacy and security threats. We never monetize biometric information.

Security considerations (RFI question 3)

When biometric technologies are added to a product in our portfolio, they become embedded in Cisco's overall security model and the Cisco Secure Development Lifecycle (CSDL), a repeatable and measurable process that is unified across all solutions and services we offer.[4] This means that biometrics-based features are developed using secure tools and processes and that they benefit from the same physical, infrastructure, platform, and application security architectures and controls as the products in which they are embedded.

In the case of Webex, the neural network models we use for facial recognition are trained on data that we fully control, are rigorously tested for accuracy and bias, and are embedded internally in the Webex service. They are thereby defended against data poisoning attacks, inference attacks, and many of the other kinds of adversarial attacks that may target ML models used by other parties or in public-facing settings. Face images and vectors are encrypted in transit and at rest, with role-based access control and segregation of duties controlling Cisco's access to this data. Face images cannot be reverse-engineered by accessing the vectors.[5]

The next section discusses Cisco's Responsible AI/ML Framework, which includes specific requirements applied to our engineering, development, and deployment processes for all AI/ML capabilities, including AI-powered biometric technologies.

Governance programs, practices, and procedures (RFI question 6)

At Cisco, we rely on broad-based governance frameworks to ensure that all of our products – not just those involving AI, ML or biometric technologies – are designed to protect privacy, safeguard security, and respect human rights. These frameworks are based on industry standards and best practices, but informed by our own unique experiences, customer set, and portfolio. We address the kinds of concerns raised in the RFI through the joint application of our Cisco Secure Development Lifecycle (described above), our Responsible AI/ML Framework, our Business and Human

[4] See the Cisco Secure Development Lifecycle Overview.
[5] For more information about the Webex security architecture, see the Cisco Webex Meetings Security White Paper.

Rights Program, and our Global Privacy Program. These programs need not be specifically tailored to biometric technologies to collectively provide the governance framework needed to establish trust in our development and use of these technologies. Global consistency is key: we rely on these programs to ensure compliance in the 170+ countries in which we operate.

Our Responsible AI/ML Framework, which is perhaps most directly applicable to the subject of the RFI, includes three key components:

- Design requirements. All Cisco products that incorporate AI or ML must comply with baseline requirements relating to model definition; data quality, relevance, licensing, attribution, and unintended bias mitigation; model monitoring and protection from attacks; user consent; fairness; and model documentation. Models that are directly involved in decisions that could have a legal or human rights impact on individuals or groups are subjected to an in-depth responsible AI/ML assessment prior to being brought to market. The assessment serves as a gating function that prevents models from being deployed until the potential for negative legal or human rights impact is minimized.

- Incident response. Our Responsible AI/ML Incident Response Team may receive reports of unfair, biased, or discriminatory decisions powered by AI or ML in our products. When we receive these reports from customers, employees, or partners, our Responsible AI/ML Incident Response Team analyzes the reports and engages the appropriate internal team to resolve the issue. Once the issue is resolved, we may report back to the original submitter or a broader group of Cisco customers, employees, and partners on the findings of the investigation and remediation steps taken.

- Oversight. Cisco has established an internal Responsible AI/ML Committee that consists of senior executives from across our lines of business, sales, privacy, security, human rights, legal, government affairs, and other functions. The committee is tasked with reviewing sensitive or high-risk uses of AI and ML being proposed by our business units, reviewing incident reports of bias or discrimination, advising Cisco's leadership and employees on responsible AI/ML

practices, and overseeing the adoption of our overall Responsible AI/ML Framework.

Through Cisco's Business and Human Rights (BHR) program, we work to identify potential human rights issues related to our supply chain, product design and use, and business relationships. The BHR team's purpose is to help prevent and mitigate harms from occurring, and to advise the business on strategies to respond if they do materialize. The BHR team works across functions to make these strategies standard practice by incorporating them into policies and decision-making frameworks. As an internal clearinghouse for human rights matters, our dedicated human rights experts answer questions, conduct due diligence to inform business decisions and product development, and train employees.

Finally, Cisco has implemented a Global Privacy Program to address risks and maintain high standards for processing personal data. The privacy program is composed of numerous components. We inventory and map the data we process and document the results in Privacy Data Sheets and Privacy Data Maps.[6] We conduct privacy impact assessments and customized risk assessments when developing new products that handle personal data. Our development process embeds privacy by design, ensures compliance with the 120+ privacy laws around the world where we operate, and provides customers with tools to comply with their own privacy requirements. We have integrated privacy incidents into our incident response process and privacy engineering methodologies into the CSDL. Our privacy office oversees all components of the program, analyzing regular reporting of relevant metrics and risk reviews, and conducting internal and external audits.

Conclusion

We believe that our approach to using biometric technologies provides compelling evidence of how these technologies can be responsibly deployed in enterprise settings to deliver value to customers and end users without compromising privacy, security, or human rights. We look forward to further engagement with OSTP on this important topic.

[6] See Privacy Data Sheets and Privacy Data Maps.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

City of Portland Smart City
PDX Program

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

City of Portland's Smart City PDX program's comments to the OSTP RFI on Public and Private Sector Uses of Biometric Technologies

Portland, Oregon January 13, 2022

In response to the Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (FR Doc. 2021-21975[1]) by the Office of Science and Technology Policy (OSTP), the City of Portland's Smart City PDX program[2] recognizes the importance of this topic and reached out to city employees to understand any current or future plan of using biometric information in our local government.

Context

The Smart City PDX program is part of the Bureau of Planning and Sustainability[3] of the City of Portland, Oregon. In recent years, the program has been developing foundational policies that embed equity and anti-racism in the use of information and technology.

In 2019, the City passed its privacy and information protection principles[4] and then the City issued a ban on use of face recognition technologies in city bureaus and by private entities in places of public accommodations[5]. These bans were an answer to community and elected officials concerns that the technology impacted disproportionately to people with dark skin color, women and elderly people.

The City of Portland is currently developing its privacy and surveillance technologies policy[6] based on the idea of digital justice[7], and engaging in conversations and literacy events with the community. This policy has the goal to develop internal capacity, infrastructure, and guidelines to manage information technologies that collect information from people's lives and movements.

---

1 https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

2 https://www.smartcitypdx.com/

3 https://www.portland.gov/bps

4 https://www.smartcitypdx.com/privacy-principles

5 https://www.smartcitypdx.com/face-recognition

6 https://www.smartcitypdx.com/surveillance-policy

7 https://www.smartcitypdx.com/news/2021/1/22/what-does-digital-justice-mean-in-portland

Internal survey and findings

Our team sent a survey to all city bureau liaison with technology services to understand the current and future use of biometric information, as defined in this RFI. We also asked about any concerns and suggestions on using this type of information.

City staff recognize some benefits in using biometric information, particularly for personnel identification and access to secure areas; however, most of the people that answered the survey see the collection of biometric information as a liability and adding more complexity to the regular protection of information that the City already implements.

City staff also recognize that this topic requires more public discussion by elected officials and with the community due to disproportionate impacts to Black, Indigenous, and People of Color communities. These comments also included improving existing City infrastructure and city staff capacity for data management to reduce risks and increase public trust prior to any future, proposed collection of biometric information.

In general, city staff is not aware of immediate broad uses of biometric information by the City other than a few, limited cases for personnel identification. All city employee personal data is already protected by State law and City policies.

In addition to this internal survey to city staff and in the context of the public engagement for the development of the City's surveillance technologies policy[8], the Smart City PDX team has also received public comments from the community in Portland. Many community comments express concerns about the future, potential use of biometric information by the City and demanded more transparency prior to the City doing so.

Smart City PDX recommendations

The following recommendations have been compiled from practical experience and policy work in local government, community and staff input, and legal advice through the policy making process.

---

8 https://www.smartcitypdx.com/news/2021/8/11/the-city-of-portland-starts-the-work-developing-its-surveillance-policy

1) Use of biometric information must be minimized to those cases where law or regulation requires it, or there is a clear value added to the community and government operations.

2) The collection of biometric information represents people's bodies and losing control over this information represents an unnecessary risk. Individuals should have the ability to restrict access to their own biometric information.

3) The use of biometric information in local government for commercial or social services should be limited to verification (one-to-one) processes rather than to identification (one-to-many).

4) A risk assessment approach may allow local governments to use specific biometric data or work with trusted vendors for specific cases where this data collection is needed.

5) Metrics around effectiveness of technological solutions relying on biometric information should be included to justify fiscal and social risks and impacts.

6) We recognize that the collection of biometric data may lead to mass surveillance systems and infrastructure that supports that. Any collection of biometric information should be connected to a specific use only in a transparent and accountable way.

7) Exemptions of the use of biometric information could be necessary in emergencies, major disruption events, or cases where robust safeguards and regulations already exist. Reports of the use of biometric information in these exemptions are recommended.

8) Local governments need access to infrastructure to support a secure use of biometric information when necessary. This infrastructure includes: full information life cycle transparency, certification entities for privacy and cybersecurity services, auditing services, training and open standards.

9) Biometric information may create additional barriers to accessing local government services needed by vulnerable residents. The use of biometric information for identity verification should be used on secure devices only and using state of the art encryption algorithms.

10) Specify a minimum retention schedule for biometric information limited to its specific use. This strategy can increase trust, reduce liability and cost to cities.

11) Sharing of any biometric information with other jurisdictions or third parties should follow the information protection standards for highly sensitive information.

12) Policies to use biometric information should be centered in the values of digital rights that protect individuals and groups like informed consent, right to know, and right to be forgotten. People should have ownership and agency over their own data as a fundamental digital right

13) All enterprises need to explore alternative and secure methods for identity verification that do not rely on biometric information.

14) There is a need for public discussion weighing the public good against the intrusion of individual privacy and other associated risks for collection and use of biometric data.

Send any comments or questions to [redacted].

Document prepared by
Hector Dominguez
[redacted]
Open Data Coordinator - Smart City PDX program
Bureau of Planning and Sustainability - City of Portland

The Smart City PDX team includes:
Kevin Martin, Smart City PDX program manager
Christine Kendrick, Smart City PDX coordinator
Judith Mowry, Office of Equity and Human Rights senior policy advisor
[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

CLEAR

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Dr. Eric S. Lander
Director
Office of Science & Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, D.C. 20504

RE: RFI Response: Biometric Technologies

Dr. Lander,

We at CLEAR are grateful to the Office of Science and Technology Policy (OSTP) for initiating this important conversation around biometric technology, and appreciate the opportunity to share our unique perspective based on our decade of experience using biometrics to create safe and easy experiences for our members.

Our extensive work with this technology drives our firm belief that biometrics are best utilized by private-sector companies on an opt-in basis. Empowering individuals to choose whether or not to utilize biometric technologies is the best way to build trust with individuals and communities, and to ensure these solutions are developed in a responsible, equitable, and reliable way. Every solution powered by CLEAR is fully opt-in, and designed to maintain the trust that we have built with our members and users. As a user, you provide the biometrics we use, and you always know when you're interacting with our services.

While we will speak broadly below about our perspective using opt-in biometrics to power frictionless experiences for our members, we intend to be primarily responsive to the following topics from the RFI:

> *1. Descriptions of use of biometric information for recognition and inference*
> *6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case*

I. Introduction

CLEAR Secure, Inc. is a secure biometric identity company, whose mission is to enable frictionless and safe experiences. With more than 8 million members and 130+ partners, CLEAR's identity platform connects you to all the things that make you, you - transforming the way people live, work and travel.

We believe that when users are in control and empowered to choose to use biometric technology, these solutions can provide safer and easier experiences that protect and improve personal privacy while removing friction from everyday life.

Demand for convenience has grown while tolerance for friction has all but disappeared — creating the need for innovative experiences that are easy for consumers. According to a survey by Whyline Inc. - a CLEAR company - 64% of people would rather abandon certain experiences than wait for them, while another survey from Talkdesk Research reports that 68% of customers state that a single negative customer service experience will reduce their loyalty to a brand. This new convenience economy has made us feel like anything and everything is just a click away, while reducing our tolerance for friction in everyday experiences.

COVID-19 has been a great accelerator of this trend, and there has never been a more critical time for both physical and digital experiences to embrace innovation. According to a July study by Deloitte and the National Retail Federation, 78% of consumers value convenience more now than before COVID-19. And a McKinsey survey of executives in fall 2020 found 63% of companies have had to change to meet shifting customer expectations due to the pandemic, and of those, 62% say they expect those changes to become permanent.

In the wake of the pandemic and our heightened awareness around public health, the new customer expectation will be experiences that are safe, but also frictionless. People will demand solutions that help them cut down on crowds, waiting shoulder-to-shoulder in lines, needlessly touching high-traffic surfaces, and constantly having to hand over the cards in their wallet to prove who they are. They want personalized experiences that value their time and their business, and help them get the most out of their day.

Biometric technologies can help to drive this evolution in experiences, but the foundation has to be built on trust. Americans must be able to trust that they will stay in control of their personal information, trust that their information is being kept secure, and trust that everyone who interacts with a technology solution is being treated equitably. A critical building block of that trust is empowering users to choose whether to engage with such novel and evolving technology. People are more apt to trust technology solutions they view as voluntary, inclusive, and

transparent. People are more apt to trust technology solutions they view as voluntary, inclusive, and transparent. At CLEAR, building and maintaining trust has been at the heart of everything we do, which is why our solutions are always opt-in.

II. Creating Safe And Frictionless Experiences

CLEAR got our start in a place where trust is paramount, and friction is high - the airport. For over 10 years, we have been partners with the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) as part of the Registered Traveler program (RT). In the wake of 9/11 and the creation of TSA, the RT program was established as a public-private partnership to leverage private-sector innovation to help maximize security and minimize stress for travelers. With the oversight of our government partners, we use biometrics to create a more frictionless experience at the security checkpoint for travelers, while meeting the highest security standards.

Today, CLEAR's opt-in travel subscription service, CLEAR+, has 115 lanes located in 40 of the largest and busiest airports across the country. Our members utilize iris or fingerprint scans to quickly verify their identity and move on to physical security screening. We have successfully used biometrics to verify identity and direct passengers to appropriate physical screening over 50 million times since 2010. We have a Net Promoter Score (NPS) of 77 providing world class service to our members, while at the same time maintaining the highest government standards for security.

In establishing and implementing the RT program, Congress and the TSA recognized how biometric technology could be leveraged to improve security and act as a force multiplier for the TSA's frontline officers. As the TSA stated in codifying the RT program, the goal of establishing such trusted traveler programs was to "use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."

And as TSA looks towards the future of the security checkpoint, they have continued to emphasize the potential of biometrics technology. In laying out their 2019 Biometrics Roadmap, the TSA recognized the opportunity to develop "a biometrics capability, built with strategic partners, that enhances aviation security, streamlines operations, and simplifies the user experience."

Greater use of biometrics will also help the TSA meet the objectives of President

Biden's recent "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." As Secretary of Homeland

Security Alejandro Mayorkas stated, under the President's EO the TSA will "test the use of innovative technologies at airport security checkpoints to reduce passenger wait times."

As one of the TSA's strategic partners, CLEAR looks forward to building the future checkpoint and improving the customer experience together.

As opt-in solutions such as CLEAR have been adopted at airports across the country, travelers have grown more comfortable with the use of biometrics in air travel. According to the International Air Transport Association's (IATA) 2021 Global Passenger Survey, 73% of global passengers are comfortable using their biometrics to improve their airport experience. In another poll conducted by the Security Industry Association (SIA), 69% of U.S. adults are comfortable with the use of biometrics at airport security, and 75% are comfortable with its use by airlines.

These trends further demonstrate that when new technology solutions allow users to choose whether to engage with them, building a foundation of trust and security, Americans can grow comfortable with their use and enjoy the frictionless journeys they can create.

Building A Frictionless World

While we got our start at airport security, CLEAR's mission has always been to create safer and easier experiences throughout your day. Being a secure identity company has always been about using biometrics to allow you to link your identity with your boarding pass at the airport, your rental car account, your ticket to the game, or your credit card and proof of age to buy a beer at the concession stand.

Amid the pandemic, we recognized that there was going to be a new source of friction as businesses and venues began to reopen, and a need to create safer experiences for everyone. We developed Health Pass to allow CLEAR users to confirm they meet COVID-related requirements for entry set by CLEAR's partners – such as proof of vaccination, negative test results, or health survey answers – just by showing the partner a green or red signal without needing to share detailed health information. We also make it safe and easy for anyone to create a free digital vaccine card that you can carry right on your phone and use wherever you need. Once again, secure opt-in identity could be used to remove friction and improve privacy while making experiences safer for everyone.
As we all grapple with evolving vaccine requirements and the complexity of operating amid COVID-19, CLEAR has been partnering with businesses across the nation to help make coming back — and staying back — easier. More than 130 organizations including major professional sports teams, corporate offices, small

businesses, travel destinations, and restaurants have used CLEAR to help keep their doors open, their workers on the job, and their customers safe.

CLEAR's vision is to empower members to use their verified identity to move frictionlessly through a network of different experiences. You are you, and you shouldn't be constantly having to hand over the cards in your wallet, or share more information than necessary, to prove who you are. But in order to do this, we know our first priority is to maintain the reputation for trust we've spent a decade building. That is why everything that CLEAR does is built on our commitment to the privacy of our members.

III. Our Commitment to Privacy

You are you, and your personal information is yours. As a secure identity company, we firmly believe in keeping users in control of their information. That is why we will never sell or rent personal information, and every solution CLEAR provides is entirely opt-in. We have spent a decade building a brand that stands for trust, and know that our first duty is always to our members.

We believe that our members and users should always know why CLEAR is asking for their information and how it is being used. The only time a member's personal information is shared with one of our partners is when the member affirmatively consents to the sharing of that information.

We will also honor any request to delete a member's personal information from our databases, since you don't truly control your information unless you have the right to have it deleted by any service you no longer wish to utilize. CLEAR has committed to members' Right to be Forgotten nationally since 2010, well before statutes such as CCPA made it mandatory in California.

Additionally, when a member trusts us with their information, it is protected by CLEAR's comprehensive security program that meets the highest government standards for data protection and privacy.

Leading With Transparency

We believe in transparency in everything we do, which is why our Privacy Policy is written in a simple, straight-forward manner that clearly provides members with a guide to what information we collect, how it is used, and how our members maintain control.

When members enroll in our CLEAR+ subscription service, they provide CLEAR with biographic, biometric, contact, and payment information, as well as an image of a

government-issued identification. In the course of enrollment, members affirmatively opt-in and agree to CLEAR's Member Terms. As we have begun offering additional services that require lower levels of identity assurance, members are prompted to provide only the information necessary to power their chosen experience.

Once enrolled, our CLEAR kiosks in airports use iris and fingerprint scans, in line with TSA guidelines, to verify members' identities, while our smartphone-based app uses selfies and facial recognition technology. Smartphone users have the option to securely link their identity to verified credentials. For example, Health Pass users can securely link their verified identity to their proof of vaccination or negative COVID-19 test results. All of CLEAR's solutions are fully opt-in and linking information is at the member's discretion.

The information we obtain about our members is used to administer CLEAR's experiences, such as managing the enrollment process, verifying members' identities, and providing better experiences for our members. We do not and will never sell user information. And our robust privacy policy ensures that member data is not shared with any third party inappropriately. Service providers retained by CLEAR are limited, and are contractually prohibited from using or disclosing any member information they access other than to perform services on behalf of CLEAR and our members.

IV. Using Biometrics To Empower

We understand that biometrics such as facial recognition, iris scans, and fingerprints are especially sensitive data, and that some products powered by this technology raise concerns about the potential for bias or abuse. As OSTP initiates this important conversation around biometric technology, it is crucial to distinguish opt-in solutions that empower users to access more frictionless experiences, while maintaining control of their information, from those that collect biometric information without a person's consent.

Unlike many of the facial recognition applications that have recently received notoriety, all of CLEAR's solutions rely on user-provided images and biometrics, and we do not capture images of non-users. We do not conduct passive monitoring, surveillance, or scanning of crowds, and our members and users always know when they are interacting with our services. We are comparing a user-provided photo against a government-issued ID that the users themselves have chosen to provide us, and we are empowering members to use their biometrics to confirm their identity.

Addressing Bias

As part of our commitment to building solutions that empower our members and users, we take the issue of bias very seriously and we proactively work to mitigate any racial and gender differentials in the algorithms that power our solutions.

All CLEAR members opt-in and provide their own images — and our processes are designed to ensure that a high-quality image is captured. Relying on high-quality, user-provided images as CLEAR does helps to significantly mitigate the risk of racial disparities in facial recognition, which depend greatly on the quality of the photo. Since all CLEAR members have opted in to our service, we can obtain higher quality photos for comparison since each member is aware their photo is being taken during the enrollment and verification process.

We are also not using biometrics to make demographic determinations such as gender, ethnicity, or age. Our only goal is to match identity based on your opt-in enrollment information.

V. Keeping Information Secure

A final element in building biometric solutions on a foundation of trust is that users must know that when they entrust personal information to a company, that company will act responsibly to protect their data, and keep it secure and confidential. CLEAR has implemented a comprehensive information security program that meets the highest government standards of data protection and privacy.

Our security program includes administrative, technical, and physical safeguards to protect against threats to the security, confidentiality, or integrity of our members' personal data. The tools we use to protect our members' data include, but are not limited to:

- Data encryption in transit and at rest
- Firewalls
- Multi-factor authentication
- Access-control procedures
- Personnel security controls
- Comprehensive privacy and security training for all team members
- Physical and environmental security procedures
- Intrusion detection and data leakage tools

CLEAR's commitment to guarding our users' data is reflected in meeting the highest industry standards for data protection and privacy:

- TSA designated CLEAR's biometric identity platform at FISMA-High — the

highest government cyber compliance rating available for protecting sensitive data.
  - TSA regularly conducts audits and inspections of CLEAR's technology infrastructure.
- CLEAR's biometric enrollment and verification platform have been SAFETY Act Certified as a Qualified Anti-Terrorism Technology by the Department of Homeland Security (DHS).
- CLEAR is compliant with the Payment Card Industry Data Security Standard, an information security standard for organizations that handle credit card information.
- CLEAR's security program was implemented in accordance with the National Institute of Standards and Technology's (NIST) security control framework.

VI. Conclusion

We would like to once again thank your office for initiating this important conversation and soliciting input from companies like CLEAR. Solutions powered by biometrics offer a remarkable technological evolution with a wide range of applications, but we believe are best utilized on an opt-in basis that empowers individuals and builds trust.

Secure identity can enable frictionless experiences, meeting consumers' new expectations for solutions that are safe and easy. And Americans are ready to embrace these solutions, provided they can trust that they will maintain control of their personal information, and that the companies they entrust with their information will keep it secure. Furthermore, Americans expect providers to build and administer these technologies responsibly and equitably. Everything CLEAR does keeps this duty front of mind.

While we know you will be hearing from a range of perspectives, from the private sector, government agencies, advocacy groups, and the public, we hope this will be only the beginning of the conversation. We hope CLEAR can continue to be a resource for you as you examine the promise and responsible use of this technology.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Clearview AI

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

COMMENT TO OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)

Docket No. 2021-21975

Submission by Clearview AI, Private Company

United States Office of Science and Technology Policy (OSTP) **January 15, 2022**
725 17th Street NW
Washington, D.C. 20528

RE: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Clearview AI, a U.S. based company dedicated to providing the most cutting-edge technology to law enforcement to investigate crimes, enhance public safety, and provide justice to victims, is pleased to provide public comment addressing the issue of biometric technologies, including facial recognition technology.

Facial recognition technology is a critical tool to ensure public safety, provided that proper safeguards are established. It is also a tool that is often characterized with inaccurate information. As stated by James Andrew Lewis, Senior Vice President at the Center for Strategic and International Studies, "[t]he level of confusion and misinformation in the FRT discussion is astounding. . . FRT is improving rapidly, and any critique based on data from even a few years ago runs the risk of being entirely wrong."[1]

Reasonable and effective policies eliminate many of the concerns surrounding the technology, including, but not limited to, discrimination, privacy concerns, and security breaches (such as access breaches).

Proper and reasonable safeguards include:

1) Accuracy requirements and non-discrimination;
2) Privacy protections by excluding and/or redacting explicit images;
3) Records to enable an audit or review of each use;
4) Match verification and secondary review of result;
5) Authorization and accountability by implementing a use policy;
6) Independent verification, the match cannot be used as sole source for positive identification;
7) Prohibition on any use of the technology to target persons engaged in protected activities.

[1] James Andrew Lewis, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (Sept. 29, 2021), available at https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

ACCURACY & TRANSPARENCY IN FACIAL RECOGNITION TECHNOLOGY

Procedures for and results of data-driven and scientific validation of biometric technologies

- Accuracy

Concerns over the use of facial recognition technology related to discrimination and bias can be eliminated by setting a 99% accuracy requirement. High-performing algorithms, as determined by the National Institute of Standards and Technology ("NIST"), do not contain racial bias and are at least 99% accurate in matching images. The Director of the Information Technology Laboratory for NIST, Dr. Charles Romine, testified in 2020 before the U.S. Homeland Security Committee that with the highest-performing algorithms they saw "undetectable" bias, further noting, that they did not see a "statistical level of significance" related to bias in these top-performing algorithms.[2]

Stringent standards for non-discrimination can be met by existing facial recognition technology. For example, NIST's October 2021 evaluation of Clearview AI's facial recognition algorithm found greater than 99% accuracy for all demographics – highlighting the dependability and accuracy in advanced algorithms.[3] In the same report, NIST also ranked Clearview's algorithm #1 in the United States and #2 in the world (most difficult-to-score category WILD photos, as well as average ranking). Subsequently in November 2021, in the most representative one-to-many investigation testing track, NIST once again ranked Clearview AI's algorithm #1 in the United States and #2 in the world (most difficult-to-score category VISA/Kiosk, as well as average ranking).[4]

While Clearview AI has achieved these very high scores in accuracy, the accuracy of facial recognition technology continues to increase generally. As noted by the U.S. Government Accountability Office ("GAO"), "[r]ecent advancements in facial recognition technology have

---

[2] *Facial Recognition and Biometric Technology*, C-SPAN (Feb. 6, 2020), available at https://www.c-span.org/video/?469047-1/homeland-security-officials-testify-facial-recognition-technology-usage.

[3] *Face Recognition Vendor Test (Part 1: Verification),* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Oct. 28, 2021), available at https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf and https://github.com/usnistgov/frvt/tree/nist-pages/reports/11 (past reports).

[4] *Face Recognition Vendor Test (Part 2: Identification)*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Nov. 22, 2021), available at https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf and https://github.com/usnistgov/frvt/tree/nist-pages/reports/1N (past reports).

increased its accuracy and its usage."[5] In fact, unlike older algorithms which use manual measurements, advanced and high-performing algorithms use a form of artificial intelligence called a "neural network".[6] These artificial neural networks operate similar to a biological brain, transmitting various signals to other neurons to map out the image. For example, Clearview AI's high-performing algorithm's neural networks are trained on millions of examples of diverse faces from all ethnicities to ensure there is no racial bias in its algorithm.

Another means of maintaining accuracy is for the provider of a facial recognition technology to regularly update its image search engine with public images obtained by its search engine accessing information available to the general public on the internet, so that the data obtained is highly accurate and up-to-date. Data available to the public from the internet is valuable because, unlike traditional government databases, it can capture persons who are not previously known to authorities. A search engine that relies on a very large library of photographs, enhances the probability that the true match is covered in it and returned to the investigator. This reduces the likelihood of search misses, and the chances of investigators arriving at a false positive match derived from a limited search space and an early conclusion.

Therefore, with facial recognition technology, investigative effectiveness increases with the size and integrity of the underlying database. Larger databases are more likely to provide key information to protect the public than are smaller ones. The use of large public datasets for facial recognition also substantially mitigates the impact of historical inequalities and reduces the likelihood of discrimination, because large public reference databases, such as that developed by Clearview AI, are demographically rich and balanced.

Finally, retrieval rank and threshold are settings whereby an algorithm can be modified to return more results that may not be as accurate. Setting a low retrieval rank or threshold tends to return more false positives. High-performing algorithms should have hardcoded bottom lines for these criteria, thereby limiting the return of false positives. The facial recognition algorithm produces a set of potential matches that are then reviewed by human investigators and trained analysts who serve as peers in the review process.

- Transparency

Transparency is another key feature and is promoted by systems that enable the reconstruction of the reason for a search involving facial recognition technology, and the results of that search. This

[5] *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 24. 2021), available at https://www.gao.gov/products/gao-21-526.

[6] *Neural Networks*, IBM CLOUD EDUCATION (Aug. 2020), available at https://www.ibm.com/cloud/learn/neural-networks.

can be done by a platform requiring users to log on with an associated case number and type, and subsequently made available to the administrative supervisor associated with each particular user agency. This enables user agencies to monitor their individual users and ensure compliance with agency policies. The application can generate statistics for user agencies to show how it is being used and who is using it, to enable administrators to ensure that their agencies policies are being followed and that the technology is only being used for authorized purposes.

AVOIDING HARM – PRIVACY & SURVEILLANCE

Exhibited and potential harms of a particular biometric technology

- Privacy

Facial recognition technology service providers should use public information, with limited exceptions. This largely eliminates any potential privacy concerns related to the individual. Specifically, facial recognition service providers should only use lawfully sourced images including those from the public internet, government databases, or client enrollment services. Government investigators already have lawful access to every public image on the internet. Databases of such public images make the processing of those images faster and more accurate. NIST has found that forensic examiners performed best when supported by facial recognition technology and the most accurate performance resulted when these efforts are combined. "[A] team of scientists from . . . NIST and three universities have tested the accuracy of professional face identifiers, providing at least one revelation that surprised even the researchers: Trained human beings perform best with a computer as a partner, not another person."[7] Facial recognition technology that maintains these kinds of protections achieves a vital public purpose. It is proportional, because the imposition on individual privacy associated with searching public imagery is small, while the benefits to public safety and to victims of crime are substantial.

- Surveillance

Opponents of facial recognition technology often mischaracterize facial recognition technology making it appear analogous to 24/7 mass surveillance. Some countries whose laws do not protect freedom of expression, freedom of movement and other civil rights can design and use the technology to engage in live monitoring of behavior, activities, or information.[8] But this type of

[7] *NIST Study Shows Face Recognition Experts Perform Better With AI as Partner*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (May 28, 2018), available at https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-expertsperform-better-ai-partner.

[8] Dave Davies, *Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'*, NATIONAL PUBLIC RADIO (Jan. 5, 2021), available at https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta.

use is not inherent in the technology, which can be limited to uses that are consistent with and strengthen human rights by protecting against false identifications as well as providing for accurate ones. The use of facial recognition as an investigative tool to look for information to identify a person after a crime or incident occurs is not surveillance. Indeed, LexisNexis, DMV databases, Google, and other search engines are routinely used to look for information after a crime or incident occurs. This type of use does not constitute surveillance even when such algorithms retrieve images to identify a person, nor does it become surveillance when the information they have is matched with a pilot image of a person to identify them. People identify other people using search engines all over the world, every moment of every day. Facial recognition technologies exist, but need to be used for appropriate purposes consistent with protecting societies, with guidelines to ensure that they are not abused.

- Example: Jan. 2021 Capitol Insurrection

Facial recognition technology was used after the fact to investigate criminal conduct during the incidents occurring on January 6, 2021, at the United States Capitol. Law enforcement entities successfully used facial recognition technology to determine if their partial or fleeting photos of those involved in criminal conduct could be matched with publicly posted photos on the internet, and found that the tool shortened the time required to identify persons involved in the incidents.[9]

SECURITY OF FACIAL RECOGNITION TECHNOLOGY

Security considerations associated with a particular biometric technology.

Facial recognition technologies have the promise of providing tremendous value to law enforcement, and companies serving this market should treat law enforcement data with the appropriate level of protection. This means companies should implement strong security programs and internal controls around customer data. These security programs should include industry standard best practices such as annual penetration tests, bug bounty programs, secure software development techniques, endpoint detection and monitoring, and data loss prevention. Internal controls should limit employee access to customer data as much as possible, and all employee and customer actions should be logged and auditable.

REAL USES OF FACIAL RECOGNITION TECHNOLOGY & POTENTIAL BENEFITS

Descriptions of use of biometric information for recognition and inference & exhibited and potential benefits of a particular biometric technology

[9] Kashmir Hill, *The facial-recognition app Clearview sees a spike in use after Capitol attack*, NEW YORK TIMES (Jan. 9, 2021), available at https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html; Jared Council, *Local Police Force Uses Facial Recognition to Identify Capitol Riot Suspects*, WALL STREET JOURNAL (Jan. 8, 2021), available at https://www.wsj.com/articles/local-police-force-uses-facial-recognition-to-identify-capitol-riot-suspects-11610164393.

Responsible use of facial recognition technology is supported by the public for appropriate public uses, such as solving crimes, protecting victims, and rescuing endangered persons. According to November 2021 research performed by Zogby Analytics, 75% of Massachusetts residents and more than 75% of Virginia residents see the use of facial recognition technology by law enforcement as appropriate and beneficial.[10] Specifically:

- 87% of Massachusetts residents said law enforcement should be able to search publicly available social media photos to help find missing children and to find or prosecute child sex offenders/traffickers;

- 83% of Massachusetts residents said law enforcement should be able to search publicly available photos to help find endangered adults and 82% are in favor of using the technology to positively identify endangered individuals;

- 69% of Massachusetts residents think that private facial recognition database that only includes arrest mug shots would have a risk of being discriminatory with 52% saying it was a high or moderate risk;

- 90% of Virginia residents said law enforcement should be able to search publicly available social media photos to help find missing children and to find or prosecute child sex offenders/traffickers;

- 84% of Virginia residents said law enforcement should be able to search publicly available photos to help find endangered adults and 86% are in favor of using the technology to positively identify endangered individuals;

- 70% of Virginia residents think that private facial recognition database that only includes arrest mug shots would have a risk of being discriminatory with 52% saying it was a high or moderate risk.

These results match with a 2019 study by the Center for Data Innovation, which found that only 26 percent of Americans believe the United States government should strictly limit the use of facial recognition technology, and only 18 percent believe the government should strictly limit its use if

[10] *Three-in-Four Massachusetts Residents See Facial Recognition Technologies as Beneficial*, CISION PR NEWSWIRE (Nov. 30, 2021), available at https://www.prnewswire.com/news-releases/three-in-four-massachusetts-residents-see-facial-recognition-technologies-as-beneficial-301433959.html; *Three-in-Four Virginians See Facial Recognition Technologies as Beneficial*, CISION PR NEWSWIRE (Nov. 30, 2021), available at https://www.prnewswire.com/news-releases/three-in-four-virginians-see-facial-recognition-technologies-as-beneficial-301433955.html.

it comes at the expense of public safety.[11] A 2020 study by NetChoice similarly found that 83 percent of Americans want state and local governments to improve law enforcement use of facial recognition rather than ban it.[12] A majority of individuals polled by NetChoice supported the technology's use for lead generation, keeping child predators off school grounds, finding missing senior citizens, and locating terrorists during an active terrorist attack.

Trafficking and Crimes Against Children

Facial recognition offers unprecedented capabilities to identify stalkers, rapists, child abusers, and other online predators and could facilitate identification of previously unknown child victims depicted in child sexual-abuse material proliferating online. A Nevada Police Department investigator needed to identify a child that was being sexually exploited before she left the city. While online prostitution ads do not always provide identifying information for the workers, the ads often have high quality pictures that are suitable for facial recognition searches.

The investigator submitted one of the images from the ads, and within 10 to 15 seconds facial recognition technology provided a possible lead, including a link to the girl's Instagram page. By researching the contents of the public Instagram profile, the investigator positively identified the victim within two hours of the search – and confirmed that she was a 16-year-old juvenile. After booking an "appointment" for the next day, the investigator recovered the victim and apprehended her trafficker. She had been trafficked and abused since she was 13 years old. Time was of the essence and local law enforcement access to the technology was critical to this victim's safety.

Attempted Child Abduction

A suspicious YouTube video was shared to a Michigan police department Facebook account. The video showed conversations in which an adult male subject attempted to solicit child sexually abusive material from a 14-year-old female, and then attempted to abduct the juvenile victim at a park. A vehicle and partial license plate was visible in the video. A facial recognition search of the profile photo resulted in a match to the suspect's real social media account. Further investigation uncovered the suspect had a vehicle matching the partial plate and vehicle seen in the video. The investigative lead was forwarded to local authorities who continued the investigation and apprehended the suspect.

---

[11] Daniel Castro and Michael McLaughlin, S*urvey: Few Americans Want Government to Limit Use of Facial Recognition Technology, Particularly for Public Safety or Airport Screening*, CENTER FOR DATA INNOVATION (Jan. 7, 2019), available at https://datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/.

[12] *Americans Want Facial Recognition Use By Law Enforcement Improved, But Not Banned*, NETCHOICE (Sept. 24, 2020), available at https://netchoice.org/media-press/americans-want-facial-recognition-use-by-law-enforcement-improved-but-not-banned/.

Identifying a Killer Who Targeted LGBTQ Victims[13]

Three members of the LGBTQ+ community were shot and killed by a man at a local home in Detroit, Michigan, in 2019. The Detroit Police Department used facial recognition – in combination with other investigative tools – to help identify the suspect based on video images from a nearby gas station. The suspect was charged with three counts of murder, in addition to other charges.

Identifying a Serial Armed Robber[14]

In 2018, detectives in Munster, Indiana, tried to identify a suspect who had attempted to rob a local business at gunpoint, after releasing a photo from the location's surveillance system which was shared by local media. No leads were generated until they used facial recognition and found a possible match, a man that had skipped parole after serving a prison sentence for nine armed robberies in Illinois. The suspect was identified after the store owner was shown a photo lineup that included the man's picture and was arrested several months later. Without facial recognition, the suspect would likely never have been found.

Scam Artist

Detectives in North Carolina were working to identify a scam artist in a fraud case. The detective searched a photo of the fraud suspect using facial recognition technology and was able to identify him from an article in New Jersey. The suspect was wanted in New Jersey for similar crimes.

SAFEGUARDS TO ENSURE THE RESPONSIBLE USE OF FACIAL RECOGNITION TECHNOLOGY

Like any technology, facial recognition can be used properly to help protect people and societies, to speed identification of people to enable them to safely secure access to protected areas, to enable them to efficiently obtain services, such as access to their online accounts. Guidelines that shape how facial recognition technologies are used are an essential element of ensuring that they protect civil liberties while meeting other important objectives consistent with living in a free society. Principles such as accuracy and non-discrimination, protecting privacy, ensuring accountability, and preventing the abuse of the technology to surveil domestic populations engaged in protected or private activity, are all essential elements of making facial recognition technology serve the public interest.

---

[13] Sarah Rahal, *Detroit man charged with triple LGBTQ killings*, THE DETROIT NEWS (Jun. 2019), available at https://www.detroitnews.com/story/news/local/detroit-city/2019/06/06/detroit-man-charged-triple-lgbtq-killings/1373342001/.

[14] Sarah Reese, *U.S. Marshalls Arrest Fugitive in Munster Payday Loan Business*, THE TIMES OF NORTHWEST INDIANA (July 7, 2018), available at https://www.nwitimes.com/news/local/illinois/u-s-marshals-arrest-fugitive-in-munster-payday-loan-business/article_9e538765-53a0-52f7-bc8a-34baa5bbdc54.html.

The chart below provides the essential principles for facial recognition technology's use in the public interest.

CIVIL LIBERTY PROTECTION PRINCIPLES	
Accuracy & Non-Discrimination.	Facial recognition technology must meet a minimum accuracy standard for face matches in all demographic groups to ensure non-discrimination against any demographic group. A facial recognition service shall be deemed to meet the standards by having participated in the business-relevant tracks evaluated by the Face Recognition Vendor Test (FRVT) from NIST and scored well. The algorithm is recommended to have received 99% or better true positive rates across all demographic groups at stringent false positive rates as selected by FRVT, or at high retrieval ranks. We note that FRVT regularly puts out new test datasets and retires old ones, so our recommendations must be put into context. On an absolute scale, algorithms will only get more accurate. Notwithstanding the foregoing, a lower standard of accuracy shall be acceptable to identify a person under the age of 18 in connection with providing the facial recognition service for protecting a minor at risk of abuse, kidnapping, or other threats to a minor's life or safety.
Privacy.	The facial recognition technology must be designed so that it protects the privacy of persons by excluding, redacting, blurring, or otherwise obscuring nudity or sexual conduct, involving any identifiable person. This limitation shall not apply to images made available to the facial recognition service provider by an authorized law enforcement agency seeking to protect a minor at risk of abuse, kidnapping, or other threats to a minor's life or safety.
Records.	Any facial recognition service provider must ensure there is a mechanism to produce a record that can be used to audit or review the information used to make a match of a person.
Result Validation.	All facial recognition technology search results must be subjected to a secondary review and verification prior to acting on the investigative lead.
Authorization & Accountability.	A facial recognition technology use policy must be in place prior to utilizing the technology.
Independent Verification of the Lead.	Information provided by facial recognition technology may be used as lead information to assist in identifying a person for an investigative purpose. A match provided by facial recognition technology cannot be used as the sole source for positive identification of a person.
Prohibition on Use by Law Enforcement for Persons Engaged in Protected Activities.	Facial recognition technology may not be used to identify a person participating in constitutionally protected activities in public spaces unless there is an articulable investigative purpose.

REQUIREMENTS FOR FACIAL RECOGNITION TECHNOLOGY SERVICE PROVIDER

#1 Undertake reasonable steps to ensure that its facial recognition technology meets the standards of each of the Facial Recognition Safety Principles before it may provide facial recognition technology to any agency.

#2 Require each user of its facial recognition technology to agree to abide by Facial Recognition Safety Principles in any use of its technology as a precondition to it providing such technology to the user.

#3 Put into place a system of data security controls on any images or biometric information provided to the facial recognition service by any user to protect the security of such images or data, including steps to protect facial recognition technology data transmission, storage, and processing to ensure the privacy and security of such images or data, using commercially reasonable encryption and other cybersecurity and privacy best practices.

#4 Notifying to the agency of any security breach or compromise of any data provided to the facial recognition service, as applicable, in the law of the jurisdiction.

#5 Providing user training on the use of the facial recognition technology.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Cognoa

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Cognoa Response to Biometric Technologies RFI

We are grateful for the opportunity to comment on the Office of Science and Technology Policy (OSTP) Request for Information on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.

We are employees of Cognoa, a privately held, pediatric behavioral health company developing digital diagnostic and therapeutic products with the goals of enabling earlier and more equitable access to care and improving the lives and outcomes of children and families living with behavioral health conditions, starting with autism. Cognoa was founded in 2013.

Cognoa believes there is enormous potential for innovations based on artificial intelligence (AI) to help facilitate transformative benefits to healthcare outcomes, streamline diagnostic and treatment pathways, and reduce healthcare inequities. Cognoa also recognizes potential harm related to both the goal and design of AI-enabled systems. We believe AI is not a “silver bullet” for goals of improving healthcare outcomes, and a critical aspect to socially responsible AI systems is the data used to train them.

With our comments, we focus on the use case of Cognoa’s AI-enabled diagnosis aid, Canvas Dx. Canvas Dx is intended for use by healthcare providers as an aid in the diagnosis of ASD for patients ages 18 months through 72 months who are at risk for developmental delay based on concerns of a parent, caregiver, or healthcare provider. The device is not intended for use as a stand-alone diagnosis device but as an adjunct to a primary care provider's clinical judgment. The device is for prescription use only (Rx only). There are no contraindications to using the device.

Current diagnostic processes are highly variable, subjective, and rely primarily on referral to a limited number of specialists with ASD diagnostic expertise. We believe a data-driven approach, one that is designed to support rather than replace providers’ clinical judgement, can help address the inherent limitations of current ASD diagnostic approaches by facilitating expedited diagnosis, improving access to timely intervention, and reducing confounding bias.

We strive to be an example of socially-responsible AI implementation, and we hope to serve as a key contributor to the evolving structure and best practices of AI-enabled innovations. We invite the OSTP to contact us for any questions, further information or discussion based on our submission below.

Best regards, and thanks again for the opportunity,

Halim Abbas & Sharief Taraman, MD, DABPN, DABPM, FAAP

Important Information

Indications for Use

Canvas Dx is intended for use by healthcare providers as an aid in the diagnosis of autism spectrum disorder (ASD) for patients ages 18 months through 72 months who are at risk for developmental delay

based on concerns of a parent, caregiver, or healthcare provider. The device is not intended for use as a stand-alone diagnostic device but as an adjunct to the diagnostic process. The device is for prescription use only (Rx only).

Contraindications
There are no contraindications to using Canvas Dx.

Precautions, Warnings
The Device is intended for use by healthcare professionals trained and qualified to interpret the results of a behavioral assessment examination and to diagnose ASD.
The Device is intended for use in conjunction with patient history, clinical observations, and other clinical evidence the healthcare provider determines are necessary before making clinical decisions. For instance, additional standardized testing may be sought to confirm the Device output, especially when the Device result is not Positive or Negative for ASD.
Canvas Dx is intended for patients with caregivers who have functional English capability (8th grade reading level or above) and have access to a compatible smartphone with an internet connection in the home environment.
The Device may give unreliable results if used in patients with other conditions that would have excluded them from the clinical study. Among those conditions are the following:

- Suspected auditory or visual hallucinations or with prior diagnosis of childhood onset schizophrenia
- Known deafness or blindness
- Known physical impairment affecting their ability to use their hands
- Major dysmorphic features or prenatal exposure to teratogens such as fetal alcohol syndrome
- History or diagnosis of genetic conditions (such as Rett syndrome or Fragile X)
- Microcephaly
- History or prior diagnosis of epilepsy or seizures
- History of or suspected neglect
- History of brain defect injury or insult requiring interventions such as surgery or chronic medication

The Device evaluation should be completed within 60 days of the time it is prescribed because neurodevelopmental milestones change rapidly in the indicated age group.

Authors

Halim Abbas
Halim Abbas is the Chief Artificial Intelligence Officer at Cognoa. Halim a high tech innovator who spearheaded world-class AI projects at game changing techs like eBay and Teradata. His technical interests span digital diagnostics and therapeutics, predictive modeling, computer vision, information retrieval, natural language processing, and big data. Halim has a proven track record of leading cross-functional teams to research and develop first-in-class products and services using novel AI techniques. His experience spans multiple industries such as healthcare, BioPharma, eCommerce, web and mobile services. He holds an B.Eng degree in Computer Systems from Carleton University and an M.Sc. degree in Machine Learning from Columbia University. Halim is a strong believer in the necessity for a socially responsible framework around the application of AI in healthcare, and leading the technology teams at Cognoa to be a paragon in the healthcare industry and a proactive participant in an effort to elevate AI research and development nationwide to a higher diversity, equity, inclusion standard.

Sharief Taraman, MD, DABPN, DABPM, FAAP
Sharief Taraman, MD is the Chief Medical Officer at Cognoa. Dr. Taraman also serves as Division Chief of Pediatric Neurology for Children's Health of Orange County, Associate Clinical Professor at the University of California-Irvine School of Medicine, Affiliate Professor at Chapman University Dale E. and Sarah Ann Fowler School of Engineering, President of the American Academy of Pediatrics-Orange County Chapter (AAP-OC), and on the Board of Directors for AAP-OC, AAP-California, and the International Society for Pediatric Innovation. He is dual board-certified in Neurology with special qualifications in Child Neurology from the American Board of Psychiatry and Neurology and Clinical Informatics from the American Board of Preventive Medicine. He completed his medical education at Wayne State University School of Medicine in 2006 and went on to complete residency training in pediatrics and pediatric neurology at the Children's Hospital of Michigan. Dr. Taraman is enthusiastic about using artificial intelligence to diagnose and treat neurodevelopmental and neurobehavioral disorders early to help children reach their fullest potential.

Topic 1: Descriptions of use of biometric information for recognition and inference

The prevalence of autism spectrum disorder (ASD) has risen steadily since 2000 and is now estimated to affect 1 in 44 children in the United States. Early initiation of ASD-specific intervention has been shown to improve long-term outcomes in several research studies (Estes A., et al., 2015; MacDonald R, et al., 2014; Peters-Scheffer N, et al., 2011; Strain PS, Bovey EH., 2011). Receiving an ASD diagnosis is a key first step in that process. However, families of children who are at risk of developmental delay typically experience an average delay of three years between a parent reporting a concern to a physician and the formal ASD diagnosis (Maenner MJ, et al., 2020; Hyman SL, et al., 2020; Baio J, et al., 2018; Zuckerman KE, et al., 2015). Additional factors, including race/ethnicity, socioeconomic background, and geographic location, may exacerbate this issue. These delays in diagnosis may prevent children from receiving ASD-specific intervention during a key neurodevelopmental window when there is greater potential to improve long-term outcomes.

Cognoa has developed a Software as a Medical Device (SaMD), Canvas Dx, a diagnosis aid intended to help healthcare providers diagnose or rule out autism spectrum disorder (ASD) in the primary care setting, which may streamline the diagnostic process and allow for more efficient specialty referrals. The goal of Canvas Dx is to help physicians and families arrive at diagnostic answers efficiently and thereby enable children to receive appropriate treatment as early as possible. ASD-specific early intervention within the first 4 years of life, particularly before the age of 3, can positively impact the development of a child with ASD and yield significant improvements in behavioral, social, emotional, and cognitive functioning (Estes A., et al., 2015; MacDonald R, et al., 2014).

Canvas Dx harnesses clinically validated AI technology to aid physicians in diagnosing ASD in children between the ages of 18 and 72 months who are at risk of developmental delay based on concerns of a parent, caregiver, or healthcare provider. The device is not intended for use as a stand-alone diagnosis device but as an adjunct to a healthcare provider's clinical judgment. The device is for prescription use only. There are no contraindications to using the device.

Canvas Dx is a data-driven diagnosis aid that integrates three distinct inputs for accurate and timely ASD evaluation in the primary care setting:

- A parent/caregiver questionnaire that asks about the child's behavior and development collected via a parent/caregiver facing app.
- A questionnaire completed by a video analyst who reviews two videos of a child's natural behavior in their home environment, recorded by a parent/caregiver. Video analysts are trained professionals with at least a master's degree and more than five years of experience diagnosing and/or treating children with ASD.
- A healthcare provider (HCP) questionnaire completed by a physician who meets with the child and a parent/caregiver, collected via a healthcare provider portal. Cognoa has contracted with a pediatric care provider to offer the option to have a qualified HCP complete the HCP questionnaire via a video visit with the caregiver and child, with the goal of allowing for a streamlined experience. Alternatively, the prescribing physician can complete the questionnaire.

The main component of the Canvas Dx software system is the underlying, clinically validated machine learning algorithm that drives device output. The algorithm evaluates the three device inputs based on key developmental behaviors that are most indicative of autism and provides one of three outputs for use in conjunction with the child's clinical presentation: positive, negative, or indeterminate. An indeterminate output is given when Canvas Dx inputs are insufficiently granular for the algorithm to render a highly predictive output. For example, a patient may exhibit an insufficient number and/or severity of features to be confidently placed within the algorithmic classifier as being either ASD negative or ASD positive. Canvas Dx's indeterminate output is a standard method of risk control in machine learning algorithms, also referred to as an 'abstention' or 'no result' output.

- By integrating the training data and clinical guidance, the algorithm detects the maximally predictive features of ASD (Abbas H, et al., 2018; Abbas H, et al., 2020; Wall DP, et al., 2012; Duda M, et al., 2014; Kosmicki JA, et al., 2015; Duda M, et al., 2016; Levy S, et al., 2017)
- The algorithm was developed and trained using patient records belonging to thousands of children of both genders with diverse conditions, presentations, and comorbidities who were diagnosed based on the clinical reference standard (Abbas H, et al., 2018; Abbas H, et al., 2020). In conjunction with algorithm training and validation, specialists with expertise in diagnosing ASD were consulted during development of the Canvas Dx clinician questionnaire to understand which questions would most benefit from clinician input as a complement to caregiver input (Abbas H, et al., 2020).

Back-end services and infrastructure, including security encryption, are in compliance with privacy laws and HIPAA. Canvas Dx is available by prescription only and is distributed via Orsini Specialty Pharmacy.

Canvas Dx received FDA Breakthrough Device Designation in October 2018, and FDA De Novo marketing authorization in June 2021. Cognoa has since begun to make Canvas Dx available for prescription use. To our knowledge, Canvas Dx is the only diagnosis aid for ASD that has been granted FDA marketing authorization to date.

Topic 2: Procedures for and results of data-driven and scientific validation of biometric technologies

Cognoa conducted multiple feasibility and validation studies over the course of several years (Abbas et al., 2018; Abbas et al., 2020; Du Y et al., 2019). Through data-driven experimentation, these early stage feasibility studies informed the algorithm's evolution with regards to biometric feature selection, modality selection, age range determination, optimal siloing, need for algorithm abstaining, and prioritization and tradeoffs between net positive/negative values, sensitivity, specificity, and coverage.

In support of Cognoa's De Novo classification request to the FDA, the accuracy of Canvas Dx was assessed in a multisite, prospective, double blinded, active comparator cohort study conducted between August 2019 and June 2020 (currently in peer-review; see abstract here). The Canvas Dx pivotal study measured the accuracy of output from Canvas Dx in comparison to the standard diagnostic approach of the child's evaluation and diagnosis by an experienced specialist using DSM-5

criteria, whose finding was confirmed by independent review. Participation required a commitment to an in-person visit with a specialist.

The study included 425 children, aged 18 to 72 months, whose caregivers or pediatricians had expressed concern about their development but who were never formally evaluated or diagnosed with autism. The children in the study were broadly representative of the U.S. population in terms of race, ethnicity, and socioeconomic background.

The primary endpoints included measurements of positive predictive value (PPV) and negative predictive value (NPV) among subjects with a determinate result, and the indeterminate rate. The secondary endpoints were sensitivity and specificity.

Pivotal study results demonstrate the potential for Canvas Dx's accurate, efficient, and consistent performance:

- The output from Canvas Dx was compared against specialist diagnosis and shown to have a PPV of 81% (95% CI: 70%–89%) and an NPV of 98% (95% CI: 91%– 100%) in those patients with a determinate device result (32%).
- Among patients with a determinate result, Canvas Dx was shown to have a sensitivity of 98% (95% CI: 92%-100%) and specificity of 79% (95% CI: 68%-88%).
- Canvas Dx performed consistently regardless of subjects' gender, race/ethnicity, income levels, parental education levels, demonstrating its potential to help address racial, ethnic, gender, and socioeconomic disparities in ASD diagnosis.
- Canvas Dx did not exhibit degradation of performance across sexes. Accuracy in females was important to establish because of the existing biases in diagnosis for females with ASD. When Canvas Dx provided a result, it correctly identified 92.3% of girls with ASD.
- In the Canvas Dx pivotal study, the average age of children diagnosed with ASD was 2.8 years, which is approximately 1.5 years earlier than the average age of diagnosis in the U.S.

Canvas Dx delivers an indeterminate output as a risk control measure when inputs are insufficiently granular to make a determinate recommendation with confidence. This allows the algorithm to render a highly predictive diagnostic output, minimizes the likelihood of false negatives, and is a common method of risk control in machine learning.

Of the 68.2% of subjects with an indeterminate result, 91.0% were identified by specialists as having one or more neurodevelopmental disorders:

- 71% (206/290) were ASD negative, with at least one other non-ASD developmental or behavioral condition.
- 20% (58/290) were ASD positive.

Topic 5: Exhibited and potential benefits of a particular biometric technology

Many children with ASD are not being diagnosed during the critical early neurodevelopmental period. While a reliable ASD diagnosis can be obtained for a child as young as 18 months, multiple factors have driven the average age of diagnosis to 4 years, 3 months, and this has remained unchanged for over 20 years (Hyman SL, et al., 2020; Zwaigenbaum L, et al., 2016). Children who are non-white, female, or

from rural areas or disadvantaged socioeconomic backgrounds are often diagnosed even later or missed altogether (Velott DL, et al., 2016).

To date, there is no medical test or procedure to diagnose ASD, and behavioral assessments that inform the diagnostic application of the DSM-5 criteria for ASD are the only available means of diagnosis (Hyman SL, et al., 2020). The median 3-year delay between initial concern and ASD diagnosis often encompasses the critical early neurodevelopmental period (Estes A., et al., 2015; MacDonald R, et al., 2014; Peters-Scheffer N, et al., 2011).

- Currently, primary care physicians are the first to screen children for developmental delays and refer those with suspected delays to specialists, including developmental pediatricians, child psychologists, child and adolescent psychiatrists, neuropsychologists, and pediatric neurologists. (Monteiro SA, et al., 2019; Hyman SL, et al., 2020).
- A shortage of specialists and time-intensive evaluations are both factors resulting in long wait times (as long as one year) for diagnostic appointments, causing substantial delays in diagnosis (Gordon-Lipkin E, et al., 2016).
    - In the United States, the number of developmental-behavioral pediatricians by state ranges from 0 to 4.4 per 100,000 children (Monteiro SA, et al., 2019).
    - Approximately 47% of hospitals report staffing vacancies in child and adolescent psychiatry and developmental pediatrics; 34% report vacancies in neurology departments (Gordon-Lipkin E, et al., 2016).
- In a 2018 study, nearly 1 in 10 respondents needed to travel more than 60 miles for diagnosis; 1/3 reported problems finding a specialist (Martinez M, Thomas KC, Williams CS, et al., 2018)
- In-person evaluations can take up to 3 hours to complete, which can be difficult for children with ASD and parents/caregivers, and multiple visits may be required (Gordon-Lipkin E, et al., 2016) .

Until now, there has not been a tool designed for use in the primary care setting to aid in the diagnosis of ASD. While pediatricians can use diagnostic tools such as ADOS®-2* and ADI-R®*, these tools were designed and validated for specialists, require extensive training, and are time-consuming (Gordon-Lipkin E, et al., 2016; Rutter M, et al., 2003). Primary care providers (PCPs) report a lack of training, knowledge, and confidence in assessing ASD, as well as the time necessary to administer the assessments and to counsel caregivers following a positive diagnosis (Beggiato A, Peyre H, Maruani A, et al., 2017; Fenikilé TS, Ellerbeck K, Filippi MK, Daley CM, 2015; Golnik A, Ireland M, Borowsky IW, 2009). As a result, while PCPs are often the first point of contact with families with concerns about a child's development, current tools are not practical for use in this setting.

To help facilitate access to early intervention services, the American Academy of Pediatrics' recently updated clinical report for ASD encourages general pediatricians comfortable with the application of the DSM-5 criteria to make a clinical diagnosis of ASD for children not requiring specialist referrals (Hyman SL, et al., 2020). However, there is a critical need to provide PCPs with the training and tools that provide a higher level of diagnostic support consistent with the DSM-5 criteria than are currently available, thus enabling them to render a diagnosis without referral to a specialist.

As demonstrated by the pivotal study results, Canvas Dx has the potential to help primary care providers effectively diagnose or rule out ASD when used in conjunction with their clinical assessment so that intervention can be initiated earlier than the current average age of diagnosis. The use of Canvas Dx to help PCPs diagnose or rule out an ASD diagnosis in the primary care setting may allow for more efficient specialist referrals and streamline the diagnostic process.

Potential to Reduce Confounding Bias

Boys are more commonly diagnosed with ASD than girls, with a male-to-female prevalence ratio of 4.3:1 as of 2016. (Maenner MJ, Shaw KA, Baio J, et al., 2016). ASD diagnostic tools were initially developed with primarily male subjects, resulting in a sex-related bias in both ASD characterization and diagnosis (Beggiato A, Peyre H, Maruani A, et al., 2017). Studies have shown that racial and socioeconomic disparities in referrals for or access to ASD diagnostic and interventional services contribute to an ASD prevalence gap seen in non-white children (Durkin MS, Maenner MJ, Baio J, et al., 2017; Baio J, Wiggins L, Christensen DL, et al., 2014; Mandell DS, Wiggins LD, Carpenter LA, et al., 2009). In the current diagnostic pathway, girls, African American children, and Latinx children are misdiagnosed more often, diagnosed less often, and diagnosed later, on average (Mandell DS, Wiggins LD, Carpenter LA, et al., 2009; Constantino JN, Abbacchi AM, Saulnier C, et al., 2020; Ros-Demarize R, Bradley C, Kanne SM, et al., 2020; Becerra TA, von Ehrenstein OS, Heck JE, et al., 2014;).

Canvas Dx may help relieve some of the inequities that exist with the current paradigm for diagnosing and treating ASD.

- In the Canvas Dx Pivotal Study, there is no evidence of device performance inconsistency across sex, race/ethnicity, income, or education level.
- By reflecting the demographics of the general population in the U.S., the Canvas Dx Pivotal Study demonstrated how Canvas Dx has the potential to perform consistently across a diverse population.
- The consistency in the performance of the Canvas Dx Pivotal Study when HCP assessments were performed remotely suggests that this device has the potential to facilitate equitable access to ASD diagnoses regardless of location.
- Use of Canvas Dx has the potential to reduce geographic barriers to care and open the door to expanded diagnostic opportunities in rural and underserved communities.
- Canvas Dx provides consistent results across a diverse population and may be used remotely, which may lead to earlier ASD-specific intervention, which in turn could lead to better long-term developmental outcomes.

Use of Canvas Dx requires a smartphone and a prescription and a primary care provider, which may present access challenges in some populations.

Potential Comparative Effectiveness

Until now, there have not been widely-available ASD diagnostic tools designed specifically for use in the primary care setting—Canvas Dx is the first ASD diagnosis aid with FDA marketing authorization.

- There is no widely accepted biomarker or medical test (eg, laboratory or genetic test) to diagnose ASD.
- Current standard of care assessments made by specialists are time-intensive, subject to interpretive bias, and require extensive training, limiting their use in the primary care setting.

PCPs who completed the Canvas Dx questionnaire reported the time it took was approximately 10 minutes.

- Current specialist tools have not been validated for use in a remote setting. The consistency in the performance of the Canvas Dx Pivotal Study when HCP assessments were performed remotely suggests that this device has the potential to facilitate access to ASD diagnoses regardless of location.

Potential Economic Value

Use of Canvas Dx in the primary care setting may allow children with ASD to be diagnosed over 1.5 years earlier than the current average age of diagnosis. The use of Canvas Dx to help pediatricians in diagnosing or ruling out an ASD diagnosis in the primary care setting may allow for more efficient specialty referrals, potentially streamlining the diagnostic process. Direct medical cost savings per early patient diagnosis are estimated to be $817,114 - $1,347,740 (in 2021 dollars) over 50 years (Sharpe DL., 2011; CPI inflation calculator). Use of Canvas Dx may result in cost-savings related to the shortened path to an ASD diagnosis for children with concern for developmental delay.

Diagnosis of ASD in the primary care setting may help shorten the diagnostic journey and facilitate earlier ASD-specific interventions. For families for whom there may be concern of ASD, and for those who receive a “negative for ASD” output, Canvas Dx may minimize use of specialists to rule out ASD. In addition, Canvas Dx has the potential to reduce geographic barriers to care, potentially enabling expanded diagnostic opportunities in rural and underserved communities.

Potential Benefits for Children and Families

The impacts of ASD include decreased parenting efficacy, increased stress, and increase in mental and physical health problems (Karst JS, Van Hecke AV, 2012). ASD imposes significant financial strain and time pressures, and results in high rates of divorce and lower overall family well-being. Over 50% of families with a child diagnosed with ASD report parental need to reduce work time or resign from work to provide needed care (Kogan MD, Strickland BB, Blumberg S, et al., 2008; Parish SL, Cloud JM., 2006).

Use of Canvas Dx in the primary care setting may allow children with ASD to be diagnosed over 1.5 years earlier than the current average age of diagnosis. Diagnosis of ASD in the primary care setting may help shorten the diagnostic journey and facilitate earlier ASD-specific interventions which can in turn improve lifelong outcomes for children.

- Earlier age of diagnosis and intervention—before the age of 4— is among the contributing factors that may help up to 25% of children with ASD progress beyond the original ASD diagnosis (Helt M, et al. 2008).
- Improvements in the domains of cognitive function, behavior, educational achievement, child maltreatment, health/accidents/injuries, and crime have been documented.

In addition, ruling out ASD in the primary care setting may spare those children and families from further diagnostic processes or interventions that are not necessary.

Topic 6: Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case

Cognoa's practices regarding data collection, useage, safeguards for the approved use of data, and post-deployment are in compliance with HIPAA and applicable privacy laws and include the following:

Data Collection

- Measures taken to ensure users are aware of what data is being collected and what it is used for, and that users consent to such collection and use
- Measures taken to ensure data is representative of the target population across all relevant demographic dimensions including gender, age, race, ethnicity, geography, level of education, socio-economic status
- Measures taken to ensure a sufficiently sized, sufficiently representative segment of data is held aside for validation and not used to train or tune the algorithms
- Best practices applied to securing access to data in a matter well controlled and logged and audited, with data access and sharing policies automatically applied
- Best practices applied to sharing data with 3rd parties and getting data from 3rd parties through data partnerships

Data Use

- Safeguards around the storage and access of data such that appropriate data access policies are enforced and automated data governance is applied in the right contexts. For example, data must be deidentified/anonymized for access purposes related to aggregate analysis and model training/validation.
- Safeguards around the use of data to create algorithms that power products and services consistent with our mission
- Safeguards and best practices to ensure data is only used as consented to during data collection
- Log trails to ensure all data use is documented and auditable
- Endeavoring to ensure any future product or service is validated and performance-gauged on data that is representative of the intended target population

Post Deployment

- Ongoing monitoring of device performance and data integrity through audits and summary metrics

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Color of Change

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Before the
Office of Science and Technology Policy

In the Matter of Public and Private Sector Uses of Biometric Technologies	Docket No. 2021-21975

Comments of

COLOR OF CHANGE

Gabrielle M. Rejouis
Color Of Change
Racial Justice Advocacy Group
[redacted]
colorofchange.org

Filed January 14, 2022

Introduction

In its request for information, the Office of Science and Technology Policy (OSTP) seeks input on past deployments, proposals, pilots, and trials, and on current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of individuals' attributes, including mental and emotional states.[1] Color Of Change urges OSTP to consider how biometric technologies disproportionately impact Black communities by reinforcing biased practices and policies. Biometric technology is often defective, accelerates racist law enforcement, and entrenches bias in employment. For these reasons, we recommend that the federal government ban all use of biometric surveillance technology and prohibit use of other forms of biased biometric technology.

1. Biometric technology frequently does not work as advertised.

Biometric technologies often do not identify or recognize Black people and, therefore, cannot do what developers propose they can. Biometric technology developers and vendors often sell promises rather than functional products. Proven inaccuracies and racial biases are built into biometric technologies.[2] If a biometric technology cannot pick up darker skin or respond to an accent, it is defective. Biased technology is not merely an inconvenience; it can potentially interfere with an individual's livelihood (by locking them out of their jobs) and liberty (by misidentifying them for law enforcement purposes). Congress and the Biden–Harris administration must boost regulations for biometric technologies in the private sector. Technology that shows evidence of bias should be banned.

A. Biometric technology is not trained to recognize darker skin.

A 2018 MIT study led by Joy Buolamwini found that when it came to identifying Black women, the error rates for facial recognition technology were up to 35 percent

[1] Office of Science and Technology Policy, Public and Private Sector Uses of Biometric Technologies - Docket No. 2021-21975, Federal Register, October 8, 2021, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.
[2] *Ibid.*

while the technology accurately identified White men over 99 percent of the time.[3] The study also found that the error rate in misidentifying Black women was nearly 49 times that of White men.[4]

The National Institute of Standards and Technology separately found that facial recognition algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a Black or East Asian individual, compared to identifying a photograph of a White individual.[5] Such racially biased inaccuracies are found in biometric technologies across the board, including those sold for commercial use. These reports demonstrate that discrimination is a feature of facial recognition technology.

Further, smart watch developers do not properly account for darker skin when developing light-sensing biometric devices. Smart phones and smart watches developed by companies like Apple[6] and Samsung[7] use biometric technology to monitor heart rate. These technologies have proven to be inaccurate[8] and less effective for individuals with darker skin tones.[9] The technology uses pulses of light to calculate heart rate.[10] When companies fail to adjust the light for darker skin, they sell ineffective products for Black communities and other people of color. Black communities already face health disparities; it is concerning that ineffective technology builds upon this already biased system.

---

[3] Lohr, S. (2018, February 9). Facial Recognition Is Accurate, if You're a White Guy. New York Times. Retrieved November 24, 2021, from https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.
[4] Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81, 1–15. Retrieved November 24, 2021, from http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf
[5] Bushwick, S. (2019, December 27). How NIST Tested Facial Recognition Algorithms for Racial Bias. Scientific American. Retrieved November 24, 2021 from, https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/.
[6] Apple. (2021, October 14). Monitor your heart rate with Apple Watch. Apple Support. Retrieved November 24, 2021, from https://support.apple.com/en-us/HT204666.
[7] Madrigal, A. (2017, July 24). Will the Apple Watch's coolest feature work for people of color? Splinter. Retrieved November 24, 2021, from https://splinternews.com/will-the-apple-watchs-coolest-feature-work-for-people-o-1793846147.
[8] Rettner, R. (2014, March 18). How well do fitness trackers monitor heart rate? LiveScience. Retrieved November 24, 2021, from https://www.livescience.com/44170-fitness-tracker-heart-rate-monitors.html.
[9] Madrigal, A. (2017, July 24). Will the Apple Watch's coolest feature work for people of color? Splinter. Retrieved November 24, 2021, from https://splinternews.com/will-the-apple-watchs-coolest-feature-work-for-people-o-1793846147.
[10] Aronson, K. (2020, September 7). How Apple Watch measures heart rate. ScreenRant. Retrieved November 24, 2021, from https://screenrant.com/apple-watch-heart-rate-measurements-accurate-explained/.

B. Speech recognition technology struggles to understand people of color and women.

Speech recognition technology has proven to be less effective for people of color and women because developers use databases with majority White male data points to train the technology.[11,12] There are major real-world negative implications for these built-in biases. Speech recognition is used to influence immigration decisions, job hiring, and transportation, among many other things.[13]

2. Criminal and immigration law enforcement agencies' use of biometric technologies accelerates the surveillance and racist policing of Black communities.

The use of biometric surveillance by law and immigration enforcement agencies accelerates existing racist policing practices.[14] Law enforcement agencies already disproportionately surveil and police Black communities, and biometric surveillance technology threatens to expand those practices.[15] The technology gives police an "objective" rationale to continue targeting the Black and Brown communities they have always surveilled.[16,17]

Biometric technology can create a vicious cycle, keeping people in constant contact with law enforcement agencies. When police departments use facial recognition

---

[11] McMillan, G. (2011, June 1). It's not you, it's it: Voice recognition doesn't recognize women. Time. Retrieved November 24, 2021, from https://techland.time.com/2011/06/01/its-not-you-its-it-voice-recognition-doesnt-recognize-women/.

[12] Palmiter Bajorek, J. (2019, May 10). Voice recognition still has significant race and gender biases. Harvard Business Review. Retrieved November 24, 2021, from https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.

[13] *Ibid.*

[14] Petty, T. (2020, July 10). Defending Black Lives Means Banning Facial Recognition. Wired. Retrieved November 24, 2021 from, https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/.

[15] Hinton, E., Henderson, L. S., and Reed, C. (n.d.). For the record: Unjust burden racial disparities. Retrieved November 24, 2021, from https://www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf.

[16] Gilbertson, A. (2020, August 20). Data-Informed Predictive Policing Was Heralded As Less Biased. Is It?. The Markup. Retrieved November 24, 2021 from, https://themarkup.org/ask-the-markup/2020/08/20/does-predictive-police-technology-contribute-to-bias;

[17] Richardson, R., Schultz, J., and Crawford, K. (2019) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. 94 N.Y.U. L. Rev. Online 192, 218-19. Retrieved November 24, 2021 from, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423.

technology in connection with mugshot databases to find suspects, they rely on a dataset that is disproportionately Black, a reflection of the racial bias of the criminal justice system.[18,19] In this reinforcement loop, Black people are disproportionately arrested and therefore overrepresented in these databases.[20] The use of facial recognition technology to find investigative leads will direct law enforcement agencies to return to people who have histories with police.[21]

Law enforcement agencies have demonstrated department policies will not protect Black communities from abuse. During the summer of 2020 uprisings, New York City police went to the home of Derrick Ingram, a Black Lives Matter activist, to arrest him. Police submitted a photo to their facial recognition technology to locate him using what appeared to be a photo taken from his Instagram account.[22] In doing so, New York City police violated their own policy, which states that facial recognition technology can only be used with a still from a surveillance video or an arrest photo.[23] A report from the Center on Privacy & Technology at Georgetown Law also found the New York Police Department (NYPD) frequently tampered with photos submitted to their facial recognition technology.[24] Making changes to a photograph to find an investigative lead could dramatically alter the results a search will yield. The NYPD also used celebrity lookalikes to find suspects. For example, detectives used a photo of Woody Harrelson to identify a suspect from surveillance footage.[25] The department also used a photo of a New York Knicks player to find another suspect.[26]

---

[18] Garvie, C., Bedoya, A., and Frankle, J. (2016, October 18). The Perpetual Line-Up. Center on Privacy & Technology at Georgetown Law. Retrieved November 24, 2021 from, https://www.perpetuallineup.org/findings/racial-bias.

[19] Kelly, J. (2020, June 10). Analysis of police arrests reveals stark racial disparity in NY, NJ and CT. ABC 7 New York. Retrieved November 24, 2021 from, https://abc7ny.com/police-racial-bias-profiling-disparity-in-arrests-black-arrest-rates/6241175/.

[20] COC Statement for Facial Recognition Technology: Examining Its Use by Law Enforcement https://docs.google.com/document/d/1tkaT0r1ZnsXGAJj0dqUn0PKIDLZtczzgY0Qm5FNkMoU/edit

[21] COC Statement for Facial Recognition Technology: Examining Its Use by Law Enforcement https://docs.google.com/document/d/1tkaT0r1ZnsXGAJj0dqUn0PKIDLZtczzgY0Qm5FNkMoU/edit

[22] Joseph, G. and Offenhartz, J. (2020, August 14). NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist's Apartment. Gothamist. Retrieved November 24, 2021 from, https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

[23] Vincent, J. (2020, August 18). NYPD used facial recognition to track down Black Lives Matter activist. The Verge. Retrieved November 24, 2021 from, https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[24] Garvie, C. Garbage In, Garbage Out: Face Recognition on Flawed Data. Center on Privacy & Technology at Georgetown Law. Retrieved November 24, 2021, from https://www.flawedfacedata.com/.

[25] *Ibid.*

[26] *Ibid.*

Due to the past practices of law enforcement agencies, the Biden–Harris administration must ban the use of biometric technology in law enforcement. Existing policies are insufficient to protect Black communities from law enforcement agencies' misuse of biometric surveillance technologies. Law enforcement agencies will not follow changes in policy to reduce abuse. Biometric technology must be removed from the law enforcement toolbox.

3. The use of biometric technology in recruitment and employment entrenches bias against Black communities.

The use of biometric technology in the workplace entrenches discrimination against Black people, including those with disabilities and those who are transgender. Biometric technology is used to evaluate job candidates and current employees. While they are marketed as more equitable than traditional evaluations, these systems can reproduce past patterns of inequity.[27]

A. Hiring technology disadvantages Black able-bodied and disabled people.

Hiring technology that incorporates automated cognitive and emotional state evaluations has the ability to punish Black able-bodied and disabled people for deviating from the White and able-bodied norm.[28] Technology developed by HireVue analyzed the language and tone of a candidate's voice and their facial expressions in job interview recordings.[29] The technology was built on a database of about 25,000 pieces of facial and linguistic information compiled by previous interviews of "successful hires."[30] The dataset labeled underrepresented traits as undesired traits, which could disadvantage and systematically exclude Black candidates and candidates with disabilities. The dataset might penalize a job applicant for mannerisms that are acceptable in their culture or that may be indicators of a disability.[31] For example, making eye contact may be seen as a

[27] Rieke, A. and Bogen, M. (2018, December). Help Wanted: An examination of hiring algorithms, equity, and Bias. Retrieved November 24, 2021, from https://www.upturn.org/reports/2018/hiring-algorithms/.
[28] Givens, A. R. (2020, February 6). How algorithmic bias hurts people with disabilities. Slate Magazine. Retrieved November 24, 2021, from https://slate.com/technology/2020/02/algorithmic-bias-people-with-disabilities.html.
[29] Manokha, I. (2019, October 7). How using facial analysis in job interviews could reinforce inequality. PBS. Retrieved November 24, 2021, from https://www.pbs.org/newshour/economy/making-sense/how-using-facial-recognition-in-job-interviews-could-reinforce-inequality.
[30] *Ibid.*
[31] Willingham, E. (2012, October 16). Low Eye Contact Is Not Just An Autism Thing. Forbes. Retrieved January 3, 2022, from

sign of disrespect or trustworthiness depending on the culture; and some people on the autistic spectrum do not make frequent eye contact when speaking. Hiring software that penalizes job candidates for failing to make eye contact will disproportionately impact people from these backgrounds.

B. Facial recognition technology disproportionately deactivates trans Uber driver accounts.

Uber facial recognition technology's failure to recognize transgender Uber drivers locked them out of their jobs. Transgender Uber drivers have been either temporarily or permanently suspended from their accounts due to an Uber security feature that requires drivers to take a photo of themselves to verify their identity.[32] If the photo does not come back as a match to other photos on file, the photo will be flagged and the account will be locked. As transgender individuals transition, their faces may change and look different from photos on file. The use of defective facial recognition in employment can result in reduced income for transgender drivers.[33] When facial recognition technology struggles to identify people with darker skin, this will disproportionately impact Black transgender people. The transgender community already faces barriers to employment. This security feature can exacerbate the economic inequalities they experience.

C. Emotion recognition can encode microaggressions against Black women.

Emotion recognition technology in customer service industries forces employees to strictly adhere to a narrow and sometimes inappropriate set of cultural norms. Companies are using biometric technologies to surveil employees and evaluate their work performance.[34] Call centers use voice analysis technology—like Voci and Cogito—to

---

https://www.forbes.com/sites/emilywillingham/2012/10/16/low-eye-contact-is-not-just-an-autism-thing/?sh=23c19df37f5c.

[32] Urbi, J. (2018, August 8). Some transgender drivers are being kicked off Uber's app. CNBC. Retrieved January 3, 2022, from https://www.cnbc.com/2018/08/08/transgender-uber-driver-suspended-tech-oversight-facial-recognition.html.

[33] Melendez, S. (2018, August 9). Uber driver troubles raise concerns about transgender face recognition. Fast Company. Retrieved January 3, 2022, from https://www.fastcompany.com/90216258/uber-face-recognition-tool-has-locked-out-some-transgender-drivers.

[34] Simonite, T. (2018, March 19). This call may be monitored for tone and emotion. Wired. Retrieved November 24, 2021, from https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/.

assess the emotion of call center employees.[35] This technology will reprimand employees for indicators of negative emotions, such as the tone of their voice or long pauses. The dataset also rewards a narrowly defined set of behaviors, which might not be appropriate for the context of the call. For example, a call center employee repeated "I'm sorry" on a call where a customer joyfully shared about the birth of a baby, aware that the emotion recognition software would register this as empathy.[36]

Biometric technology may provide justification for otherwise biased reviews from their managers. Black women in particular are often judged more harshly for the tone of their voice.[37] Other industries already use biometric surveillance as a pretext to fire Black workers.[38] Amazon monitors the rate at which employees work using a measure called "time off task." If a worker is assigned to assembling orders, time off task (TOT) will track every moment they are not scanning an item.[39] Farhiyo Warsame led worker organizing at the Amazon Shakopee warehouse. After being transferred to a new department, Amazon reported that Warsame was violating the TOT policy. When Black workers are more likely to be fired for raising concerns about workplace conditions,[40] biometric surveillance technology should not provide cover for employers' biased decisions and retaliation.

D. Without regulation and enforcement, private actors will continue to use discriminatory biometric technology.

Regulation is needed because employers will continue to use biometric technology despite these risks. Following the Electronic Privacy Information Center's

---

[35] Dzieza, J. (2020, February 27). How hard will the robots make us work? The Verge. Retrieved November 24, 2021, from https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon.

[36] *Ibid.*

[37] Barratt, B. (2021, June 19). The Microaggressions Towards Black Women You Might Be Complicit In At Work. Forbes. Retrieved January 3, 2022, from https://www.forbes.com/sites/biancabarratt/2020/06/19/the-microaggressions-towards-black-women-you-might-be-complicit-in-at-work/.

[38] Peters, J. (2020, October 2). 'You can see the disrespect': Workers at Amazon center in Minnesota walk out, claiming rushed work conditions, unjust firing. Sahan Journal. Retrieved January 3, 2022, from https://sahanjournal.com/business-work/amazon-shakopee-minnesota-protest/.

[39] Evans, W. (2019, November 25). Ruthless Quotas at Amazon Are Maiming Employees. *The Atlantic.* Retrieved January 10, 2022, from https://www.theatlantic.com/technology/archive/2019/11/amazon-warehouse-reports-show-worker-injuries/602530/.

[40] Tung, I. and Padin, L. (2020, June 10). Silenced About COVID-19 in the Workplace. National Employment Law Project. Retrieved January 10, 2022, from https://www.nelp.org/publication/silenced-covid-19-workplace/.

complaint before the Federal Trade Commission, HireVue conducted a third-party audit of its algorithms and released the results.[41] The audit identified several areas where the company could do more to address racial bias in its algorithms. The audit recommended that HireVue look into potential bias for job candidates with different accents.[42] It also found that candidates of color were more likely to give shorter answers to questions, resulting in these interviews being disproportionately flagged for human reviewers, which might harm candidates' chances to advance to the next phase.[43] Despite these proven concerns of bias, HireVue says that about 700 companies, including GE, Unilever, Delta, and Hilton, have used or continue to use its technology.[44] It is vital that biometric technology developers are given standards to prevent products with bias from going to market.

4. The Biden–Harris administration must protect Black communities by regulating and banning certain biometric technologies.

Law enforcement agencies' use of biometric technologies must be suspended and banned. Addressing the use of this technology is an urgent racial justice issue. A law enforcement agency biometric technology moratorium is vital to protect Black communities. Facial recognition technology increases the surveillance of Black people both in the criminal justice system and in our everyday lives. Law enforcement agencies have proven that they are unlikely to follow changes in policy or regulation. The only way to protect Black communities is to prevent law enforcement from using the technology. Color Of Change supports the Facial Recognition and Biometric Technology Moratorium Act of 2021. The bill would prohibit the use of facial recognition technology by federal entities as well as the use of federal dollars for biometric surveillance systems.

Private actors must adhere to civil rights laws when developing and using biometric technology. They must avoid using technology that advances discrimination and should not be able to pass blame for bias onto the systems they use. Regulation is necessary to create assessment and testing requirements to proactively detect and correct bias in biometric technology. Employers must also be banned from using

[41] Knight, W. (2021, January 12). Job screening service halts facial analysis of applicants. Wired. Retrieved November 24, 2021, from https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/.
[42] Kahn, J. (2021, January 19). Why HireVue will no longer assess job seekers' facial expressions. Fortune. Retrieved November 24, 2021, from https://fortune.com/2021/01/19/hirevue-drops-facial-monitoring-amid-a-i-algorithm-audit/.
[43] *Ibid.*
[44] Knight, W. (2021, January 12). Job screening service halts facial analysis of applicants. Wired. Retrieved November 24, 2021, from https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/.

biometric surveillance technology. The federal government must provide obligations to suspend all use of biometric technology that has discriminatory impact.

Conclusion

Biometric technologies have not delivered the promises of their developers and vendors. These technologies threaten to entrench discrimination in areas such as law enforcement and employment. Improving the accuracy of biometric surveillance technology will not prevent it from enhancing discrimination. Flawed technology should not invite repair but discontinued use. It is paramount for algorithmic accountability regulation to protect Black communities by incentivizing proactive testing and swift termination of technologies that discriminate.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Common Sense Media

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Comments to the Office of Science and Technology Policy

Introduction

Common Sense Media (Common Sense) is pleased to submit these comments in response to the Office of Science and Technology Policy's request for information on how biometric technology is being used in education. Common Sense is an independent, nonpartisan voice for children that champions policy solutions that puts children first and works to ensure that they can thrive in the 21st century.

Biometric technology, like all invasive technology, raises special privacy questions and concerns for children because of their unique vulnerabilities that stem from their brain development and young age. This is most apparent in the education context, in which some students have needed to agree to using certain technology to fully participate in school.

These comments discuss two ways in which biometric technology is being used in education: ed tech software, namely remote exam proctoring software and student activity monitoring software, and facial recognition in school buildings. Remote exam proctoring software and certain aspects of student activity monitoring software, such as the monitoring of keystrokes and eye movement, surveil students to a degree they find intrusive and disturbing, and can expose them to the risk of privacy breaches. Facial recognition software, which is increasingly used in school buildings to track attendance and admission, can also open students up to the risk of privacy breaches, and is often inaccurate, particularly for students of color. This can lead to wrongful identification and discipline of students, which exacerbates already existing inequities in education in which black children are more likely to be disciplined.

Children and teens are uniquely vulnerable on the internet. Their brains are still developing, which makes it difficult for them to distinguish advertising from content and understand the persuasive intent behind ads.[1] They are also prone to oversharing online without understanding the consequences of their sharing.[2] Young children in particular believe information remains at a device level or within an app, and they do not expect or understand that an app may gather information about them from third party sources or

[1] Ofcom, Children and parents: media use and attitudes report, November 2016.
[2] Adriana Galvan et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents* 26 Journal of Neuroscience 25 (2006) (teens' brain development can bias them towards risky behaviors).

that the information they delete remains available.[3] Some young children even consider monitoring by others to be positive.[4] Older children – as well as many adults – also cannot comprehend often long and legalistic privacy policies to better understand how their data is being collected and shared.[5] Many teens think that social networking sites do a bad job at explaining how they treat user information.[6] Because of children and teens' vulnerabilities, schools must prioritize their well-being and interests when considering whether to utilize biometric technology in the education context.

I. Students are increasingly using remote exam proctoring software and student monitoring software, making students uncomfortable and opening them up to the risk of privacy breaches

The use of technology in education has become more prominent than ever. In 2020, with most children attending school virtually because of the pandemic, there was a 69 percent increase in the amount of time kids spent using a computer or laptop for education.[7] This increase was driven largely by five- to 10-year olds.[8] Children also spent more time on tablets for education than anything else, a shift from the year before when gaming took the top spot.[9] Even before the pandemic forced students to stay home, educators increasingly saw the value of using technology in the classroom. In a 2019 survey, 89.6 percent of educators responded that they believed technology is a great way to engage students in the classroom, which was a sharp increase from 31.8 percent the previous year.[10]

In particular, schools are increasingly using remote exam proctoring software and student monitoring software. However, both of these types of software open students up to the risk of privacy breaches, and have been shown to make them uncomfortable and exacerbate inequities.

---

[3] "They See You're a Girl if You Pick a Pink Robot with a Skirt": How Children Conceptualize Data Processing and Digital Privacy Risks. In CHI '21: ACM CHI Conference on Human Factors in Computing Systems, May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA

[4] Gelman, Martinez, Davidson, Noles (2018), Child Development Journal; Sonia Livingstone, Mariya Soilova, Rishita Nadagiri, Children's data and privacy online: Growing up in a digital age, An evidence review, (Dec. 2018).; p. 18.

[5] Children's data and privacy online: Growing up in a digital age, An evidence review, Sonia Livingstone, Mariya Soilova, Rishita Nadagiri, p. 15. (Dec. 2018).

[6] Ofcom, Children and Parents: Media Use and Attitudes Report, (Nov. 2016). Common Sense Media, Privacy Matters: Protecting Digital Privacy for Parents and Kids, (2018).

[7] Ryan Tuchow, Kid device usage changing as a result of the pandemic, Kidscreen, (Feb. 19, 2021).

[8] *Ibid*

[9] *Id.*

[10] The State of Technology in Education, 2019-2020 Report, Promethean (2019).

A. *Remote exam proctoring software*

Schools have needed to turn to remote exam proctoring more than ever during the pandemic to conduct online exams and ensure students are not cheating. However, students have expressed privacy concerns about their remote proctoring experiences and reported disturbing incidents.[11] Remote proctoring software Proctorio claims to identify "suspicious behavior" by monitoring a student's webcam, microphone, keyboard, and other computer activity during an exam and then utilizes an algorithm to look for "abnormalities" between a student and their classmates.[12] Everything from abnormal head and eye movements, mouse clicks and scrolls, websites visited, audio levels, the time it takes to finish the test, to the number of faces detected on screen can all result in a student's test session being flagged as suspicious.[13] In addition to invasion of privacy complaints from this intense surveillance, students and faculty have voiced concern on a wide range of other issues Proctorio and similar remote proctoring services pose, such as bias against students of color, students with accessibility needs, and students with learning disabilities, as well as bias against low-income and rural students.[14]

Many schools have also used ProctorU, a software that similarly uses facial biometrics to match students to their photo identification, and then requests access to the camera, microphone, screen, and keystrokes.[15] In April 2020, nearly 4,000 students at Australia's University of Queensland signed a petition asking the university to come up with a better solution for final exams because of their fears the software would threaten their data privacy.[16] Although the company's privacy policy states the data it collects is only used for the exam session and is not sold to other parties, the data is at risk of being sold or transferred if "involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets."[17]

---

[11] Chris Burt, Concerns about biometric online proctoring expressed by students in Australia, U.S., and Canada, Biometric Update (Jul. 3, 2020).
[12] Tyler Sonnemaker, Tech companies promised schools an easy way to detect cheaters during the pandemic. Critics responded by demanding schools stop policing them like criminals in the first place, Business Insider (Nov. 1, 2020).
[13] *Id.*
[14] *Id.*
[15] Luana Pascu, Australian students fear exam platform threatens biometric data privacy, Biometric Update (Apr. 20, 2020).
[16] *Id.*
[17] *Id.*

B. Student activity monitoring software

Additionally, the number of teachers who reported distribution programs of school-issued devices to educate students at home rose from 43 to 86 percent in the first several months of the pandemic, and this number has only risen since.[18] This has created more opportunities for students to be monitored, particularly for students using school-issued devices.[19] Eighty-one percent of teachers report that their school uses some kind of monitoring software, yet only one in four of those teachers report that monitoring is only limited to school hours.[20] Monitoring software is usually installed directly on a device, which grants access to more of the device's information than browser-based software, which only monitors student content and web activity.[21] This puts students who depend on student-issued devices such as low-income students at greater risk.

Student activity monitoring software can interact with different operating systems and device permissions, such as access to biometric information like keystrokes and input devices like cameras and microphones, as well as content on the device screen. In the United States, thousands of school districts have installed surveillance software on school-issued devices to monitor students' online interactions.[22] Several universities have also started using technology to collect data on students' attention, such as a Paris university that tracks students' eye movement and facial expressions through laptop webcams.[23] This surveillance can make students uncomfortable, affecting their ability to freely learn.

The monitoring activity not involving biometrics is worth noting as well. Programs such as Bark, Gnosis IQ, Gaggle, and Lightspeed can be installed to search for language in student emails and chats and online behavior that indicates the possibility of violent tendencies, suicidal ideation, drug use, pornography use, or eating disorders.[24] School districts sometimes monitor students out of concern for their physical safety and mental health, particularly with students' reported increase in self-harm incidents and aggressive

[18] Elizabeth Laird, Research Report: Protecting Students' Privacy and Advancing Digital Equity, Center for Democracy & Technology (Oct. 22, 2020).
[19] Teachers reported monitoring software use in 71 percent of school-issued devices, compared to only 16 percent of personal devices. Sustained Surveillance: Unintended Consequences of School-Issued Devices, Center for Democracy & Technology (Sept. 21, 2021).
[20] Laird *supra* note 18.
[21] L. Holden Williams, Student Activity Monitoring Software and the Risks to Privacy, Center for Democracy & Technology (Oct. 6, 2021).
[22] Jessa Crispin, US schools gave kids laptops during the pandemic. Then they spied on them, The Guardian (Oct. 11, 2021).
[23] Erika Gimbel, Biometric tech can track how well students are paying attention, Ed Tech (Feb. 23, 2018).
[24] *Id.*

impulses since the start of the pandemic.[25] However, civil groups, teachers, and parents have warned this surveillance results in harmful, unintended consequences.[26] Most notably, online monitoring could be used to discipline students, "out" LGBTQ+ students who are not ready to come out, and chill student speech.[27] Forty three percent of teachers whose schools or districts use student activity monitoring software report that it is used to identify violations of disciplinary policies.[28] There is also a risk that schools may share this data with law enforcement or other external agencies.[29]

II. Schools are utilizing facial recognition technology that is often inaccurate for children, which can exacerbate inequities by leading to wrongful disciplining of children of color, and chill expression

An increasing number of school districts are utilizing facial recognition technology in schools in the name of reducing paperwork and improving school safety, such as by tracking attendance and entrances into school events. However, facial recognition software is often inaccurate, particularly for people of color and for children who are quickly growing and whose faces are changing. This is problematic because facial recognition software is often linked to criminal databases, and can produce wrongful identifications which can lead to schools disciplining the wrong students and chilling their freedom of expression.

Aside from monitoring of students on school-issued devices, the collection of biometric data is also on the rise in school buildings. School districts are launching biometric initiatives to cut down on paperwork as well as improve school safety.[30] For example, in 2019, a school district in Missouri installed 95 biometric facial recognition cameras that are linked to law enforcement databases.[31] If a camera detects a face from a criminal database, they trigger a school lockdown.[32] Biometrics such as fingerprint scans have also

---

[25] Emily Berger, More children are self-harming since the start of the pandemic. Here's what parents and teachers can do to help, The Conversation (Sept. 7, 2021); Beata Mostafavi, National Poll: Pandemic Negatively Impacted Teens' Mental Health, Michigan Health (Mar. 15, 2021).
[26] *Supra* note 19.
[27] *Id.*
[28] Navigating the New Normal: Ensuring Equitable and Trustworthy EdTech for the Future, Center for Democracy & Technology (Nov. 16, 2021).
[29] *Id.*
[30] Shawna De La Rosa, Biometrics can make schools safer, but privacy concerns persist, K-12 Dive (May 9, 2019).
[31] Chris Burt, Missouri school district deploys Panasonic facial recognition for security and access control, Biometric Update (Apr. 10, 2019).
[32] *Id.*

been used to track student tardiness, library check-out, and entrances to dances and athletic events.[33]

While using biometrics can help make schools safer or cut down on paperwork, like all other types of data, biometric information can be breached and sold. Little is known about how these vendors store and use data.[34] Additionally, most districts do not have full-time employees dedicated to protecting student privacy. Teachers also receive little education on student privacy.[35] However, an increasing number of teachers have received training related to student privacy issues, with the number having risen from 56 to 66 percent of teachers from 2020 to 2021.[36]

The accuracy of facial recognition technology in particular raises concerns. Over time, the appearance of faces change, especially for children who are actively developing and growing. In a 2019 NIST report on facial recognition, researchers found aging increased false negative rates.[37] Factors such as the environment in which a face is scanned, the person's posture, and lighting can also affect the accuracy of a facial scan.[38] Many studies have also shown that facial recognition software is less accurate for people of color and women compared to white men.[39] One study found that such software was inaccurate for up to 35 percent of darker-skinned women.[40]

The consequences are particularly problematic for children of color. Inaccurate facial recognition could lead to misidentification of students suspected of fighting, skipping class, and breaking other school rules, which could lead to the wrong children being investigated or disciplined.[41] This would only further perpetuate the institutional racism seen in school systems and the criminal justice system, which already disproportionately harms black children, because it could encourage them to trust a software's identification over a child's own words.[42]

---

[33] *Id.*
[34] De La Rosa *supra* note 30.
[35] Nadia Tamez-Robledo, What do teachers know about student privacy? Not enough, researchers say, EdSurge (Oct. 8, 2021).
[36] Key Views Toward EdTech, School Data, and Student Privacy, Center for Democracy and Technology (Nov. 2021).
[37] Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT), Part 2: Identification, National Institute of Standards and Technology (Sept. 2019).
[38] *Id.*
[39] Facial recognition technology in US schools threatens rights, Human Rights Watch (June 21, 2019).
[40] Steve Lohr, Facial recognition is accurate, if you're a white guy, N.Y. Times (Feb. 9, 2018).
[41] *Supra* note 39.
[42] *Id.*

Even if facial recognition was completely accurate, the risks to children do not stop there. Having facial recognition cameras around could chill children's freedom of expression, such as by discouraging them from being spontaneous or playful or associating with friends or siblings the school regards as troublemakers.[43] This could significantly impact children's emotional and intellectual development.[44]

III. Schools must prioritize students' well-being and interests when deciding whether to utilize new biometric technology

Biometric technology is largely left unregulated, with only a small number of states having passed a biometric-specific law, and even fewer having passed laws restricting the use of facial recognition technology specifically. Due to children's unique developmental vulnerabilities, until more legislation is passed, schools must prioritize students' well-being and interests when utilizing this technology both in an online schooling and an in-person schooling context. Until more legislation is passed, private and public entities must exercise caution in utilizing facial recognition and other biometric technology.

Currently, only five states have a biometric-specific law.[45] Illinois passed the Biometric Information Privacy Act (BIPA) in 2008, becoming the first U.S. state to regulate the collection of biometric data. BIPA requires private entities that obtain biometric information to first inform the subject in writing that their information is being collected and stored, inform the subject of the specific purpose for collection and the term of storage, and obtain a written release from the subject.[46] It prohibits disclosure of biometric information without the subject's consent, unless an exception is satisfied. Since then, Arkansas, California, Texas, and Washington have adopted legislation modeled after BIPA.[47]

Most recently, this summer, Maine passed a law prohibiting the use of facial recognition in all levels of government, making it the toughest facial recognition law yet.[48] However, other states have had very little success in passing laws that ban or heavily restrict facial

---

[43] *Id.*
[44] Lindsey Barrett, Ban facial recognition technologies for children–and for everyone else, 26 B.U. J. Sci. & Tech. L. 225, 252 (2020).
[45] Amy De La Lama, Lauren J. Caisman, and Melissa R. Whigham, United States: U.S. Biometric Laws & Pending Legislation, Mondaq (May 18, 2021).
[46] Dmitry Shifrin and Mary Buckley Tobin, Past, present and future: What's happening with Illinois' and other biometric privacy laws, National Law Review (May 28, 2021).
[47] Christopher G. Ward and Kelsey C. Boehm, Developments in biometric information privacy laws, Foley (June 17, 2021).
[48] Grace Woodruff, Maine now has the toughest facial recognition restrictions in the U.S., Slate (July 2, 2021).

recognition.[49] Such bills failed to advance or were rejected by at least 17 states during the 2020 and 2021 sessions.[50] Washington is the only other state to have a statewide facial recognition law, but it authorizes state police to use facial recognition technology for "mass surveillance of people's public movements, habits, and associations."[51]

In 2019, New York became the first state to enact a moratorium on purchasing or using any biometric identifying technology for school until at least July 2022.[52] The ban also required the New York State Department of Information Technology Services to conduct a study on whether and under what conditions technologies such as facial recognition technology should ever be used in schools.[53]

Children specifically must be given more thought and care. Because of their young age and developing brains, children are already uniquely vulnerable. Using facial recognition and other biometric technology on children can lead to misidentification, particularly for children of color, which can lead to unfair discipline, as well as chill children's freedom of expression. In utilizing this technology, private and government entities must acknowledge the unique vulnerabilities of children before determining whether to put it to use. They must carefully evaluate the negative consequences on students and put their well-being and privacy first. If the benefits do not significantly outweigh the consequences or potential consequences, schools should not utilize the technology.

IV. The Department of Education and the Federal Trade Commission should establish a working group to study the impact of biometric technology on children

Children and teens' unique vulnerabilities make the many concerns biometric technology such as facial recognition poses in the education context so important to address. As a first step, the Department of Education and the Federal Trade Commission should work together to establish a working group that brings key stakeholders together to further study the impact of this technology on children. This working group should include academic researchers, pediatricians, and children's advocates who have specific knowledge of children's development and tendencies. This would offer these agencies

[49] Jake Parker, Most state legislatures have rejected bans and severe restrictions on facial recognition, Security Info Watch (July 12, 2021).
[50] *Id.*
[51] Woodruff *supra* note 41.
[52] Press Release, NYCLU, New York creates first-in-the-nation moratorium on facial recognition in schools (Dec. 22, 2020).
[53] *Id.*

and OSTP with additional information on biometric technology that can be used to inform policy making and proposed regulations.

Conclusion

Common Sense appreciates the opportunity to provide information OSTP with information on how biometric technology is being used in the educational context. OSTP should be aware of the harms that can come from using this technology on children in schools, and encourage entities to use special care when doing so.

Respectfully submitted,
Irene Ly
Policy Counsel, Common Sense Media

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Computing Community Consortium at Computing Research Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Response to RFI on Public and Private Sector Uses of Biometric Technologies

Written by: David Danks (University of California, San Diego), Maria Gini (University of Minnesota), Odest Chadwicke Jenkins (University of Michigan), Daniel Lopresti (CCC and Lehigh University), Melanie Mitchell (Santa Fe Institute) and Katie Siek (Indiana University, Bloomington)

1. Descriptions of use of biometric information for recognition and inference: Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

The characterization of "biometric technology" is incredibly broad. There are many current uses of technology that seemingly qualify as biometric on this definition, but that we believe should not qualify. Parties are strongly encouraged to consider the convergence of data streams that create biometric knowledge. For example, a cognitive tutor (or similar EdTech system) arguably counts since it uses behavior (= student responses) to infer cognitive state (= subject knowledge). More contentiously, the recommendation engine underlying Amazon counts as biometric technology since it uses behavior (= user search terms & clicks) to infer cognitive state (= preferences).

Parties are also encouraged to consider how technology that is typically not utilized for biometrics can be harnessed to abstract similar biometric knowledge. For example, in smart homes for older adults, researchers determined that it was easier to use an ultrasonic sensor in a doorway to identify people instead of a gait sensor because the ultrasonic sensor could detect a person's height with the assumption that people with varying heights live together.

We don't think that NIST has these kinds of uses in mind, as the example behaviors are all physical ones and the example cognitive and/or emotional states are all highly effective ones. But we do believe that they are focused on what most people would consider "biometric technology" when the actual definitions that they give is much broader leading to a counterproductive definition.

[1] This material is based upon work supported by the National Science Foundation under Grant No. 1734706. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

2. Procedures for and results of data-driven and scientific validation of biometric technologies: Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

Existing practice in academia for publishing new research has generally involved testing on standard datasets that were collected when there was far less awareness about the serious privacy and ethical issues. The community depends on these datasets, and it's not clear whether it is broadly accepted that past practices are wrong and need to be changed. Already better benchmark datasets (most obviously, the dataset built by the Gender Shades project), have been developed but the community hasn't shifted to using those datasets. It will be extremely disruptive to tell researchers they can no longer use datasets they've been depending on for years. This could slow down the careers of young faculty members, and could delay the graduation of PhD students, but the transition has to happen and it seems likely government support will be needed to help facilitate this.

The entire community, including journal publishers and conference organizers, need to come together to map a way forward. Even measuring the amount of work it will take to transition the community to new datasets that meet the new ethical standards is going to be a challenge -- someone needs to do this work, and someone needs to fund it. Beyond this, there is also the question of which biometrics are appropriate to develop, and which are not (e.g., facial recognition, at least the way it's practiced now). In addition, evaluation needs to go beyond the current narrow focus which is entirely technical ("this method is 1% better than that method") and directly include the ethical issues -- datasets and evaluation measures need to be transparent and fair, and be calibrated to identify potential risks and damages. Researchers don't have the ability to control every use of the technology that they build, but there needs to be an increased effort to identify likely (or "easy") real-world uses of the system, since that is what really matters. Systems that perform well in the lab might predictably fail in the real-world, and researchers should bear some responsibility for thinking about "obvious" misuses.

Human computer interaction researchers investigated biometrics for emotional state awareness acceptance through wizard of oz studies and small pilot studies. Researchers utilized facial recognition during clinical encounters to help healthcare providers understand “non-verbal cues” of their patients - especially when providing difficult news. They found that healthcare providers appreciated viewing the emotional sensed data ambiently and reminded them to listen better, but some were concerned it may take their concentration away from their patients. Researchers created intervention applications with facial recognition for emotion detection for people with autism. The pilot studies are small because they are technology feasibility studies, however support

for creating more robust systems that can support larger studies are needed to understand the *in-situ* efficacy of these systems.

3. *Security considerations associated with a particular biometric technology. Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.*

There has already been some work in the security community on biometric technology, but one research area from this domain that deserves more attention is the creation and use of fake biometric data, which could be more dangerous than fake information. Particularly with regards to adversarial attacks that do not directly compromise the hardware (e.g., wearing glasses with particular patterns to deceive a face recognition system). There aren't many folks in the security community really thinking about these attacks and there are concerns about whether the Machine Learning researchers fully understand the security worries. Interestingly, there is a gap between the security community (which tends to be paranoid and worst-case) and the pattern recognition / machine learning community which develops and tests biometrics (which tends to be optimistic and average-case). The two research areas need to work closely together to achieve the proper equilibrium between the differing attitudes when developing and evaluating biometrics; government funding could help with this as well.

4. *Exhibited and potential harms of a particular biometric technology: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.*

There are a couple different facets to consider when viewing this problem. Some of this seems to be a matter of education. Researchers generally know when to trust and not trust a certain biometric, but those actually using biometrics in the field may place far too much trust in them and have no understanding at all of their failure modes. That can be very dangerous to society. Biometrics are also easily abused: developed for one specific purpose and validated in that context, but then applied for another purpose that may seem similar, but where there are significant differences that make the biometric inappropriate. When used for identification purposes, there may be false presumptions of uniqueness based on “conventional wisdom” as opposed to science. For example, in

the early stages of DNA fingerprinting there were overly broad statistical assumptions about uniqueness that had not yet been proved because not enough real-world data had been collected yet. This resulted in people being identified with an extremely high probability of having committed a certain crime. Juries can't understand the intricacies of statistics. It's unlikely that individual researchers will have data that is both broad enough and deep enough to understand the impacts on "edge cases" -- in this case, individuals or groups who are highly underrepresented in their data. There are huge questions that are hard to answer, such as who decides what margins of error are acceptable? And what recourse do individuals have when biometrics make an error that harms them? While questions such as these are basically impossible for individual researchers to answer, there is more that researchers can be doing to mitigate the risks. Researchers can't prevent all misuse, but they could potentially build into their system a "check" of whether the input had been significantly modified in various ways, and simply refuse to run on heavily manipulated images or video.

In addition, using biometric data for emotional inference is problematic and potentially harmful because the definition of specific emotions is based on the developers' interpretation, cultural norms, and the data set used. A cultural example would be nodding one's head from side to side - which may mean they disagree in some cultures, but in others it may mean they agree. An accessibility example would be someone with autism spectrum disorder not showing emotions as would be expected and thus a system misinterpreting their biometrics. Systems would need to process multiple and sometimes private data streams from an individual to appropriately interpret an individual's emotions, however this could introduce more privacy issues and personal harms.

6a. *Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case: Information regarding stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;*

Some individual researchers are working with stakeholder groups to tackle this issue, but it is usually to understand the needs of the biometric tech *owners/users*, rather than the needs of the *targets* of the biometric tech. There is a question of whether these engagement processes should/could lead to realization that a type of biometric tech ought not be researched or built? While it is impossible to prevent research on specific topics, certain biometric technologies could be forbidden by law. All industries and researchers engaging in biometric data and inference systems should have a compensated advisory board of public members (researchers, stakeholders including target users and humans who generate the data streams) who review upcoming studies, technologies, data, and discuss the implications. The industries and researchers should have to publicly respond to concerns of the advisory board. In addition, the associated research communities should also develop their own "ethics boards" who are well-versed in such issues, but this may prove challenging for organizations that are largely organized and run by volunteers.

Finally, federal funding agencies who fund biometric research and industry members who create biometric technologies should organize a unified, compensated review board that meets annually to review biometric research and technology developed and deployed to see if these types of systems are beneficial to society and potential harms and make recommendations to the relevant parties including federal policy makers.

6c. *Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;*

Likewise, it will be important to investigate the current standard practices of the research communities who collect and use standard datasets for developing new biometrics. As noted earlier, support will likely be necessary to help research communities to transition away from their existing datasets to new datasets that are more fair and less biased. Many of the other important issues mentioned here (disclosure, consent, review, security, sharing, storage, monitoring) fall on volunteers who are already overburdened and will probably require funding support to transition to better practices.

Biometrics are data from individuals - individuals who have limited bargaining power over the value of their data. We must rethink how individuals' data is collected, used, shared, and distributed to not only ensure there are no harms, but also to negotiate with industries on the use and financial gains of this personal data. The Computing Community Consortium (CCC) wrote a whitepaper in regards to this topic - Modernizing Data Control: Making Personal Digital Data Mutually Beneficial for Citizens and Industry.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Connected Health Initiative

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Suresh Venkatasubramanian
Assistant Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Connected Health Initiative Response to the Request for Information Regarding Public and Private Sector Uses of Biometric Technologies

I. Introduction and Statement of Interest

We write on behalf of ACT | The App Association's Connected Health Initiative[1] (CHI) to provide comments to the Office of Science and Technology Policy (OSTP) on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.[2]

CHI is the leading effort by stakeholders across the connected health ecosystem to clarify outdated health regulations, encourage the use of remote monitoring (RM), and support an environment in which patients and consumers can see improvement in their health. This coalition of leading mobile health companies and stakeholders urges Congress, the Administration, specialized agencies including the Office of the National Coordinator for Health IT (ONC), the Food and Drug Administration (FDA), the Centers for Medicare & Medicaid Services (CMS), and other regulators, policymakers, and researchers to adopt frameworks that encourage mobile health innovation using interoperable data while keeping sensitive health data private and secure. CHI supports OSTP's timely effort to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation.

[1] http://connectedhi.com.

[2] 86 FR 56300.

Care providers and patients (and others) who rely on innovative digital health products and services expect their valuable data is kept safe and secure, particularly their sensitive biometric data. The digital health community CHI represents practices and promotes responsible and efficient data stewardship to solve problems identified across consumer and enterprise health use cases. Patients, as well as stakeholders throughout the healthcare value chain, have strong data security and privacy expectations, and, as such, ensuring that the data collection and use practices reflect those expectations by utilising the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. CHI recognizes that privacy and security are a shared responsibility, and we serve as a leading resource in the biometrics and privacy space for thought leadership and education for the digital health ecosystem.

CHI recognizes the specific subsets of biometric data described by OSTP are the focus of this request for information. However, we strongly urge OSTP to recognize that the use of patient-generated health data (PGHD), which includes biometric data, is integral to the future of the American healthcare system. The demonstrated benefits of the monitoring and timely action on PGHD include reduced hospitalizations and cost, avoidance of complications, and improved care and satisfaction, particularly for the chronically ill.[3] For example, the Department of Veterans Affairs provides a compelling use case for the use of virtual chronic care management, which ultimately resulted in a substantial decrease in hospital and emergency room visits.[4] Emerging technologies like telemedicine tools, wireless communication systems, portable monitors, and cloud-based patient portals that provide access to health records are revolutionizing RM and asynchronous technologies.[5] Healthcare providers will also benefit from the potential of cost savings as a result of great responsible use of PGHD. Monitoring of PGHD demonstrably improves patient engagement dealing with chronic and persistent diseases to improve the management of such conditions.

Further, CHI urges OSTP to support the use of health data and PGHD through artificial intelligence (AI) in research, health administration and operations, population health, practice delivery improvement, and direct clinical care. The Administration's policies should contribute to the investment in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining AI systems with an eye

[3] *See* Hindricks, et al., The Lancet, Volume 384, Issue 9943, Pages 583 - 590, 16 August 2014 doi:10.1016/S0140-6736(14)61176-4.

[4] Darkins, Telehealth Services in the United States Department of Veterans Affairs (VA), *available at* http://c.ymcdn.com/sites/www.hisa.org.au/resource/resmgr/telehealth2014/Adam-Darkins.pdf.

[5] The global wearable medical devices market is expected to progress from US$2.73 bn in 2014 to US$10.7 billion by 2023, predicted to progress at a 16.40% CAGR from 2015 to 2023. See http://www.medgadget.com/2016/05/global-wearable-medical-devices-market-to-reach-us10-7-bn-by-2023-as-increasing-incidence-of-chronic-pain-creates-strong-customer-base.html.

toward ensuring value, ultimately offering a pathway for the voluntary adoption and integration of AI systems throughout the care continuum.

We believe OSTP shares CHI's vision of a seamless and interoperable healthcare ecosystem that leverages the power of PGHD, including biometric data, and can be realized through the trusted framework. Providers of health plans and the beneficiaries they serve now expect access to seamless and secure patient data across the care continuum, where "[i]ndividuals are able to seamlessly integrate and compile longitudinal electronic health information across online tools, mobile platforms and devices to participate in shared decision-making with their care, support and service terms."[6] We support, and urge new policy activities related to this request for information to align with, parallel efforts by this Administration to develop the trusted framework for the responsible use of PGHD, including but not limited to:

- ONC's development of an Interoperability Roadmap and PGHD framework;
- CMS' continued efforts to support and pay for tools in Medicare that leverage PGHD, and to advance important changes to the future value-driven Medicare system which will permit caregivers to incorporate PGHD into how they coordinate care and engage with beneficiaries; and
- The FDA's collaborative efforts to develop a governance framework for AI tools that meet the definition of a medical device under the Food, Drug & Cosmetic Act.

Notably, utilizing new and improved technology to ensure the confidentiality, integrity, and appropriate accessibility of data, such digital health tools allow for greater fraud and abuse detection, and would be of immense benefit to the Drug Enforcement Agency's electronic prescribing of controlled substances (EPCS) program. Further, the ongoing COVID-19 public health emergency (PHE) has necessitated reducing in-person contact as much as possible, which the EPCS program can assist with for those legally prescribed controlled substances. CHI believes the DEA should reduce the regulatory burdens associated with its biometrics requirements, especially those that ignore advancements in technology and have kept costs unnecessarily high for those who electronically prescribe controlled substances. These regulations currently prevent innovators, and particularly small business innovators, from participating in the EPCS market. For example, the capability exists today for iPhones to provide a biometric factor (e.g., fingerprint or face scan) as a first authentication, with a software application installed on the same phone providing a separate and distinct authentication (e.g., a soft token). Sadly, such a scenario is prohibited by DEA's interim EPCS rules with no discernable public benefit. CHI encourages reform to the EPCS program and urges the Administration's consideration of detailed CHI recommendations provided directly to the DEA.[7]

[6] ONC, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap* at 73.

[7] https://www.regulations.gov/comment/DEA-2010-0010-0157.

II. Responses to the Request for Information

OSTP's request for information (RFI) asks for input regarding two separate, but related categories of biometric technologies: 1) biometric recognition, which includes *verification* (one-to-one biometric matching) and *identification* (one-to-many queries that match an individual input against a larger database); and 2) biometric inference of cognitive and/or emotional states, such as mood or attentiveness. Below, CHI includes some findings on the two categories.

Biometric Recognition

Digital health innovators currently leverage numerous innovative biometric-assisted technologies, including facial verification, in order to provide services patients need and demand in the digital economy. Facial verification involves the comparison of a baseline, or "gallery", image against another image, the "comparison" or "probe" image, sometimes provided by the consumer's own device or by a device managed by the entity carrying out the comparison. Facial verification technologies are most often used for security purposes, i.e., to verify whether a person really is who they say they are. To share one key use-case, innovators currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log-in to apps using a scan of their face from the camera app. An app developer can choose integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.[8]

In recent years, academic and media reports have questioned the ethics and efficacy of various facial recognition technologies.[9] Often those reports discuss facial *identification*, the sub-set of facial recognition technologies that match an individual against a much larger database of images and which have struggled with accuracy rates, bias, and

[8] Apple, "About Face ID advanced technology", September 14, 2021, https://support.apple.com/en-us/HT208108

[9] *See e.g.,* Joy Buolamwini and Timnit Gebru "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research 81:1–15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", ACLU, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

questionable deployment strategies.[10] Facial verification currently programs, by contrast, are much more limited in scope and typically prove highly-reliable in testing. In its most recent Facial Recognition Vendor Test, the National Institute for Standards and Technology (NIST) found that the highest performing facial verification algorithms can achieve accuracy rates as high as 99.97 percent.[11] While those accuracy rates tend to drop when the image collection occurs in less controlled environments (for example, verification via cameras in a crowded airport terminal), collection for a use-case like Face ID is typically well-controlled. Notably, many facial identification algorithms also perform increasingly well on recent NIST tests, some showing marked improvements over just the past few years since the negative reports first surfaced. In its latest assessment of facial identification algorithms, NIST concluded that "at least 30 developers' algorithms outperformed the most accurate algorithm from late 2013."[12]

As the underlying technology continues to improve, digital health innovators are likely to implement a greater variety of facial recognition use-cases. Therefore, it will become increasingly important that regulation ensure that appropriate governance and accountability structures attach to each use-case commensurate with its risk. For example, in existing risk frameworks created by academics, targeted use of facial verification algorithms on a one-to-one basis typically represents a lower risk deployment, whereas real-time deployment of facial identification in public spaces is among the highest.[13]

CHI supports legislation to limit particularly risky uses of facial recognition technology and consistently advocates for a federal privacy law that would limit how companies can process consumer data without their consent,[14] and believes that a cross-sectoral risk-based framework for privacy will allow for the appropriately heightened steps to be taken for more sensitive data, including biometric data. Crafting rules that differentiate between targeted, consent-based uses of biometrics versus drag-net applications will be an important task for regulators going forward.

[10] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[11] https://pages.nist.gov/frvt/html/frvt1N.html

[12] https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

[13] Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Risk Framework", Georgetown Center Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/risk-framework

[14] ACT | The App Association, "Testimony of Morgan Reed, President at ACT | The App Association Before the U.S. Senate Committee on Commerce, Science, and Transportation on Protecting Consumer Privacy", September 19, 2021, https://actonline.org/wp-content/uploads/Reed-Testimony.pdf

Biometric Inferences of Cognitive or Emotional States

The collection of biometrics, including inputs that relate to or can infer cognitive or emotional states, holds both great promise and risk as one element in broader efforts to improve the quality of patient care in the United States. CHI seeks to advance responsible pro-digital health policies and laws that can harness the great potential of connected healthcare devices and tools, some of which may leverage biometric inputs, to unlock a higher standard of care for patients while minimizing potential harms.

One of the most exciting potential benefits of connected health technology is the ability of wearable devices that capture biometrics to improve equitable outcomes in healthcare. As co-creator of the Health Equity and Access Leadership ("HEAL") Coalition, a group comprising about 35 organizations spanning the health ecosystem, CHI recently co-released a report highlighting how wearable devices, among other innovations, can contribute to reducing the divides in health outcomes across racial lines.[15] As the report points out, access to traditional healthcare facilities, often stratified along income and racial lines, remains one of the major social determinants of health. The remote collection of health data through wearables can help ameliorate some of those disparities in access by allowing personalized diagnostics to occur outside of traditional healthcare institutions. For example, fitness trackers that collect valuable data, such as sleep patterns, activity and stress levels, can automatically share relevant information with clinicians, therapists, or coaches so that they can use granularized data to create more personalized care routines without requiring an in-person visit.

Connected health technologies that make use of biometrics to recommend cognitive or behavioral changes have shown efficacy in a number of different contexts to-date. For example, a trial of a mobile phone application that creates personalized behavioral interventions, including behavioral coaching, to improve for blood glucose control resulted in "substantially reduced glycated hemoglobin levels over 1 year."[16] The WellDoc mobile diabetes management platform also showed statistically significant improvements in A1c, in part due to behavioral recommendations.[17] Some studies have also shown significant mental health improvements among users of certain mental health apps, depending on the level of engagement of the user.[18]

In light of the COIVD-19 pandemic, many turned to digital health platforms, tools, and services to consult with caregivers in greater numbers as in an effort to avoid the risk of exposing themselves or others to the virus. Wearable ownership and use increased in 2020, with 43 percent of respondents using wearables in 2020, compared to 33 percent

[15] *See* Appendix 1.

[16] https://diabetesjournals.org/care/article/34/9/1934/38702/Cluster-Randomized-Trial-of-a-Mobile-Phone

[17] https://www.liebertpub.com/doi/pdf/10.1089/dia.2008.0283

[18] https://www.sciencedirect.com/science/article/abs/pii/S0165032717316786

in the year prior.[19] Additionally, during the COVID-19 public health emergency, more than half of all owners and users of wearables reported using them to manage a diagnosed health condition.[20] 62 percent of physicians reported in a recent study that they believe wearable devices would increase the overall quality of care for their patients.[21]

Clearly, usership of technologies that can pull biometrics and infer cognitive or emotional states will continue to increase, especially as efficacy improves and the benefits become clearer to users. CHI is keenly aware of the need to create appropriate guardrails to keep up with the growth of the industry and to ensure that mobile health players that collect sensitive biometric data continue to do so responsibly. Aside from advocating federal privacy legislation, as mentioned earlier, CHI continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of such AI innovations, including by developing Good Machine Learning Practices specifically for AI development and risk management of AI,[22] as well as targeted recommendations on how to improve transparency for caregivers and patients.[23]

[19] https://rockhealth.com/insights/digital-health-consumer-adoption-report-2020/

[20] Ibid.

[21] https://vitalconnect.com/5-key-attributes-medical-wearables-seeking-adoption-hospitals/

[22] The CHI's good machine learning practices for FDA-regulated AI are available at https://bit.ly/3gcar1e.

[23] The CHI's *Advancing Transparency for Artificial Intelligence in the Healthcare Ecosystem* is available at: https://bit.ly/3n36WO5.

III. Conclusion

CHI strongly supports risk-based guardrails around the use of biometrics that provide consumers and patients with a baseline level of trust and that set a clear set of expectations for the businesses that seek to do good through these services. While the technology offers incredible potential, we understand the risks of misuse are particularly high in this context.

We thank OSTP in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Matt Schwartz
Policy Associate

Leanna Wade
Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005

Advancing Health Equity Through Technology

November 2021

Produced in partnership with:

Consumer Technology Association™

ConnectedHealth

INTRODUCTION

Disparities in health are a long-standing issue in the United States due to the complex intersection of race, poverty, education quality and access, as well as the urban and rural divide. These disparities do not only affect the individuals and communities experiencing the disparities. They also impact overall health and well-being, and result in higher costs for health care across the country. The issue is particularly relevant today given the increasing diversity of the U.S. population coupled with worsening health outcomes in the country more broadly as compared to other developed nations.[1]

Not all people living in the United States have the same opportunities to pursue a healthy lifestyle and that people of color, people with disabilities and those living in rural and low-income areas often have worse health outcomes.

This is largely due to access barriers to high-quality health care and social determinants of health ("SDOH").

Social determinants of health are conditions in the environments in which people are born, live, learn, work, play, worship and age that affect health and quality-of-life outcomes and health risks.[2] Inequities in factors like education, financial stability and food security are all driving forces behind the health disparities that exist in the United States today.

For instance, income tracks closely with health outcomes. Although Blacks and Hispanics have higher rates of disease overall than non-Hispanic Whites, these differences are "dwarfed by the disparities identified between high- and low-income populations within each racial/ethnic group."[3] Blacks, Hispanics and American Indian/Alaska Native people with higher incomes have better health than those with lower incomes.

The impact of income disparities is reflected in health outcomes. Residents of high-poverty areas (county poverty rate greater than or equal to 20%) have a life expectancy of 76.7 years – 6.2 years shorter than the life expectancy for the residents of low-poverty areas (county poverty rate less than 5%). When stratified by gender, race and poverty level, life expectancy in 2012-2016 ranged from 71 years among Black men in high-poverty areas to 84.6 years among White women in low-poverty areas of the United States.[4] Similar trends can be seen along the urban-rural divide and among those with and without a high school diploma.

SOCIAL DETERMINANTS OF HEALTH

Examples of social determinants of health:

- Availability of resources to meet daily needs (e.g., safe housing and local food markets)
- Access to educational, economic, and job opportunities
- Access to healthcare services
- Quality of education and job training
- Transportation options
- Public safety
- Social support
- Socioeconomic conditions like concentrated poverty and the stressful conditions that accompany it
- Access to mass media and emerging technologies (e.g., cell phones, the internet, and social media)
- Residential segregation
- Language/Literacy
- Social norms and attitudes like discrimination, racism, and distrust of government
- Exposure to crime, violence and social disorder
- Culture

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Consumer Technology Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Consumer Technology Association
Comments on
OSTP Request for Information on Biometric Technologies and an AI Bill of Rights

Respondent Name: Consumer Technology Association
Respondent Type: Industry Association

I. Introduction

The Consumer Technology Association® ("CTA")®[1] respectfully submits these comments in response to the Office of Science Technology and Policy ("OSTP") request for information ("RFI") related to Public and Private Sector Uses of Biometric Technologies.[2] CTA supports OSTP's effort to understand the innovative potential of biometric technologies in considering whether an artificial intelligence ("AI") Bill of Rights ("AI Bill of Rights") is necessary.

CTA is pleased to share our members' perspectives regarding the development, use, and potential of biometric technologies. We believe that these tools present great opportunity to further consumer protection, reduce inequality, and improve quality of life for all Americans.

CTA supports efforts to ensure that biometric technologies and AI are designed, developed, used, and evaluated in a responsible manner. As CTA has previously explained, "these tools should be used carefully, subject to proper guardrails that promote beneficial uses while safeguarding against privacy and civil liberties harms."[3] Left untethered and in the hands of bad actors, these powerful technologies can pose risks to consumers. These risks are not consistent across technologies or contexts, but in fact vary depending on the use case, developer, and end user. The dual goals of developing responsible AI and enabling innovation are best served through an intentional commitment to develop and implement codes of conduct, voluntary standards, and best practices that complement developing or existing policy initiatives and encourage self-regulation. When based upon clear and targeted frameworks and principles, self-regulation can result in meaningful protection for users and profound innovation while minimizing potential bias and enhancing trustworthiness. OSTP has an opportunity with its AI Bill of Rights to present such a statement of principles, resulting in a flexible tool that adapts to changing technologies, rather than a rigid, quickly outdated set of fixed rules that neither encourages nor adapts to innovation. In addition, educational activities that enhance people's understanding concerning ethics related to biometric technologies are beneficial for extending an appropriate way of using these technologies.

[1] CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support millions of jobs. CTA owns and produces CES®—the largest, most influential tech event on the planet.

[2] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56300, Office of Science and Technology Policy (rel. Oct. 8, 2021).

[3] Consumer Tech. Ass'n, UNDERSTANDING FACIAL RECOGNITION AND BIOMETRIC TECHNOLOGIES: HOW TO PREVENT ABUSE AND PROTECT INNOVATION (2020), at 10.

Respectfully, CTA urges OSTP to consider a risk-based approach to an AI Bill of Rights, one that recognizes the variety of biometric technologies and leverages existing law, regulation, and best practices to match any potential new regulation to the degree of risk (and corresponding benefits) any particular biometric-based AI tool may create. This is necessary to ensure that the public, the economy, and the world can benefit from the tremendous potential of biometric technologies and AI, and to allow regulators to better understand and evaluate the potential costs, and benefits, of implementing a framework that may lead to new rules and restrictions on the development and use of AI.

II. Biometric Technologies Present Real and Potential Benefits to the Public.

The benefit of biometric technologies is incontrovertible. As CTA explained in its June 2020 report on facial recognition and biometric technologies, "biometric technologies are already offering consumers increased convenience, enhanced data security, and improved physical safety."[4] The potential benefits of biometric technologies are limited only by the imagination of entrepreneurs and engineers. We explore below examples of just a few of the many benefits to consumers:

a. **Accessibility**. Several companies use facial recognition and other biometric technologies to address challenges faced by individuals with a range of disabilities. For example, Aria, which provides tools to assist blind and low-vision individuals, has created specialized glasses to connect individuals with visual impairments with remote agents who can see the user's surrounding environment through the glasses and describe it to them in real time, increasing accessibility without compromising safety. Among other things, Aria's technology employs facial recognition tools to identify individuals nearby who are known to the user, allowing the remote agent to help the user interact fluidly with their colleagues, friends, and family. As another example, Intel developed an AI-powered motorized wheelchair allowing severely disabled users to use facial movement to direct the chair's movement, improving mobility and independence. As automated vehicles develop and expand, integration of biometric technology will allow individuals who otherwise would not be able to operate a vehicle independently to easily run errands, visit family and friends, and enjoy newfound mobility.[5]

b. **Public Safety**. Biometric technologies are used throughout public and private life to further personal and collective safety and security. Fingerprint/finger vein scanners, iris identification, and facial recognition tools can determine who is—and who is not—authorized to enter a property, building or room, for instance. Banks and other financial institutions look to facial recognition technology, and some are experimenting with fingerprint/finger vein technology, to prevent fraud and confirm identity[6] and prevent or

[4] *Id*. at 5.
[5] Norton Rose Fulbright, AUTONOMOUS VEHICLES: 'IT'S ALL ABOUT YOU!' THE INTEGRATION OF BIOMETRICS INTO AUTONOMOUS VEHICLES (2019).
[6] Mejia, Niccolo. *Facial Recognition in Banking – Current Applications*, EMERJ (Dec. 5, 2019), https://emerj.com/ai-sector-overviews/facial-recognition-in-banking-current-applications/.

solve ATM thefts.[7] To address vehicle theft, manufacturers are installing biometric recognition tools to determine who is permitted to start and drive a car or truck.[8] Driving on the streets is safer due to some vehicles' inclusion of face and posture analysis software that identifies inattentiveness, drowsiness, and other potential safety issues, alerting the driver so they can avoid accidents and stay safe.[9] Biometric technologies improve consumer security in their personal technology as well, such as fingerprint/finger vein scanners or face scans to open sensitive phone apps, verify identity, complete a transaction, provide enhanced cybersecurity, or sign into a personal device. Furthermore, consumers increasingly look to biometric technology to enhance their security in the home. Smart locks, security cameras, and other devices identify guests and family members thus giving consumers peace of mind and furthering protection of their homes and families.

c. **Travel Convenience and Safety**. U.S. Customs and Border Protection ("CBP") and the Transportation Security Administration ("TSA") have deployed facial recognition technologies to facilitate screening increasing volumes of travelers.[10] These systems help verify identities, furthering individual and collective security while enabling travelers to proceed quickly to their destination. Similarly, Japanese authorities began using facial recognition technology at Narita Airport in Tokyo in 2019, and announced plans to expand the program to additional airports.[11]

d. **Energy Efficiency**. Biometric technologies can significantly enhance individual and collective energy efficiency. For example, sensors embedded in clothing and furniture will allow for dynamic adjustment of temperatures within a home. Appliances and other facilities in the home could be automated to activate when sensors perceive the need and otherwise hibernate.[12] These efficiencies would be reliant on the use of biometric technology—and the development of the technologies itself requires the expansion and use of such technology.

e. **Healthcare efficiency.** Biometric technologies are in active use in the healthcare setting to improve patient experiences, assist care teams, and create efficiencies in diagnoses with remote patient monitoring. For example, several hospitals and care facilities have integrated in-room devices to enable patients to better communicate with their care teams

[7] Grant Jensen, How Banks and Financial Institutions Use Face Recognition to Protect People, Property, and Assets, BRIEFCAM (Jan. 14. 2021), https://www.briefcam.com/resources/blog/how-banks-and-financial-institutions-use-face-recognition-to-protect-people-property-and-assets/.
[8] Valentina Zezeli, *Face Recognition in Cars Improves Safety and Convenience*, VISAGE TECHNOLOGIES (Nov. 12, 2019), http://www.visagetechnologies.com/face-recognition-in-cars.
[9] *Id*.
[10] Dep't of Homeland Security, Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress (2016).
[11] *Six Major Airports in Japan Set to Adopt Facial Recognition Tech by 2020*, FUTURE TRAVEL EXPERIENCE (Jul. 16. 2019), http://www.futuretravelexperience.com/2019/07/six-major-airports-in-japan-set-to-adopt-facial-recognition.
[12] Katya Pivcevic, *Tech-based clothing, smart mirrors and biometrics in every room: our homes in 2071*, BIOMETRIC UPDATE (Jun 18, 2021), https://www.biometricupdate.com/202106/tech-based-clothing-smart-mirrors-and-biometrics-in-every-room-our-homes-in-2071.

and families,[13] and to share post-surgical data between at-home patients and their care teams.[14] Voice biomarkers may also assist in detecting certain conditions or even adverse issues within a patient's home. Additionally, care teams may leverage voice services for note capture during visits and paired with AI, voice technologies may help care teams with condition diagnosis and medical claims. Biometric technologies also expedited secure, authenticated, and efficient mechanisms for providers and patients to access appropriate records through proof of identity.

As noted above, biometric technology is not only used in the commercial sector but also used by public sector actors, including numerous federal agencies to help keep the public safe, enhance cybersecurity and national security, secure borders and improve the delivery of medical services. These and many other use cases were outlined in a recent GAO Report summarizing the many federal agencies that currently use this technology to fulfill their missions.[15] Thus, any accounting of the benefits of biometric technologies must also consider the increasingly important role of this technology to help government agencies fulfill critical missions and mandates.

III. Existing Law and Standards Protect Consumers.

A range of existing laws at the state, federal, and international level and robust industry and global standards help manage the risks of biometric technologies. We outline below just a few of the many ways the development and use of biometric technologies and AI are currently regulated and consumer harm alleviated:

a. **The FTC Act and State UDAP Statutes:** Section 5 of the Federal Trade Commission (FTC) Act prohibits "[u]nfair methods of competition" and "unfair or deceptive acts or practices in affecting commerce." Similarly, each state has its own corollary law or laws, referred to as "Unfair or Deceptive Acts or Practices" ("UDAP") statutes. The FTC, state attorneys general, and, in many states, private citizens can act against deceptive or unfair uses of information from biometric technologies and AI. Indeed, the FTC has already articulated its intention to use existing authority to ensure that AI tools, including those enabled by biometric technology are transparent, truthful and representative.[16]

b. **Federal and State Anti-Discrimination Laws:** The Civil Rights Act of 1964 bars employers from discriminating against applicants or employees on the basis of race, religion, sex, and national origin. The Act prohibits not only affirmative and intentional discrimination but also facially neutral practices with a disproportionate impact on

[13] https://www.fiercehealthcare.com/tech/alexa-finding-a-voice-healthcare-amazon-launches-service-to-help-hospitals-deploy-voice#:~:text=voice%20in%20healthcare.-,Cedars%2DSinai%2C%20Boston%20Children's%20sign%20on%20for,new%20Amazon%20smart%20hospital%20service&text=Using%20Amazon%20Alexa%20devices%20in,music%2C%20according%20to%20the%20company.

[14] https://www.healthcareitnews.com/news/boston-childrens-hospital-launches-amazon-alexa-app-kidsmd

[15] U.S. Gov't Accounting Off. Report, GAO-21-526, FACIAL RECOGNITION TECHNOLOGY, CURRENT AND PLANNED USES BY FEDERAL AGENCIES (Aug. 2021).

[16] Elissa Jillson, "*Aiming for truth, fairness, and equity in your company's use of AI*," F.T.C. (Apr. 19, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

protected classes. Many states have similar legislation. The Genetic Information Nondiscrimination Act prevents employers from using an applicant's or employee's genetic information as the basis for an employment decision. Other state and federal laws prohibit discrimination on the basis of pregnancy, age, disability, and citizenship. Individually and collectively, these laws help ensure that information collected using biometric technologies is not used inappropriately in employment-related decisions.

c. **Children's Online Privacy Protection Act ("COPPA"):** COPPA limits the ability of website operators and online service providers to collect personal information from children. This protects children from the online collection of their biometric information, and appropriately puts parents and guardians in the "driver's seat" around information collected about their children.

d. **California Consumer Privacy Act/California Privacy Rights Act ("CCPA"/"CPRA") and Other State Privacy Laws:** The CCPA and new, similar state privacy statutes (i.e., Colorado Privacy Act, Virginia Consumer Data Protection Act) impose a variety of obligations on companies that collect, process, and/or retain the personal information of individuals in their respective states. Among other things, companies must provide notice at or before the collection of personal information and allow residents the ability to "opt out" of any "sale" of their personal information, which includes biometric information. Each state considers "biometric information" sensitive personal information, which affords it greater protection. Colorado and Virginia even require that a company receive affirmative, opt-in consent to use biometric information.

e. **Illinois and Other State and Local Biometric Privacy Laws:** Illinois's Biometric Information Privacy Act ("BIPA") imposes a range of obligations on companies collecting biometric information, including requirements to: (1) obtain written consent before collecting biometric information; (2) securely store biometric information; (3) destroy biometric information in a timely manner; and (4) disclose their policies on information use and retention. BIPA contains a private right of action and has resulted in significant damage and injunctive relief settlements for consumers. Several other states and localities, including Washington, Texas, New York City, Portland, OR, San Francisco, Oakland, CA, and several cities in Massachusetts have similar laws regulating the use of biometric-based applications, generally, or facial recognition technology, specifically by private sector and public sector actors.

Further, existing laws and norms at the international and multi-national level address data protection and privacy, discrimination, and consumer protection related to biometric information. For example, companies operating in Europe are subject to certain notice, consent, and transparency obligations under the GDPR for any data processing of EU subjects' data. These laws are successful in protecting consumers, enabling recourse, and setting standards and compliance expectations for companies developing AI systems and using biometric technologies.

Any consideration of laws, standards and existing norms currently protecting consumers should also consider that biometric technologies are shaped and regulated not only by black-letter law,

but also by robust standards and governance practices developed by the industry and leading developers of this technology.

For example, CTA has contributed to and published numerous studies and standards regarding AI development, including CTA-2096 regarding developing trustworthy AI systems,[17] CTA-2089 regarding the definitions and characteristics of AI,[18] and the published standard CTA-2090 regarding the use of AI in healthcare and trustworthiness.[19]

The International Organization for Standardization and International Electrotechnical Commission published ISO/IEC JTC1 standards project 23894 regarding AI risk management,[20] the National Institute of Standards and Technology is creating an AI Risk Management Framework,[21] and the Organisation for Economic Cooperation and Development (OECD) is in the process of developing its own framework for assessing the opportunities and potential risks presented by different types of AI systems.[22] Thus, policymakers should recognize that these standards can provide a framework for acceptable uses that enable innovation while mitigating risks. Policymakers should also consider expanding voluntary testing and performance standards, and updating public sector best practices and guidance documents,[23] as means of achieving these goals.

IV. A Deliberate Approach that Balances Risks Against Benefits and Current Industry Safeguards and Practices Will Result in a Meaningful AI Bill of Rights that Will be Supported by Consumers and Industry.

An AI Bill of Rights could be a reliable tool for cultivating and protecting innovation while establishing common principles to address potential risks and harm. As OSTP develops its AI Bill of Rights, CTA recommends that OSTP leverage the protections afforded under existing law and industry safeguards, while also embracing the many benefits of biometric technology and AI tools already in the marketplace.

CTA suggests the following be considered as part of any AI Bill of Rights:

[17] Consumer Tech. Ass'n, *Guidelines for Developing Trustworthy AI*, CTA-2096 (Dec. 20, 2019), https://standards.cta.tech/apps/group_public/project/details.php?project_id=637.

[18] Consumer Tech. Ass'n, *Definitions and Characteristics of Artificial Intelligence*, CTA-2089 (Mar. 4, 2020), https://standards.cta.tech/apps/group_public/project/details.php?project_id=601.

[19] Consumer Tech. Ass'n, *The Use of Artificial Intelligence in Health Care: Trustworthiness*, ANSI/CTA-2090 (Feb. 2021), https://shop.cta.tech/products/the-use-of-artificial-intelligence-in-healthcare-trustworthiness-cta-2090.

[20] Int'l Org. for Standardization and Int'l Electrotechnical Commission, *Artificial Intelligence Risk Management*, ISO/IEC JTC 1/SC 42.

[21] Nat'l Inst. Sci. Tech., AI RISK MANAGEMENT FRAMEWORK CONCEPT PAPER (Dec. 13, 2021); Nat'l Inst. Sci. Tech., Docket 21076-01510, 86 Fed. Reg. 40810, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (Jul. 29, 2021).

[22] OECD, FRAMEWORK FOR THE CLASSIFICATION OF AI SYSTEMS – PUBLIC CONSULTATION ON PRELIMINARY FINDINGS (2021), https://aipo-api.buddyweb.fr/app/uploads/2021/06/Report-for-consultation_OECD.AI_Classification.pdf.

[23] *See, e.g.*, Dep't of Justice, Bureau of Justice Assistance, FACE RECOGNITION POLICY DEVELOPMENT TEMPLATE FOR USE IN CRIMINAL INTELLIGENCE AND INVESTIGATIVE ACTIVITIES (Dec. 2017); F.T.C., FACING FACTS, BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012).

a. **Risk-Attentive.** Not all biometric technologies and AI systems present equivalent potential risk to all consumers; risk is context-specific, implementation dependent, and potential harm may significantly vary from user to user. CTA urges OSTP to recognize that the diversity and variety in biometric technologies and AI demands a flexible approach to evaluate risk associated with specific uses. A risk-benefit analysis may be more meaningful in this context than hardline standards.

b. **Incorporation of Existing Laws and Standards.** The AI Bill of Rights should leverage existing and proven laws and standards by: (a) incorporating a focus on compliance with existing applicable law; and (b) emphasizing that industry groups, jurisdictions, or other actors should be encouraged to self-regulate; and (3) acknowledging that existing laws already establish important ground rules when developing self-regulatory standards or any potential new regulation. Leveraging existing law not only ensures that the public and businesses understand their rights and responsibilities but also furthers the efficient implementation of any AI Bill of Rights. Businesses can utilize their existing governance processes to ensure compliance with existing laws, resulting in further efficiency and cost reduction as they ensure their practices are aligned with an AI Bill of Rights and aligned with perceived and actual risk that will enhance the deployment, adoption, and use of biometric technologies and AI systems.

c. **Nuanced.** The AI Bill of Rights should recognize the benefits of technological innovation and broad data collection, including of biometric information, where such collection is consistent with existing legal requirements. Appropriate collection and incorporation of additional and varied data inputs will improve AI systems and help address and mitigate potential and harmful bias over time. Better functioning AI (i.e., AI trained on greater amounts and more diverse data, and deployed with appropriate considerations and mitigations) can provide further benefits to the public, such that the AI systems produce more accurate, trustworthy, and ethical outputs. Without sufficient and varied data inputs, desirable outputs may remain unattainable and consumer distrust of the technologies may thwart further development and deployment.

d. **Flexible.** The AI Bill of Rights must be flexible. An extensive, costly (double-digit) compliance process before biometric technology or an AI system can be developed or used may not be appropriate across applications and instances without regard to inherent or perceived risk, including ***lack of*** risk. Overly prescriptive rules may stifle innovation and foreclose use of this technology, especially for those applications where possible harm is minimal.

e. **Iterative.** References to a "Bill of Rights" connote fixed, "Constitutional" standards in the American imagination. Such an approach for an AI Bill of Rights would be significantly and harmfully out-of-step with the reality of technological development, innovation, and the actual and potential benefit of biometric technology and AI. CTA emphasizes that, as technology develops, policies and regulations must be able to change. While a Bill of Rights could be a statement of principles regarding biometric technology and AI development, OSTP should emphasize that it is only the start of a process that

will require additional data, evidence, and robust risk-benefit analyses. Further iterations of a Bill of Rights and any resulting recommendations should recognize these complexities. OSTP might consider an incremental and iterative process for a Bill of Rights development: a series of drafts leading to an initial Bill of Rights, with a clear statement that the Bill of Rights is intended to evolve as technology changes.

V. Conclusion

The development and deployment of biometric technologies present immense and transformative benefits for society. CTA is a proud, active participant in the global conversation regarding the regulation of these technologies. We commend OSTP's efforts to join this dialogue and believe an AI Bill of Rights can serve as a helpful synthesis of principles enshrined in law and recognized by industry. The United States is a hub for the development of biometric technology and AI; we must preserve our leadership and culture of innovation, while ensuring that we protect consumers as AI systems become increasingly interwoven in all aspects of our everyday professional and personal lives.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Courtney Radsch

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

OSTP BIOMETRIC TECHNOLOGIES CONSULTATION: FOCUS ON GLOBAL GOVERNANCE OF FACIAL RECOGNITION TECHNOLOGIES

Submitted by Dr. Courtney C. Radsch, Fellow UCLA Institute for Technology, Law and Policy
With Research Assistants
Bharath Gurugavendran, Leo Pu-Cheng Huang, and Lucía Chibán Zamar

As the OSTP embarks on its review of biometric technologies, we would like to highlight facial recognition as a specific type of biometric technology used for identify verification, identification of individuals and groups, and inference of attributes (including protected status). Given the pervasiveness of facial recognition technology as well as the grave risks posed by its unfettered proliferation and the lack of regulatory frameworks to govern its use and development in the United States, we have conducted a global survey of relevant regulations to inform the OSTP's request for information. This submission includes an analysis of principles and regulatory frameworks elaborated by the United Nations, the European Commission, and national frameworks in Argentina, Australia, Brazil, India, Japan, México, South Africa, and the UK. The specific details of various legislation and regulation is included as an appendix.

As a scholar-practitioner working at the nexus of media, technology, and human rights for the past two decades, most recently as Director of Advocacy at the Committee to Protect Journalists and now as a Fellow at ITLP, I have seen first-hand the impact that new surveillance technologies can have on a wide range of human and civil rights, often affecting the most vulnerable and marginalized populations as well as those on the frontlines of promoting and protecting these rights, such as journalists and human rights defenders.

Similarly, technologies and legal frameworks developed in the United States have profound implications not just on its citizens, but on populations around the world. Therefore, we urge the OSTP to adopt the guidance provided by international standards and learn from other countries that have already adopted legal frameworks to govern the development and deployment of facial recognition technologies.

At the very core is the State obligation to protect human rights and for States and the private sector to comply with the principles of legality, necessity, and proportionality. Comprehensive human rights due diligence, increase transparency by adequately informing the public and affected individuals, and enabling independent and external auditing of these automated systems.

The international standards promulgated by the United Nations and the European Commission require that the processing of biometric data in facial recognition systems be authorized on an appropriate legal basis that complies with the general principles of legality, necessity and proportionality. To this end, States must address detailed explanations of the specific use and purpose for its deployment that takes into consideration the minimum reliability and accuracy of

the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria and the traceability of the process (among other factors).

Other important aspects to take into consideration in the design and use of this technology involve having data protection systems by default; processors that provide sufficient safeguards and act only on instructions from the data controller; maintenance of a record of processing activities; and a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

Country	Key Principles for the U.S.
United Nations	Processing of personal data must be authorized by an **appropriate legal basis**, complying with the general principles of **legality**, **necessity** and **proportionality**.
European Union	Processing personal data must meet the **proportionality** and **necessity** principles, the principle of processing personal data on **valid legal basis.** In determining proportionality and necessity, the legal framework should address notably: *the detailed explanation of the specific use and the purpose; the minimum reliability and accuracy of the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria; the traceability of the process; the safeguards.* Different tests of necessity and proportionality can be legally addressed "depending on whether the purpose is **verification or identification**, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected."
Argentina	N/A
Brazil	Processing of personal data on security and public safety purposes "shall be governed by specific legislation, which shall provide **proportional** and **strictly necessary** measures for fulfilling the public interest, subject to due legal process"
Mexico	Any responsible party that intends to process sensitive personal data **must carry out an "impact assessment"** on the protection of personal data, and submit it for review by the relevant authorities
South Africa	Personal information must be processed **lawfully**, and a reasonable manner that does not infringe the privacy of the data subject. Personal information may only be processed **if the purpose for processing is adequate, relevant, and not excessive.**

	Personal information must be **collected directly** form the data subject unless certain exceptions are met.
Japan	N/A
India	The Supreme Court of India has clarified that any law that encroached upon the right to privacy would be subject to constitutional scrutiny and would have to meet the three-fold requirement for: **Legality**, **Necessity**, and **Proportionality**.
United Kingdom	N/A
Australia	Collecting sensitive information about an individual must receive **consent** and the information is **reasonably necessary**

APPENDIX: LEGAL ANALYSIS OF

FACIAL RECOGNITION TECNOLOGY GOVERNANCE GLOBALLY

1. Facial recognition under United Nations standards

The right to privacy is stipulated in Article 12 of the Universal Declaration of Human Rights[1] and in Article 17 of International Covenant on Civil and Political Rights[2].On the report *The right to privacy in digital age*[3], the OHCHR highlights that advances in the field of biometric recognition technology have led to its increasing use by law enforcement and national security agencies. What raises serious concerns is that these processes are deployed by authorities across the globe and increasingly carried out in real time and remotely.[4] "Some of these concerns reflect the problems associated with predictive tools, including the possibility of erroneous identification of individuals and disproportionate impacts on members of certain groups. Moreover, facial recognition technology can be used to profile individuals on the basis of their ethnicity, race, national origin, gender and other characteristics."

Furthermore, remote biometric recognition directly impacts on the right to privacy, as it reveals unique characteristics and key attributes of personality. This function has led many States authority to "systematically identity and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement."[5]

Also, this type of artificial intelligence has served a security purpose to decide whether people's emotional and mental state from their facial expressions and other "predictive biometrics" deduced from the system constitute a security threat.[6] In this sense, "facial emotional recognition

[1] Article 12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

[2] Article 17 states that "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks." https://www.un.org/en/about-us/universal-declaration-of-human-rights

[3] OHCHR. Report "The right to privacy in the digital age". 2021. https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx.

[4] Paragraph 25 of the Report "The right to privacy in the digital age".

[5] Paragraph 27 of the Report "The right to privacy in the digital age".

[6] Paragraph 28 of the Report "The right to privacy in the digital age".

systems operate on the premise that it is possible to automatically and systematically infer the emotional state of human beings from their facial expressions, which lacks a solid scientific basis."

In the report, the High Commissioner recommends States to impose a moratorium on the use of biometric technologies in public spaces, at least until authorities can demonstrate that there are no significant issues with accuracy or discriminatory impacts and that these AI systems comply with robust privacy and data protection standards.[7]

The Special Rapporteur on freedom of opinion and expression stated that when these technologies are used for surveillance purposes, they can directly impact on human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation.[8] In this regard, the Special Rapporteur urged States to adopt national measures that are consistent with international human rights standards and that serve to protect individuals from unlawful surveillance. In particular, he urged "development of public mechanisms for approval and oversight of surveillance technologies; strengthening of export controls; and assurance of legal tools of redress."[9]

The Special Rapporteur on freedom of opinion also expressed that the use of these technologies is marketed and supported by private companies, who appear to be operating without constraint.[10] Therefore, "it is critical that companies themselves adhere to their human rights responsibilities, including by disclosing their transfers, conducting rigorous human rights impact assessments, and avoiding transfers to States unable to guarantee their compliance with their human rights obligations."

In this regard, the High Commissioner expressed that both States and businesses "should ensure that **comprehensive human rights due diligence** is conducted when AI systems are acquired, developed, deployed and operated, as well as before big data held about individuals are shared or used. As well as resourcing and leading such processes, States may also require or otherwise incentivize companies to conduct comprehensive human rights due diligence."[11]

The report of the High Commissioner also recommends States to dramatically increase the **transparency** of their use of AI, including by adequately informing the public and affected individuals and enabling independent and external auditing of automated systems. The more likely

[7] UN. *Urgent action needed over artificial intelligence risks to human rights*. September 15, 2021. https://news.un.org/en/story/2021/09/1099972

[8] Report "Surveillance and Human Rights", of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.. May 18, 2019. https://www.undocs.org/A/HRC/41/35

[9] Id. Supra.

[10] OHCHR. *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools*. June 25, 2019. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

[11] Paragraph 48 of the Report "The right to privacy in the digital age".

and serious the potential or actual human rights impacts linked to the use of AI are, the more transparency is needed.[12]

With respect to the use of facial recognition and surveillance technologies to track and control specific demographic groups, the Committee on the Elimination of Racial Discrimination raises concern when profiling people based on race, color, national or ethnic origin or gender, since it has been demonstrated that the accuracy of facial recognition technology may differ depending on the color, ethnicity or gender of the persons assessed, which may lead to discrimination.[13]

Therefore, States should carefully assess the potential human rights impact prior to employing facial recognition technology, which can lead to misidentification owing to a lack of representation in data collection. "Before national deployment, States should consider a pilot period under the supervision of an independent oversight body that is inclusive of individuals who reflect the diverse composition of the population, to mitigate against any potential instances of misidentification and profiling based on skin color."

2. Facial recognition under European Commission standards

The European Commission is based on the rule of law.[14] This means that every action taken by the EU is founded on treaties that are binding for EU member countries. Under these treaties, EU institutions can adopt legislation, which the member countries then implement.[15] The European Commission is the EU's politically independent executive arm. It is alone responsible for drawing up proposals for new European legislation.[16] The Council of Europe is the continent's leading human rights organization. It includes 47 member states, 28 of which are members of the European Union.[17] In relation to the conventions adopted by the Council of Europe, their legal existence is owed by the consent of those member States that sign and ratify them.

- **Convention for the protection of individuals with regard to the processing of personal data - Convention 108 +** The Convention for the protection of individuals with regard to the processing of personal data (Convention 108+)[18] is the only legal binding multilateral instrument which protects individuals with regard to the processing of their personal data, thereby contributing

[12] Paragraph 55 of the Report "The right to privacy in the digital age".
[13] Committee on the Elimination of Racial Discrimination. *General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials.* December 17, 2020. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=6&DocTypeID=11
[14] https://ec.europa.eu/info/law/law-making-process/types-eu-law_en
[15] https://european-union.europa.eu/principles-countries-history/principles-and-values/founding-agreements_en
[16] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/european-commission_en
[17] https://www.coe.int/en/web/yerevan/the-coe/about-coe
[18] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy. "Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data."[19]

This Convention stipulates core protection principles when processing personal data, related to the legitimacy of data processing, "such as the proportionality and necessity, the principle of processing personal data on valid legal basis, for explicit, specified legitimate purposes and to the quality of data (Article 5), special categories of data (Article 6), data security (Article 7), transparency (Article 8), accountability measures such as privacy by design, data protection impact assessments (Article 10), and new generation of data subject's rights such as the right not to be subject to a decision based solely on automated processing, right to know the reasoning of the processing, right to object (Article 9)."[20]

Regarding special categories of data, Article 6 of the Convention states that biometric data uniquely identifying a person "shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention", and that "such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."

Under this provision, processing of biometric data is also considered sensitive when it is precisely used to uniquely identify the data subject, and therefore has the potential to adversely affect data subjects' rights when it is processed for specific information it reveals.

In order to prevent adverse effects for the data subject, processing of sensitive data for legitimate purposes needs to be accompanied by "appropriate safeguards", such as "a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted".[21]

As appropriate safeguards, necessity has to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects. This legal framework should, according to each different use, address notably: the detailed explanation of the specific use and the purpose;

[19] https://www.coe.int/en/web/data-protection/convention108/background

[20] Submission by the Data Protection Unit of the Council of Europe to the OHCHR for the preparation of the thematic report on "the right to privacy in the digital age"

[21] Explanatory Report on Convention 108+

the minimum reliability and accuracy of the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria; the traceability of the process; the safeguards.[22]

Guidelines for facial recognition technologies

In January 2021, the Council of Europe's Committee of Convention 108 drafted guidelines for facial recognition technologies.[23] The guidance was drawn up for government and private entities, as well as facial recognition developers, manufacturers and service providers. The Guidelines call for strict rules to avoid the significant risks to privacy and data protection posed by the increasing use of facial recognition technologies.[24]

Principal guidelines for legislators and decision makers:

1. Strict Limitation by Law of Certain Uses

According to the Guidelines, the use of live facial recognition technologies in uncontrolled environments -as places freely accessible to individuals-, in light of the intrusiveness it bares upon the right to privacy and the dignity of individuals, coupled with a risk of adverse impact on other human rights and fundamental freedoms, should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis.

The use of facial recognition for the sole purpose of determining a person's skin color, religious or other beliefs, sex, racial or ethnic origin, age, health condition or social condition should be prohibited unless appropriate safeguards are provided for by law to avoid any risk of discrimination.

Similarly, affect recognition (attempted to identify or classify human emotions) can also be carried out with facial recognition technologies to arguably detect personality traits, inner feelings, mental health or workers' engagement from face images. Linking recognition of affect, for instance, to hiring of staff, access to insurance, or education may pose risks of great concern, both at the individual and societal levels and should be prohibited.

1.1. Integrating Digital Images to the Facial Recognition Technologies

[22] Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data. Guidelines on Facial Recognition. January, 2021.
[23] Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data. Guidelines on Facial Recognition. January, 2021.
[24] Lexology. Council of Europe's useful guidance concerning facial recognition. March 15, 2021. https://www.lexology.com/library/detail.aspx?g=c068fce0-e8fa-45fa-b90a-5296a78e2fc8

Legislators and decision-makers shall ensure that images available in a digital format cannot be processed to extract biometric templates or to integrate them into biometric systems without a specific legal basis for the new processing, when those images were initially captured for other purposes (from social media for instance).

Legislators and decision-makers should ensure that existing databases of digital image initially used for other purposes can only be used to extract biometric templates and integrate them into biometric systems when it is for overriding legitimate purposes and it is provided by law and strictly necessary and proportionate for these purposes (for instance law enforcement or medical purposes).

1.2. Use of Facial Recognition Technologies in the Public Sector

Different tests of necessity and proportionality can be legally addressed “depending on whether the purpose is verification or identification, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected.”

Biometric data processed by facial recognition technologies for identification purposes in a controlled or uncontrolled environment should be generally restricted to law enforcement purposes, and it should be carried out solely by the competent authorities in the security domain.

For these purposes, a strict test of both necessity and proportionality must be observed in the design, deployment, and use of facial recognition technologies in an uncontrolled environment. In this sense, clear parameters should be followed by law enforcement authorities when creating databases for specific, legitimate, and explicit law enforcement purposes.

Furthermore, given the intrusive nature of these technologies, in the deployment phase of live facial recognition technologies, laws should ensure that enforcement authorities demonstrate that factors such as location and timing justify the strict necessity and proportionality for its use.

In cases other than law enforcement, legislators and decision-makers must consider an explicit and precise legal basis for safeguards in the processing of biometric data. For verification purposes, the necessity and proportionality test should take into account the vulnerability of data subjects and the nature of the environment in which these technologies are being deployed.1.3. Use of Facial Recognition Technologies in the Private Sector

The use of facial recognition technologies by private entities, except for private entities authorized to carry out similar tasks as public authorities, requires according to Article 5 of Convention 108+ the explicit, specific, free, and informed consent of data subjects whose biometric data is processed.

Considering the requirement for such a consent of data subjects, the use of facial recognition technologies can only take place in controlled environments for verification or for authentication or for categorization purposes. Private entities shall not deploy facial recognition technologies in uncontrolled environments, especially to identify persons of interest, for marketing purposes or for private security purposes.

- **GDPR and Facial Recognition Technology**

Under the GDPR, data collected by FRT is classified as biometric data, which is prohibited to be processed for identification purposes. However, according to Article 9(2), there are some exceptions:

(1) The data subject has given explicit consent to the personal data processing; or
(2) The data processing is necessary for reasons of significant public interest. Article 9(2)(g).

The provision implies that the use of FRT is only possible when legal consent is obtained in accordance with the GDPR. Companies looking to use FRT should establish definitive legal grounds prior to the technology implementation.

Also, to establish the necessity for processing biometric data to identify a person, the GDPR requires "a systematic description of the envisaged processing operations and the purposes of the processing" and "an assessment of the necessity and proportionality of the processing operations in relation to the purposes." *See* Article 35.

Furthermore, before data processing, one has to collect the data. According to the Article 5(1)(a) of the GDPR, "it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed."

Finally, in processing the data, one has to abide by the "principle of data security." That is, the data must be processed in a manner that ensures appropriate security for personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (Article 5(1)(f) GDPR). Further, the principle can also be found in Article 32 of the GDPR which prescribes that the controller and processor should implement proportionate technical and organizational measures to prevent that personal data is disclosed to, or accessed by, unauthorized persons or organs.[25]

- ***The AI Act (a draft law currently being negotiated in the European Union)***

[25] See https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf).

The European Commission presented the Artificial Intelligence Act, which seeks to establish high standards for the regulation of the use of AI in Europe. It sets out core horizontal rules for the development, trade and use of AI driven products, services and systems within the EU, and it applies to all industries (the legislation is not sectoral in nature).

The Act introduces a sophisticated product safety regime that is constructed around a set of 4 risk categories. It stipulates that a mandatory CE-marking procedure is a prerequisite for market entrance and certification of High-Risk AI systems. It combines a risk-based approach (based on the pyramid of criticality) with a layered enforcement mechanism. The strictness of the rules is directly proportional to the nature of the risk. And it stipulates that there must be a ban on applications that have unacceptable risk. Fines for violating the rules can be up to 6 percent of the global turnover for companies.

Objectives:

1. ensure that AI systems are safe and respect existing law on fundamental rights and Union values;
2. ensure legal certainty to facilitate investment and innovation in AI;
3. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation

Unacceptable Risk AI systems are any AI systems that are considered a clear threat to the safety, livelihoods and rights of people. This includes AI applications that manipulate human behavior to circumvent users' free will and systems that allow 'social scoring' by governments.

High risk AI systems are AI applications used in : a) critical infrastructure (transport), b) essential private and public services, c) law enforcement, d) migration asylum and border control management, e) administration of justice and democratic processes, (among other designated High Risk AI uses)

The AI Act imposes strong obligations on these High Risk AI systems prior to market deployment:

a) Adequate risk assessment and mitigation systems
b) High Quality of datasets
c) Logging of activity to ensure traceability of results
d) Detailed documentation (both of information and purpose) to authorities for compliance
e) Appropriate human oversight to minimize risk
f) High level of robustness, security, and accuracy

All remote biometric identification systems are considered high risk and subject to strict requirements. **And the Act does stipulate a prohibition in principle of the live use of such identification systems (AFR) in publicly accessible spaces for law enforcement purposes.** There are however, limited exceptions such as in the case of a missing child, or to prevent a specific

and imminent terrorist threat, or to identify or prosecute a perpetrator or suspect of a serious criminal offence. It is required however, that a judicial or other independent body authorize these searches, and set appropriate limits in time, geographical search and the databases searched.

- ***The European Parliament's Resolution (that strongly recommended bans on multiple use cases of AFR technology, specially in the context of law enforcement and judicial use. 2020/2016(INI))***

The European Parliament called for a ban on the police use of facial recognition technology in public places, and on predictive policing. In an EU resolution on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters, the Parliament adopted by 377 votes to 248 (with 62 abstentions). It outlined the important considerations that stand to be violated as a result of using AI for law enforcement use. The voting record on this non-binding resolution is useful as it's a useful way to predict the nature of the negotiations that are liable to (Salient points among the 36 operative sections of the Resolution are given below):

1) Respect for Fundamental Rights: The EU Legal Framework on data protection and privacy must be fully respected and should form a basis for any future regulation of AI for law enforcement and judicial use, and when AI solutions stand to be incompatible with fundamental rights, they ought to be prohibited. (AI solutions need to respect the principles of human dignity, non-discrimination, freedom of movement, the presumption of innocence, and the right of defense, and other salient rights in accordance with the Charter and the European Convention on Human Rights

2) Risk of discrimination: The EU Parliament called for algorithmic explainability, transparency, traceability, and verification as a necessary part of the oversight mechanism, to ensure that the development, deployment and use of AI systems for the judiciary and law enforcement comply with fundamental rights, and are trusted by citizens, as well as in order to ensure that results generated by AI algorithms can be rendered intelligible to users and to those subject to these systems, and that there is transparency on the source data and how the system arrived at a certain conclusion

3) Mandatory Impact Assessments: Calls for a compulsory fundamental rights impact assessment to be conducted prior to the implementation or deployment of any AI systems for law enforcement or the judiciary, in order to assess any potential risks to fundamental rights; recalls that the prior data protection impact assessment is mandatory for any type of processing, in particular, using new technologies, that is likely to result in a high risk to the rights and freedoms of natural persons and is of the opinion that this is the case for most AI technologies in the area of law enforcement and judiciary

4) Stresses that only robust European AI governance with independent evaluation can enable the necessary operationalization of fundamental rights principles; calls for periodic mandatory auditing of all AI systems used by law enforcement and the judiciary where there is the potential

to significantly affect the lives of individuals, by an independent authority, to test and evaluate algorithmic systems, their context, purpose, accuracy, performance and scale, and, once they are in operation, in order to detect, investigate, diagnose and rectify any unwanted and adverse effects and to ensure the AI systems are performing as intended

5) Supports the recommendations of the **Commission's High-Level Expert Group on AI** that advocated for a ban on AI-enabled mass scale scoring of individuals

6) The resolution also expressed great concern over the use of private facial recognition databases by law enforcement actors and intelligence services such as Clearview AI. It additionally called on Member States to oblige law enforcement actors to disclose whether they are using Clearview technology or other equivalent technologies from other providers. It referenced another **opinion of the European Data Protection Board** that the use of services such as Clearview by law enforcement authorities would likely be inconsistent with the EU data protection regime.

- **Legal Provisions within the broader context of the EU's multi-level framework (specifically, the Charter of fundamental rights, and the Law Enforcement Directive)**

The use of FRT implies the processing of data for the purpose of identification. It's use by public authorities will entail an infringement of Art. 8 (Charter of fundamental rights of the European Union) as it violates the right to data protection (the use of the technology will have to comply with Art. 8(2)). It also has the capacity to interfere with the right to private life under article 7 CFR.

The Law Enforcement Directive is a piece of EU Legislation that is parallel to GDPR, and it deals with the processing of personal data by data controllers for 'law enforcement purposes' - which typically falls outside the scope of GDPR. It effectively provides rules on the protection of natural persons (w.r.t. processing of personal data by competent authorities) for the specific purpose of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the protection against threats to public security and its prevention. Several obligations under the Law Enforcement Directive are identical to those under GDPR.

Some of the important obligations include:

1) Implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive (Art. 19)
2) Implement data protection by design and by default (Art. 20)
3) Use processors that provide sufficient guarantees and act only on instructions from the data controller (Art. 22)
4) Maintain a record of processing activities (Art. 24)
5) Implement logging measures (Art. 25)
6) Cooperate with the supervisory authority in performance of its tasks on request (Art. 26)

7) Carry out a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons (Art. 27)
8) The requirement to notify a supervisory authority of a personal data breach without delay (where feasible no later than 72 hours after having become aware) (Art. 30)
9) Communicate the personal data breach to the data subject without undue delay (where the breach is liable to result in a high risk to their rights and freedoms) (Art. 31)
10) To make a clear distinction between personal data of different categories of data subjects, e.g., a) persons convicted of a criminal offence, b) victims of a criminal offence, c) other parties to a criminal offence (Art. 6)
11) Processing of the data must be lawful, i.e., necessary for the performance of a task carried out by a competent authority (Art. 8)
12) Processing of special categories of data is allowed only when strictly necessary Art. 10

3. Argentina

The National Constitution enshrines the right to privacy as a fundamental right in Articles 18 and 19 and boasts a robust — although outdated — data protection regime, through Article 43 of the Constitution and National Law Nº 25.326 on the protection of personal data[26]. It is also a signatory to Convention 108+ 183 and the European Commission recognized Argentina as having an adequate level of data protection in 2003, through decision 2003/490 EC.[27]

Unfortunately, these laws have proven to be insufficient to protect citizens from state surveillance. "Governments use the exceptions in these laws as legal bases for the deployment of surveillance programs for the normal exercise of state functions, service improvement, and public safety."[28]

In Argentina, there is no federal law regulating government **use of face surveillance technology**. However, deployment of facial recognition technology for public safety purposes is currently underway in the following provinces and municipalities:

1. Ciudad Autónoma de Buenos Aires: is the only district where the legislative branch passed an amendment to the Law No. 5688 on Integral Public Security System, In September 2020, the Legislature issued Law No. 6339, that incorporated the Fugitive Facial Recognition System (the "Recognition System") on the Public Security System. The objective of the Recognition System is to recognize the faces of people sought by the authorities as a result of a court order that have been registered in the Databases of the

[26] Law no. 25.326 on the protection of personal data. Approved on October 4, 2000. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[27] EUR-Lex. Document 32003D0490. 2003. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32003D0490
[28] Access Now. *Surveillance Tech in Latin America*. August, 2021. https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Coworker

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 18, 2022
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

VIA EMAIL
BiometricRFI@ostp.eop.gov

Re: Comments of Coworker.og on RFI Response: Biometric Technologies

Coworker.org welcomes this public consultation by the White House Office of Science and Technology Policy (OSTP) on public and private uses of biometric technologies. Coworker.org is a laboratory for workers to experiment with power-building strategies and win meaningful changes in the 21st-century economy. For the past four years, we have been conducting research and analysis for the field on how data-mining techniques innovated in the consumer realm had moved into the workplace[1]. The past year, we have been investigating and documenting the increasing number of tech products and tech companies collecting and processing biometric data from workers at every step of the labor process — hiring/recruitment, workplace safety and productivity, benefit provision, workforce development, et al. Dubbing this tech ecosystem as "Little Tech", we launched a public database[2] to bring attention to the rapidly growing and expansive unregulated marketplace of tech products increasingly collecting, aggregating, and analyzing sensitive biometric data about workers. Our research shows that the AI-enabled biometric products are not only getting more pervasive, but also more increasingly reliant on sensitive data points such as workers' medical/health info (i.e. body temperature, respiratory rate, and heart rate[3]), gestures, sentiment/mood, stress levels, cognitive functioning, etc.

[1] "*The Datafication of Employment. How Surveillance and Capitalism Are Shaping Workers' Futures Without Their Knowledge*." Sam Adler-Bell and Michelle Miller. The Century Foundation. 12/19/18.
[2] "Bossware and Employment Tech Database."
[3] See Scorecard by Fight for the Future highlighting which top retailers are employing facial recognition technologies in the workplace: Ban Facial Recognition In Stores.

While it's been encouraging to see more state biometric laws and local ordinances emerging (e.g. Portland, Oregon, and NYC), as well as class-actions for non-compliance — the collection of biometric data is largely unregulated. Additionally, while AI-enabled biometric technologies in the public and private sector are becoming more prevalent, most users still do not fully understand potential risks and their obligations. In fact, industry reports have found that many companies are deploying various forms of AI throughout their businesses with little consideration for their ethical implications[4].

In order to assist OSTP's analysis of public and private uses of AI-enabled biometric technologies, the analysis below provides an overview of the *current* and *anticipated* uses of these technologies in the workplace and labor markets.

1. **The collection of workers' biometric data is proliferating and AI-enabled biometric technologies are being integrated into almost every part of the labor process (e.g. hiring and recruitment, productivity and risk monitoring, workplace safety, etc).**

   The past eight years, American workplaces have relied on a suite of business intelligence and enterprise technology tools to measure productivity through keystrokes and time keeping and management. Yet, as the technology has advanced so have the products and the data mining that enables them. Now most AI-enabled biometric products in the workplace now regularly capture sensitive data points such as workers' sentiment, behaviors, mental health, facial and audio data, etc., and for a more diverse type of labor uses such as hiring and recruitment, insider threat detection, maintaining workplace safety, etc. Additionally, when we have investigated recently filed patents, we also found that corporate vendors are planning to develop more sophisticated AI-enabled biometric technologies that can make predictions about workers' well-being in the workplace. For example, Microsoft filed a patent on 10/29/20: US 2020/0342895 to be able to use audio and visual data from workers in meetings in order to develop an individual sentiment rating system looking at whether someone appeared concerned, ambivalent, appeared distracted, annoyed, etc.

[4] "Report finds startling disinterest in ethical, responsible use of AI among business leaders." Jonathan Greig. ZDNet. 5/25/21.

Below is an overview of how workers' biometric data is currently collected and used in workplaces and the labor process:

- **Predict employee misbehavior and formulate risk scores for workers using collected behavioral and productivity analytics:** Products in this category are used in both white collar and blue collar jobs and include products from both established corporate vendors such as Oracle and newer startups. They collect workers' audio and video conversations data (among other data points) in order to analyze human behavior and provide modern governance, risk, and compliance controls. Products and companies in this category are eLoomina, Retail XBRi Loss Prevention by Oracle, Aware's Organizational Insights, Trendzact's Agent Interact: Workspace Monitoring & Response Solutions, Veriato's Cerebral: AI Driven Insider Threat Detection, Forcepoint's Behavioral Analytics solution, Netwrix's User Behavior Analytics Solution, and SearchInform's User Behavior.

- **Digital identity verification:** Workers are having to utilize digital identity verification systems in order to secure vital benefits. Examples of this are the current public/private sector partnership between states and facial recognition company, ID.Me, in order to process unemployment benefits. Socure, a company currently being used in the financial services, banking, gaming, healthcare, telecom, and e-commerce industries and currently eying expansion into the public sector with its recent hire of Jordan Burris, former chief of staff at the White House Office of the Federal Chief Information Officer (CIO), takes things one step further[5]. Their product Socure ID+ not only collects biometric data for identity verification, but then this data is combined with predictive analytics for fraud detection. It does this through a single, modular API and self-learning correlations of over 6,000 predictors to determine riskiness of identity[6].

- **Supervise remote workers:** With an increase in the number of remote workers due to the pandemic, employers have been acquiring a variety of work monitoring software to keep tabs on workers' productivity, time management, as well as detecting problematic behavior. Some

[5] "*Socure targets public sector expansion with hiring of an ex Federal CIO chief.*" By Frank Hersey. Dec 7, 2021. Biometric Update.
[6] "*Real-Time & Predictive Analytics Platform | Socure ID+.*" Company Website: https://www.socure.com/products/socure-id. Accessed 1.15.22.

products we have found such as Teleperformance TP Observer provide an AI-enabled webcam that can be installed in remote workers' computers that recognizes their face, tags their location, and scans for "*breaches*" of rules at random points during a shift. Such breaches include an "*unknown person*" detected at the desk via the facial recognition software, "*missing from desk,*" "*detecting an idle user,*" and "*unauthorized mobile phone usage*". Other products such as Teramind, collect audio recordings from workers (without their knowledge) among other employee activity data points in order to support workplace investigations.

- **Covid workplace safety (including enforcing social distancing and the use of masks):** A wide variety of AI products have been rolled out in the retail, restaurant, and hospitality industries in response to the pandemic that utilize face- or temperature-detecting algorithms. They include products such as Cogent Facial Recognition Platform, which counts the United States Immigration and Customs Enforcement (ICE) as a customer; Feevr; FindFace Pro, Tech5 Biometric Technologies; TrueFace Aware, Alibi Single Person Thermal Wrist Temperature Detection and Face Recognition Unit; Density; THine CTI-T66; Fitbit; PcW Checkin; and Gateway COVID-19 Response. Other products, such as the Dasha Covid-19 Screener, use voice AI to determine if workers have Covid-19 symptoms. In 2020, experts noted in a New York Times article that many of the virus screening tools being integrated in the workplace were not reliable or accurate.[7]

- **Hiring and recruitment.** The products in this category target everything from Fortune 500 companies and specific industries such as financial services, retail, manufacturing, hospitality, aviation, and technology (e.g., HiredScore, Hirevue, Human) to hiring and recruitment more broadly (Jobandtalent, Pymetrics Talent Acquisition Platform). Some of these products claim to track emotions such as anger, contempt, disgust, engagement, joy, sadness, surprise and valence (a measure of the positive or negative nature of the recorded person's experience) by analyzing a video clip. An emotion recognition API by the company Affectiva, which claims that it can track emotions such as anger, contempt, disgust, engagement, joy, sadness, and surprise, and measure how pleasant or unpleasant they are by analyzing a video clip, can also be integrated into many of these platforms. Other AI-enabled

[7] "Employers Rush to Adopt Virus Screening. The Tools May Not Help Much." Natasha Singer. The New York Times. 5/11/20.

biometric products in this category are Human, which analyzes video-based job applications and scores candidates' emotional reactions and Microsoft Wellness Insights, which seeks to help workers manage workplace anxiety by providing wellness recommendations based on their biometric data (heart rate, blood pressure, and more).

Now that we have outlined some current areas where AI-enabled biometric technologies are used in the labor process, below we discuss key areas where OSTP's leadership would be a much-needed intervention in helping to provide better protections and redress for workers.

- **Work with key labor regulatory agencies to create a taxonomy of data harms:** This should include working with agencies such as the Equal Employment Opportunity Commission (EEOC), National Labor Relations Board (NLRB), Federal Trade Commission (FTC) or Occupational Safety and Health Administration (OSHA) to expand the taxonomy of data harms that can emerge from the use of AI-enabled biometric technologies in the labor process. This should focus around three core areas: privacy, economic exploitation, and discrimination. First, the taxonomy should lay out the data harms that arise from *privacy violations* such as misuse of workers' biometric information which can lead to serious issues like identity theft. Additionally, when biometric data becomes compromised, it will never be completely secure as a method of authentication again which is more damaging than when other types of data is stolen, like a person's credit card number (you can order a new credit card but you can never change your fingerprints.) Therefore, understanding specific implications of this on workers, will be essential.

  Second, more research is needed to better understand AI-enabled biometric technologies that facilitate exploitative labor practices, especially for low-wage, disabled, or BIPOC workers. These can include instances of wage theft, wage suppression,[8] discrimination, at-risk employment relationships, economic mobility, and more. Finally, researchers have already found that biometric technologies have the potential to discriminate against protected classes, such as disabled workers.[9] For example, AI-powered hiring and recruitment products such as Pymetrics and Humantic AI utilize online tests that are not suitable for candidates with ADHD, dyslexia, and/or color

[8] "Identifying the policy levers generating wage suppression and wage inequality." Lawrence Mishel and Josh Bivens. Economic Policy Institute. 5/13/21.
[9] "Report – Algorithm-driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?" Lydia X. Z. Brown, Ridhi Shetty, Michelle Richardson. Center for Democracy and Technology. 12/3/20.

blindness, are unforgiving of time gaps in résumés even for pregnancy or medical reasons, may demand online tests to measure attention span or culture fit, and can require videos to be recorded to analyze voice or emotions. Therefore, data harms that can contribute to discrimination need to be better defined according to protected classes.

This information will be essential in not only increasing regulatory investigations surrounding potential abuses of workers' biometric data but also help support FTC rulemaking in this area, the increasing number of state-level complaints and class action suits taking place, especially in Illinois where the Biometric Information Privacy Act (BIPA) is the most comprehensive biometric legislation in the country, as well as new regulations and laws emerging in different states.

- **OSTP should provide biometric privacy industry standards to instruct the public and private sector on how they should handle and safeguard this data.** There is an immediate need for greater clarity and public education around the development of comprehensive biometric data policies in private and public sector uses. These standards should help guide actors in each sector to understand how to ensure proper data security, provide notice of biometric data collection and intended use purposes, obtaining written consent to disseminate biometric data, and banning the sale of this information. Additional standards are also needed in terms of the proper legal process for the retention and destruction of workers' biometric data.

The rapid advancement of AI technologies in recent years means that regulators are engaged in a game of catch up. And while the United States does not yet have a comprehensive AI regulatory framework, the OSTP can play a unique role in increasing the public and regulatory agencies better understand by providing a framework for understanding risks that emerge from biometric technologies and necessary safeguards to ensure these technologies do not run afoul of restrictions set out in laws and regulations relating to privacy, anti-discrimination, data security, labor violations, and other related frameworks. We welcome OSTP's leadership in helping to safeguard workers' sensitive data.

Thank you for the opportunity to provide these comments.
Wilneida Negrón, PhD
Director of Research and Policy
Coworker.org

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Cyber Farm Labs

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: SILIS
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Monday, October 11, 2021 7:39:39 PM
Attachments: LOGO.png

We can provide a **response to all (6) topics listed and of concern posted for the RFI posted by the OSTP**:

With a high degree and level of confidence, ALL developed AI-based, biometric technologies - currently in use and under developed, have a single common denominator.

ALL (current & future) AI-based biometric technologies provide an individual and or group human-coding/programming genesis of creation and attribution to a single and or group of biological human author(s), coder(s) and or programmer(s)/ AI-engineer(s). Attribution can be linked - similar to patent filings; to a single source code/programmer/AI-Engineer or group of AI engineers and coders, who can be identified as the developer(s) of ALL AI-based biometric technologies (current & future).

Should current and future ethical, moral, legal, regulatory, procedural and protocol guidelines of concern develop and or made known to be in violation of current individual rights under federal rules of regulation of ALL AI-based technologies, which address the (6) listed topics for the RFI posted by the OSTP discussed herein, then the OSTP has the sole legal and regulatory authority to petition a Senate or Congressional investigative inquiry to interview ALL authors, coders, programmers and AI engineers that are listed, as the genesis creators of the AI-based technologies under investigation and scrutiny for federal regulatory compliance and potential violation of ethical, moral, legal, regulatory, procedural and policy conflicts of interest and or bias, prejudice discovered through official parliamentary Q&A sessions of the human creators of the AI-based technologies in question.

Conclusion, hardware machines are not and can not be manufactured, engineered and programmed to exhibit ethnic, racial, socio-economic, religious affiliation bias, prejudice and discrimination - which would be viewed as violation of US Constitutional Amendments and Articles.

ALL computing software finds its creation genesis from a single or group of human computer scientist, software coders, developers and systems engineers. It is the human creator who generates the coding and programming biases, prejudices and discriminatory social factors or variables - converted to mathematical stochastic equations and algorithms, which produce the AI technologies that reveal a clandestine cyber capability providing human anonymity for its creators, developers and engineers.

Potential Mitigating Solution

Implementation of embedded software coding directives, which would act as a diagnostic toolkit, capable of detecting potentially biased, prejudicial and or discriminatory coding and programming syntax analysis - *i.e. source code review SDK*; before the AI technology product can be marketed, advertised and or sold to any potential customer or client for public use and consumption. In addition, the human coders, developers and AI engineers could also be mandated to undergo screening prior to and post AI technology production and deployment for public and or general use.

We developed AI/DL technology - SILIS (Super-Intelligence Learning Information System). SILIS was created and developed to enhance human enduser intelligence, through real-time, human enduser terminal activity and usage. Machine super intelligence is not and will not be a viable strategic initiative worth short or long term investment. However, high performance engineered, computing systems can be developed to allow the machine to expand and elevate the cognitive learning capability of its human terminal endusers - producing an generally, acceptable level of quasi-technological singularity within a decade or two.

Respectfully Submitted,

Robert Bass
Founder/Director of Cyber Intelligence and AI/DL

An FTL TECHNOLOGIES CORPORATION COMPANY

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Data & Society Research Institute

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

DATA&
SOCIETY

January 14, 2021

Request for Information on Public and Private Sector Uses of Biometric Technologies

Dear Dr. Eric Lander and Dr. Alondra Nelson,

Data & Society Research Institute is pleased to submit a response to the Request for Information (RFI) published by the Office of Science and Technology Policy (OSTP) on past deployments and current use of biometric technologies in the public sector.

Our organization is an independent, nonprofit research institute studying the social implications of data-centric technologies and automation. We are working to help ensure that artificial intelligence (AI) systems are accountable to the communities within which they are applied, and to produce empirical research that challenges the power asymmetries created and amplified by technology in society. We have worked extensively with civil society and advocacy communities, and in solidarity with marginalized communities and workers directly affected by algorithmic harms.

We are pleased to see the OSTP's commitment to create a Bill of Rights for an Automated Society and to ensure new and emerging data-driven technologies abide by democratic values.[1] It is essential that we develop AI policy and governance mechanisms responsive to the prevalence of AI systems that enable discriminatory practices and that expose marginalized communities to harm.

In this comment, we highlight the biometric surveillance of care workers and care recipients through electronic visit verification (EVV) systems, in order to encourage OSTP to explore how the public sector adoption of biometric technology has ignored the needs of marginalized communities and has led to tangible harm. By centering the harms generated by the growing landscape of punitive technologies that target and criminalize both low-wage workers and public benefits recipients, OSTP can ensure that the government commits to community- and justice-informed uses of algorithmic systems.

In this comment, we recommend that OSTP:

- **Support federal agencies in their efforts to better understand the use of automated systems in public benefits delivery, and ultimately recommend the**

[1] https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/

prohibition of technology that further marginalizes and harms the communities who are entitled to benefits and care.

- **Commit to research and policy proposals that center community and justice-informed uses of algorithmic systems.**

1. Electronic Visit Verification Systems & Biometric Surveillance *(Questions 1, 4)*

Emerging harms from uncritical public sector adoption of algorithmic technology

Public institutions are increasingly turning to technical fixes to solve structural problems, and consequently, sidelining questions of inequality, accountability, and justice. **Within public benefits programs, federal and state governments are introducing algorithmic technologies like EVV to police vulnerable communities under the guise of rooting out fraud, waste and abuse, rather than passing and implementing policy in consultation with those communities and in response to their needs.** These technologies introduce automated, algorithmic processes that lack transparency and mechanisms for appeal, putting the onus on vulnerable individuals with scarce resources to not only push back, but to advocate for services and benefits they have a right to expect from the state.

As the largest single funder of long-term services and supports, the United States government—through programs like Medicaid—plays a significant role in providing necessary care and support services for people with disabilities and older adults. As a result, greater public sector use of technology is impacting both the care workforce and the families they support. Just as the use of automated systems in areas like education, criminal justice, and welfare have already led to deeply inequitable outcomes, the adoption of these technologies in Medicaid home- and community-based programs may perpetuate extractive and punitive approaches towards managing, quantifying, and distributing care across our society.

Our recent research report, "Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care,"[2] finds that the surveillance of US home care workers through a state-funded EVV mobile apps erodes critical support for people with disabilities and older adults while offloading significant, unacknowledged burdens onto both workers and service recipients within Medicaid home- and community-based services. The implementation of EVV systems highlights the risks of uncritical adoption of data-centric and biometric technologies in the provision of public services.

[2] https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care/

Biometric Surveillance of Care Workers and Care Recipients

Congress passed the 21st Century CURES Act in 2016, which included a provision that required all Medicaid-funded personal care and home health care services to use EVV systems. EVV systems are a form of digital workplace monitoring that tracks homecare workers' time, location, and other data in order to confirm that services were delivered.

While EVV systems may seem to be just another digital timekeeping tool and method for ensuring quality of care, these systems were federally mandated to serve wider policy ambitions to reduce "fraud, waste, and abuse" in publicly-funded personal care and home health services. However, rather than producing an accurate measurement of fraud, waste, and abuse, EVV systems routinely flag workers for minor errors and glitches. **Although the federal legislation that mandated EVV required the systems to be "minimally burdensome," in practice, little federal policy guidance was provided on how to adhere to this goal, resulting in deeply invasive data collection being encoded into state policies and technology design, including GPS location tracking, geofencing, and biometric data collection like facial and voice recognition.**

EVV systems use GPS location tracking, geofencing, and biometric data collection to track workers and, by extension, their clients. Rigid policies and biometric technology requirements that pressure individuals to comply with strict program rules have had a chilling effect on service recipients' lives and has made workers' jobs more difficult. Home- and community-based services are essential and life-sustaining for Medicaid service recipients, which means they have no choice but to opt into data collection through EVV systems as a condition of receiving services. Service recipients and workers spoke of feeling criminalized, viewing EVV as an extension of broader legacies of government surveillance over people of color, and poor, disabled, and older adults.

These GPS and biometric features have been some of the most contested aspects of the EVV mandate. Advocacy groups have particularly focused on banning the use of GPS tracking and biometric data collection on a national level,[3] and their use has also contributed to privacy backlash from disability communities at the state level.[4]

- **Facial Recognition**: Facial recognition is commonly implemented within EVV platforms for the purpose of identity verification, which seeks to match a photograph taken by the worker to a photo kept on file. Typically, a worker is required to

[3] https://www.foley.com/en/insights/publications/2020/05/century-cures-act-personalized-medicine-covid-19
[4] https://coloradosun.com/2019/12/23/evv-requirement-for-medicaid/

photograph themselves and/or their client when clocking into a shift. If the system fails to prove a match, then that worker log-in is flagged for further review, and can result in lost or delayed wages. Although it is not required by the mandate, EVV vendors such as FreedomCare and Direct Care Innovations use facial verification. In addition to privacy issues, the use of this technology raises concerns over workplace bias and discrimination. Facial recognition technologies have well-documented racial and gender biases, showing lower accuracy rates for identifying people of color, particularly Black women. These biases apply particularly to the U.S. homecare workforce: nearly 90% are women, 63% of whom are women of color.[5] Facial recognition technologies also raise concerns over consent and coercion, as older adults and people with disabilities may be pressured to choose between opting into biometric data collection or losing access to critical services. Workers may similarly feel pressured to coerce their clients into complying with daily biometric data collection in order to do their jobs.

- **Voice Verification**: Some EVV systems also use voice authentication, a form of biometric surveillance which requires a worker and/or their client to speak into their phone in order to match their voice to an existing voice record. Interactive Voice Response (IVR), often referred to as "voice verification," requires the Personal Care Services (PCS) worker and/or consumer to login and out using biometric voice authentication on a landline or cellular device, raising privacy concerns associated with collecting, storing, and using such biometric information. Service recipients have also expressed that their autonomy can be limited by IVR in situations where they experience speech disorders, which can prevent IVR from properly recognizing their voices, thus resulting in non-compliance with EVV.[6]
- **GPS Tracking and Geofencing**: The EVV mandate requires that workers must log the location where services are provided when clocking in and out. In EVV systems, this is achieved through the GPS location tracking capabilities of the worker's smartphone. Geofencing is the practice of setting geographic perimeters around a location, and is used to limit where workers are allowed to log their work. Because home- and community-based services are integrated into service recipients' everyday lives, digitally tracking workers' location data also generates extensive digital maps of service recipients' movements, as well as that of their families and

[5] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proceedings of Machine Learning Research, 81 (2018): 1–15.; http://phinational.org/resource/direct-care-workers-in-the-united-states-key-facts-2/

[6] https://healthworkforce.ucsf.edu/publication/impact-electronic-visit-verification-evv-personal-care-services-workers-and-consumers

social networks. Service recipients also expressed fears that their location data could be scrutinized and misconstrued to justify denial of services. In some states, geofencing has been used to require that workers log their work only within approved service locations, which entrenches ableist assumptions that service recipients are homebound. For many service recipients, this form of surveillance enforces a state of de facto house arrest by limiting their movements. To date, regulators have taken little action to limit either feature, despite both features pressurring service recipients and their workers to re-orient their lives to conform with compliance rules and avoid being flagged for potential fraud.

EVV's place at the center of labor, digital and care concerns

Pressures to follow EVV system rules often strained employment relationships, as workers struggled to make their work visible to digital systems. In some states, exasperated service recipients described placing reminders all over their homes or setting up dozens of phone alarms to keep up with constant electronic check-ins. Even small errors in compliance could lead to delayed or lost wages, and any deviation could result in a convoluted negotiation with healthcare bureaucracies. Poor system design and a lack of transparency made workers wary of invasive data collection, while geofencing requirements significantly limited service recipients' abilities to move freely in their own communities.

In addition to the immediate harms, the rollout of EVV systems and similar data-centric technologies that use biometric surveillance might have further-reaching impacts to U.S. care infrastructures. Some advocates have argued that the EVV mandate undermines many of the gains won by the disability rights and Independent Living movements in their push for the right to live independently in their communities rather than in institutions. Furthermore, growing surveillance and compliance burdens on service recipients may create barriers to accessing critical services in ways that are substantial but not easily measurable in the long-term. It's also possible that data generated by EVV systems could be used in the future in ways that data subjects have not consented to.

2. Governance and Stakeholder Engagement Recommendations *(Questions 6a, 6h)*

Through the process for developing a Bill of Rights for an Automated Society, we encourage OSTP to examine the consequences of uncritical adoption and government mandates for use of biometric technologies. The government has a responsibility to understand the full implications of adopting technical systems with such expansive and unexplored social impacts, particularly for communities that rely on government services

and are increasingly having their interactions with government institutions mediated by biometric technologies.

In this effort, we emphasize the following recommendations:

1. OSTP should support federal agencies in their efforts to better understand the use of automated systems in public benefits delivery, and ultimately recommend the prohibition of technology that further marginalizes and harms the communities who are entitled to benefits and care.

The United States is experiencing a care crisis that has been exacerbated by the COVID-19 pandemic, including a shift away from institutional care settings as occupancy rates in nursing homes and other congregate-living settings dropped sharply across the country. Government efforts to invest in and reform the country's care infrastructure have been met with significant contestation over funding. Investment in these programs would include wage increases and better training and benefits for workers, as well as enhanced quality of care and expanded access to services to more people who need them.

Labor, disability, and elder rights advocates have warned that the current system is ill-equipped to meet growing demand. **Rather than heeding these calls by expanding services and investing directly in the workforce, government actors have often instead deployed new technologies to recalculate the distribution of already thin resources, or to police, surveil, and restrict those who receive them.**

These systems' inability to factor in the subtleties of individuals' care needs led to drastic service cuts with devastating effects to service recipients' health and well-being. These measures may serve the interests of controlling costs, but ultimately do not address the underlying state of chronic underinvestment. Furthermore, because this technology is designed in order to further institutional aims like cost-cutting, rather than being designed in response to the needs of care workers and recipients, it will likely continue to result in further harm and flattening of the complexity and interpersonal nature of care and support work.

The assumption that automated systems can be used to reduce fraud and increase efficiency is compounding inequality in the way that public benefits are delivered. These attempts to reduce fraud cannot be understood outside the context of racism, sexism, and the deep stigmatization of poverty and disability that have long shaped labor and care

infrastructures in the U.S. Unlike fraud oversight practices that focus on institutional accountability—such as audits of home health agencies' billing practices—EVV systems direct the digital surveillance spotlight onto individual workers and their clients' daily lives by perpetuating an environment in which the default assumption is that everyone is committing fraud and cannot be trusted.

This is consistent with widespread digital surveillance of low-wage work, which is rooted in racist perceptions of the workforce as unskilled, untrustworthy, or lazy. Extensive surveillance—both subtle and overt—has long been normalized in the context of low-wage work. Rather than focusing on improving workplace conditions—including poor wages, lack of benefits and training, lack of access to technology, and overall social devaluation—policy efforts are instead marshalling technology to more closely monitor and discipline the workforce.

The failures of EVV go beyond poor user design and failed implementation and extend to serious questions about whether this technology improves job or care quality. Our research indicates it does not when its users' needs are not prioritized. While data-centric technologies are often hailed as solutions to social problems, EVV demonstrates how the government's use of data-centric and biometric technologies is often guided by punitive aims that reinforce racism, sexism, and classism.

OSTP's efforts to highlight this dynamic could educate and inform other federal agencies grappling with these challenges, and could facilitate a more holistic reckoning with the government's use of data-centric and biometric technologies.

OSTP could also take steps toward recommending the prohibition of the use of such technologies in certain contexts absent effective oversight. Leaving this set of governance concerns up to companies through self-regulation, company principles, and other "responsible AI" initiatives is not going to result in meaningful checks on harms, particularly to historically marginalized groups who are already radically under-represented in the design of predictive systems.

2. OSTP should commit to research and policy proposals that center community- and justice-informed uses of algorithmic systems.

We need to question both the centrality of tech companies in relation to the state provision of services and benefits, and the ability of the companies' technologies to serve vulnerable

communities in ways that don't further unjustly criminalize them. **Instead of calling for the elimination of all technology in care and labor contexts, our research indicates the need for greater visibility of the harms technologies can create, and a deeper commitment to community-oriented policy approaches that ensure any technology deployed in the provision of public benefits and services is subject to more meaningful democratic deliberation.**

In the years following the 2016 legislation mandating EVV, public backlash emerged as service recipients and workers struggled to adapt to the new requirement. Dozens of town halls across the country surfaced deep confusion among EVV users over opaque policies and glitchy, inaccessible systems. In a 2018 stakeholder call hosted by the Centers for Medicare and Medicaid Services, officials summarized the public input they had received from around the country: this included significant concerns over privacy, financial and administrative burdens, and fears that EVV would exacerbate labor shortages and push service recipients into institutions or out of Medicaid entirely.

Public input and participation in an accountability process is not synonymous with accountability to the public. The timing and nature of the public engagement, who represents "the public," and the response to that input by the institution controlling the technology all matter deeply.

These issues are emerging at a time when tech companies are looking to enhance the scope and predictive power of their products. Despite significant implementation failures involving more rudimentary technologies, multiple state governments have already adopted powerful, automated-decision making tools to assess disabled people's eligibility for Medicaid and home- and community-based services, often with little public debate or transparency over how decisions are made. While it is unclear whether EVV-generated data has yet been used to cut services, it is one potential trajectory for future use of the technology.

Moving forward, we encourage OSTP to support federal and state governments to think expansively and creatively about stakeholder engagement, drawing on communities' lived experiences of algorithmic systems to determine whether and in which ways existing regulatory tools can be applied to mitigate algorithmic-driven harms. In instances where those tools are not sufficient, we encourage close collaboration with labor and disability rights coalitions to imagine and implement alternatives that are responsive to community needs.

DATA& SOCIETY

Resources and Further Reading

Our research outlines many instances in which labor and disability rights advocates foresaw the harms that EVV systems would bring. Many groups have continued to advocate for alternative policies, including a ban on the use of geolocation (GPS) and biometrics by EVV systems. The following resources significantly informed our work and provide additional analysis on the impact biometric technology is having on care workers and care recipients.

- The National Council on Independent Living, Electronic Visit Verification (EVV) Task Force Statement of Principles and Goals
- Kendra Scalia, Electronic Visit Verification (EVV) Is Here: What you need to know and how to get involved
- Stop EVV, Electronic Visit Verification (EVV): What It Is and What It Does to Our People
- Alicia Hopkins, How Electronic Visit Verification Is Harming People With Disabilities

Sincerely,

Alexandra Mateescu, Researcher
Serena Oduro, Policy Research Analyst
Brittany Smith, Policy Director

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Data for Black Lives

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

WRITTEN STATEMENT of

Data for Black Lives

Before the

Office of Science and Technology Policy (OSTP)

January 6, 2022

Dear Dr. Eric Lander, President's Science Advisor and Director of the White House Office of Science & Technology Policy (OSTP) and Dr. Alondra Nelson, OSTP Deputy Director for Science & Society:

Data for Black Lives is a movement of activists, organizers, and mathematicians committed to the mission of using data science to create concrete and measurable change in the lives of Black people.

Since the advent of computing, big data and algorithms have penetrated virtually every aspect of our social and economic lives. We recognize that these new data systems have tremendous potential to empower communities. Tools like statistical modeling, data visualization, and crowd-sourcing, in the right hands, are powerful instruments for fighting bias, building progressive movements, and promoting civic engagement.

We value the use of data for technological innovation and recognize its significance in bettering the lives of millions of people. Whether it's through identifying and responding to community members who lack access to the internet, collecting data to implement tools that support community members with disabilities or chronic illnesses, or the use of data to understand and engage in the political process -- data is leveraged for technological innovation and the evolution of humankind.

However, at Data for Black Lives we also understand that data is too often wielded as an instrument of oppression, reinforcing inequality and perpetuating injustice. As an example, redlining was a data-driven enterprise that resulted in the systematic exclusion of Black communities from key financial services. Facial recognition, a form of biometric data, poses a similar, more dangerous threat to our lives.

We agree with your assessment that “Data sets that fail to represent American society can result in virtual assistants that don’t understand Southern accents; facial recognition technology that leads to wrongful, discriminatory arrests; and health care algorithms that discount the severity of kidney disease in African Americans, preventing people from getting kidney transplants.” Several groundbreaking research efforts have made these disparities clear.

Prior to the misidentification cases of Robert Williams, Michael Oliver, Nijeer Parks, and Lamya Robinson, research showed the risk of these technologies and how they might harm Black and brown people the most. The Gender Shades Study by Joy Buolamwini, Timnit Gebru, and Deborah Raji recognized the discrepancies in how facial recognition sees or does not see darker skin tones among other findings. Research from Georgetown’s Center on Privacy and Technology pointed to the ways facial recognition was already being manipulated by law enforcement. And the Our Data Bodies research collective rooted their research in marginalized neighborhoods in Charlotte, North Carolina, Detroit, Michigan, and Los Angeles, California, further exposing the impact of vast networks of local surveillance. Community members that Our Data Bodies interviewed expressed that they felt that their information was being extracted from them for the benefit of corporations, law enforcement, and governmental institutions, not for their benefit. They indicated that the smallest “mistakes” in their lives (i.e., an inability to afford their water bills) was trailing them and preventing them from upward mobility. They also indicated that they felt targeted by surveillance structures, whether they were a formerly incarcerated resident who had served their time, trying to get back on their feet, or a person who had been previously evicted from their home, trying to make a fresh start. The feeling of being targeted and not valued as a human being was consistent across all three cities.

Data for Black Lives discovered through our own organizing and research in Detroit, Michigan, a city with a near 80% Black population, that commitments to surveilling communities of color is only growing. Despite Detroit’s median household income of under $31,000 per year (a number sliced nearly in half through job loss, since the pandemic), quality-of-life issues have rarely been addressed by city government, and instead, biometric surveillance has prevailed.

Much like your current efforts, Detroiters understand the significance of challenging the City’s Constitution, and attempted to pursue a Detroiters’ Bill of Rights. Dozens of social justice organizations, hundreds of impacted residents, and some city officials engaged in numerous meetings with an elected charter revision commission in an attempt to amend the City’s Charter. The Detroiters’ Bill of Rights, which became Proposal P, was in response to a decades-long

effort by Detroiters to be seen. Demanding that their city government work for them, Proposal P was real hope for a new, more racially equitable Detroit. But as with most progressive efforts, a massive, well-funded propaganda campaign of disinformation succeeded in swaying public opinion against the historic attempt to pass Proposal P.

In the words of Professor Peter Hammer, “As public money is diverted to private projects, Detroiters are told to be patient. They are told that the benefits will 'trickle down' to them over time. In truth, these benefits remain tightly controlled in private hands. Little is trickling down anywhere.”

One of the most contentious points of Proposal P, was an effort to rid Detroit of the mass surveillance, public-private partnership known as Project Green Light, and its companion technology facial recognition. The Detroit Police Department had been using facial recognition for over a year under a standard operating agreement, without a public hearing, and with no oversight from the civilian oversight body. Since a facial recognition policy was implemented following over a year of persistent public outcry, we have been made aware that although Detroit is 79% Black, facial recognition is used almost exclusively on Black residents.[1] We have also been made aware that even though the policy is to be used for violent crimes only, it is still being used for non-violent crimes.

Last year, Detroit City Council had a hearing on renewing contracts for facial recognition technology and hundreds of residents attended in protest. However, the Detroit City Council not only approved an additional $220,000 to extend the DataWorks Plus facial recognition contract, they also recently approved an additional $51,000 for BriefCam, which would allow a rapid search of videos across locations, despite the fact that the current facial recognition policy prohibits real-time tracking.[2]

Detroiters are suffering a great deal of economic hardship. Thousands of residents were overtaxed more than $600 million dollars leading to massive tax foreclosures, a situation which

[1] Edward Ongweso, Jr., “Detroit extends contract of facial recognition contract that doesn’t work,” *Vice,* September 30, 2020, https://www.vice.com/en/article/n7wx8b/detroit-extends-contract-of-facial-recognition-program-that-doesnt-work

[2] Erin Einhorn, “Detroit police can keep using facial recognition - with limits,” *NBC News*, September 19, 2019, https://www.nbcnews.com/news/us-news/detroit-police-can-keep-using-facial-recognition-limits-n1056706

has not been rectified.[3] Water shutoffs, which community leaders had to fight to end despite Detroiters suffering thousands of deaths during the pandemic - - are on hold until 2022, but still a looming threat to our health and safety.[4] Our infrastructure is crumbling, and residents suffered tremendous damage to their homes during recent flooding, on several occasions.

Surveillance is not safety. Massive investment in surveillance programs like Project Green Light, will not create the type of environment Detroiters deserve.[5] Movement around Detroit is being regulated by the thousands of flashing green lights. Although not as bright as the floodlights being resisted in New York City public housing, if your bedroom is behind one of these lights, you simply do not get a good night's sleep.[6] The lights never go off.

Many residents live under the constant feeling that they are in a perpetual line-up, being monitored everywhere they go. It has had an impact on the businesses they visit, although they are sometimes still forced to patronize establishments that use facial recognition out of necessity. The ubiquitous feeling of being surveilled is difficult to describe. One that keeps your shoulders tense with the dread that you might be the next person misidentified and falsely accused of a crime because the face recognition algorithm thinks your driver’s license or state ID matches one of the images captured at a crime scene.

If research and history is any indication, the four known misidentification cases, including the misidentification of a 14 year old child who was kicked out of a skating rink, are just the tip of the iceberg. It is our fear that we will look up forty years from now, if we do nothing, and have to exonerate people (some posthumously) who spent decades in jail because they were arrested by a faulty, racially biased algorithm. Or worse, we may never find out who they are.

---

[3] Christine MacDonald, “Detroit homeowners overtaxed $600 million,” *The Detroit News*, https://www.detroitnews.com/story/news/local/detroit-city/housing/2020/01/09/detroit-homeowners-overtaxed-600-million/2698518001/

[4] Heather Moody, Linda Elaine Easley, Melissa Sissen, “Water Shutoffs During COVID-19 and Black Lives: Case Study Detroit,” *Mary Ann Liebert, Inc. (Environmental Justice), July 8, 2021,* https://www.liebertpub.com/doi/10.1089/env.2020.0064

[5] Rebecca Smith, “Project Green Light: Surveillance and the Spaces of the City,” *University of Michigan Carceral State Project*, April 2021, https://storymaps.arcgis.com/stories/14dd97b35cbb4a4298786c75855f8080

[6] Film by Nadia Hallgren, Text by David Kortava, “The Controversial Floodlights Illuminating New York City’s Public-Housing Developments,” *The New Yorker*, June 30, 2021, https://www.newyorker.com/culture/the-new-yorker-documentary/the-controversial-floodlights-illuminating-new-york-citys-public-housing-developments?utm_source=twitter&utm_medium=social&utm_campaign=onsite-share&utm_brand=the-new-yorker&utm_social-type=earned

Much like Detroit, Atlanta is expanding its usage of mass surveillance. For example, Atlanta is expanding the use of automatic license plate readers as part of building a citywide network of cameras that feeds into a real-time crime center. The public is being told that the license plate readers' intended use is tracking stolen vehicles or vehicles with warrants, but an investigation shows that police agencies are also gathering data about travel patterns of people regardless of their connection to any crime.[7]

If we fail to act, we will continue to see cities like Detroit and Atlanta fall further and further into the realm of an authoritarian-regime style social credit system. We will find ourselves surrounded by surveillance cameras, real-time crime centers, drones, and facial recognition, funneling more and more Black, Brown, and Indigenous residents unjustly into the criminal justice system. We have already learned a great deal since the rise of mass incarceration. Facial recognition has the potential to increase the incarceration disparity to a degree that we may not be able to quantify.

It's time we rid ourselves of *data weapons* (any technological tool used to surveil, police and criminalize Black and Brown communities) before the harm is irreversible. We have a long way to go in increasing racial equity within our police departments. We should not be exacerbating existing inequity by turning over policing to artificial intelligence.

If policing by AI continues in Detroit, Atlanta, and other predominantly Black and Brown communities, it will most likely be packaged and rolled out across vulnerable communities across the United States.

Thank you in advance for reading and internalizing our plea. Our data, biometric or otherwise, should not be weaponized against us.

Sincerely,

[redacted]

Yeshimabeit Milner
Founder/Executive Director, Data for Black Lives

[7] Josh Wade and Aaron Diamant, "Eyes on the Road," *Action News WSB-TV Atlanta*, November 8, 2018, http://specials.ajc.com/plate-data/

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Data to Actionable
Knowledge Lab at Harvard
University

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Harvard John A. Paulson School of Engineering and Applied Sciences
SEAS, 29 Oxford Street, Cambridge, MA 02138
[redacted]
Finale.seas.harvard.edu

Finale Doshi-Velez
Gordon McKay Professor of Computer Science

JANUARY 15, 2022

New and emerging data-driven **biometric technologies <u>are not</u> at odds with American democratic values**; however, **A.i. may force us to *<u>quantify values</u>***. More concretely, **AI accountability and progress are *not* at odds**, provided we engineer a practical to use, critical to trust and fair regulatory framework so we can engineer regulatable A.i. that embeds our values into our decision-making technology. That said, **what can't be quantified needs to be participatory (see 3).** This might mean part of Director Lander's **answer to President Biden**'s 'day-one' letter will require research on **building a more "Regulatable" Artificial Intelligence**.

As the Science Division builds recommendations, the Data to Actionable Knowledge Lab (DtAK)'s usage of biometric technologies suggests a few points that might merit consideration when setting this research agenda:

1. How should we define A.i. explainability? Pragmatically. *Explanation is information about the AI/ML provided to the user such that they can make the decision they are trying to make.*
2. How do we mediate **between** assessing the **effectiveness** of an intervention subject to quantifiable **societal values**? **Meta-algorithms can be useful. We give one example for better study design**.
3. How can the new wave of intelligent systems account for the **complexity of medical work**? We suggest one potential avenue would be using a **socio-technical lens towards co-designing A.i. systems**.

Governance that takes into account our democratic community's diversity despite the complexities of explaining these systems will be paramount.

4. What **stakeholder engagement** looks like? We unpack our **roadmap** for responsible ML for health care
5. What an open **Auditing of A.i**. could look like? We discuss the concept of an **AI "Check Engine"** light regulatory framework.
6. What is public **transparency** in this context? We understand it in terms of **A.i. Explainability**, or lack thereof.

Item 6, transparency understood as combating lack of explainability, is crucial. Even the language around A.i. Explainability may need to be more inclusive to all stake holders when setting research priorities. **<u>A potential suggestion we leave the OSTP would be "Explainable A.i. (XAi) for All" – 'XAi4ALL' research agenda.</u>**

<u>Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies</u> *

This is a regulatory comment on Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies to (a) Dr. Eric Lander, Cabinet Member, Presidential Science Advisor, and Director of the White House Office of Science & Technology Policy ('OSTP') || (b) Dr. Alondra R. Nelson, Deputy Director for Science and Society at OSTP's Science Division (SCI)|| (c) Dr. Suresh Venkatasubramanian. Assistant Director, Science and Justice at SCI, henceforth collectively referenced to as "OSTP;" dated in Washington, DC, on or about October 4, 2021 and signed by Ms. Stacy Murphy, OSTP Operations Manager to the Federal Registrar as [FR Doc. 2021-21975 Filed 10-7-21; 8:45 am] with billing code 3270-FI-P

*

Harvard John A. Paulson School of Engineering and Applied Sciences, 150 Western Ave, Allston, MA 02134

*Note that the <u>views expressed here are solely our own</u> from working on probabilistic machine learning methods to address many decision-making scenarios. They **do not necessarily reflect** the official or unofficial opinion of Harvard University, Harvard's John A. Paulson School of Engineering and Applied Sciences or **any of the researchers whose research and insights summarize for this regulatory comment**.

Table of Contents

Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies
Response from the Harvard's Data to Actionable Knowledge lab, led by Professor Finale Doshi-Velez to the White House's Office of Science and Technology Policy
Saturday, January 15, 2022

Preamble:

Header Note

As per the OSTP Request for Information ("RFI") Dated in Washington, DC, on or about October 4, 2021 and signed by Ms. Stacy Murphy, OSTP Operations Manager to the Federal Registrar as [FR Doc. 2021-21975 Filed 10-7-21; 8:45 am] under "Request for Information on Public and Private Sector Uses of Biometric Technologies." [1] This **comment addresses 2 of its 6 items, focusing on health & wellness applications,** (we refer the OSTP to the Appendix for biometrics used for identification based on a World Bank report on Identity for Development).

Note that the ***views expressed here are solely our own,*** and do not necessarily correspond to the official or unofficial views of Harvard University (or its Harvard John A. Paulson School of Engineering and Applied Sciences), nor the World Bank Group or any governmental entity nor other researchers referenced herein.

Executive Summary: OSTP Might Consider Research into Regulatable A.i.

Making sure new and emerging data-driven technologies abide by the enduring values of American democracy depends on the biggest difference between accountability for AI systems versus other systems: A.i. may force us to quantify our values.[2] That said, what can't be quantified must be participatory. **We suggest that what this means for the OSTP is that we may need to set a broad research agenda on "Regulatable" A.i.**

Put simply, **Artificial Intelligence accountability does not need to stop AI progress**. Demanding explanations or other forms of evidence and transparency does not imply disclosing trade secrets no more than asking people to explain themselves implies disclosing how electricity flows through their neurons. Pragmatically, explanations involve sharing the part of a model's decision-making logic that is relevant for adjudicating the question on hand.[3] Below, we summarize our thoughts relating to the two items (**validation and governance**) **addressed from the RFI's six**. We leave to an **Appendix various examples** and generalizations of Artificial Intelligence Explainability for All (XAi4ALL) research agenda discussed in our governance section.

With respect to ***validation***, we suggest three goals to the OSTP's agenda-setting power in biometric technology research. One, **OSTP could use its convening power** to **shape language around the definition of AI "Explainability" (XAi) to be pragmatic**: an explanation is the "information about the AI provided to the user such that they can make the decision they are trying to make." Even if different contexts will require different explanations, a potential goal is to provide support for pragmatism in validation mechanisms.

Two, we provide a deep dive into our recent research on pre-deployment, rigorously defined trade-off mechanism for biometrics, validated using mobile health (mHealth) applications' HeartSteps project under Professor Susan A. Murphy and team.[4]. The work **operationalizes effectiveness – values tradeoffs** using statistical methods for study design, but it is only one example of **research the OSTP might highlight that assess effectiveness of an intervention subject to quantifiable societal values.**

Three, A.i. validation by co-design with stakeholders can use a sociotechnical lens: **Explanation Systems** (sometimes referenced as "Decision Support Tools' or DST) built on the recent AI explainability literature. More concretely, these DST can help expose discrepancies between how the model is operating and how people believe it

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Vol. 86 No. 193 Fed. Reg. 56300-56302 (October 4th, 2021).

[2] See Been Kim, Finale Doshi-Velez (2021) "Machine Learning Techniques for Accountability," Ai-The Social Disruption Spring 2021 Issue of Ai Magazine, Accessible at https://beenkim.github.io/papers/AIMagazine2021.pdf

[3] See 'Local Counterfactual Faithfulness,' "as humans we don't expect these explanations to be the same or even consistent what we do expect is that the explanation holds for similar circumstances" See summary presentation here: https://youtu.be/4lIr8rgo5zE?t=488 ; For a more detailed note see Finale Doshi-Velez, Sam Gershman, et al (2017) "Accountability of AI Under the Law: The Role of Explanation" working draft at https://arxiv.org/pdf/1711.01134 - As part of Harvard's Berkman Klein Center Working Group on AI Interpretability, a collaborative effort between legal scholars, computer scientists, and cognitive scientists)

[4] See Predrag "Pedja" Klasnja, Susan A. Murphy, Ambuj Tewari, Eric Hekler, Beverly Green HeartSteps https://heartsteps.net/welcome

should be acting. We review and explain A.i. validation by co-design with stakeholders (at the domain-expert-level).[5] Clinicians start by reviewing a platform where an A.i. suggests treatment (biometrics model choosing an anti-depressant) and justifies itself to the doctor (exposing quantitative and qualitative factors for the recommendation). **Feedback suggests we need more inclusive engagement** with the healthcare sociotechnical system, and even design for patient-provider collaboration. Unfortunately, this means current trends in explainable AI may be inappropriate for clinical environments. Therefore, we suggest that the **OSTP might consider** an entire **research agenda into determining how the new wave of intelligent systems can account for the complexity of medical work.**

As for ***governance*** of biometric technologies, we suggest the **OSTP might need a 'whole of government approach'** because an **"accountable A.i." revolves around the quantification of values** with various repercussions – put simply, it **presumes accountability has somehow been defined**.[6] Elsewhere we urged regulators such as the FDIC to coordinate determinations of said definitions within their regulatory perimeter.[7] We discuss research on 6 of 8 RFI lettered items: (a) our biometric stakeholder engagement example is our roadmap for responsible ML for health care, (b) piloting project-MIMIC-type governance (a reference in biometrics for research) elsewhere merits consideration, (e) Auditing A.i. research will entail not allowing models to "fail silently;" we go over a concrete solution-concept – an A.i. "Check that Engine Light" Regulatory Framework – that gives back agency to users while maintaining regulatory supervision of potential externalities.

For (c) biometric data collection, we note the "Data Nutrition Project" at MIT/Harvard Law School (https://datanutrition.org/) produces "nutrition labels" for the datasets being ingested by AI models & an appendix on an example of the multidisciplinary research from Harvard SEAS' Privacy Tools for Sharing Research:[8] DataTags (http://datatags.org/).[9] We close on (g) courts and (h) transparency discussing the state of A.i. Explainability research. Finally, we leave to the appendix an example of A.i. explainability geared to the general public (Algocount).[10]

One theme is clear: **A.i. accountability is likely not just a research problem, but a societal imperative for all.** Therefore, **we suggest to the OSTP that inclusive language might capture this sentiment such as:**

"A.i. Explainability for All (XAi4ALL)" research agenda

[5] See Doshi-Velez, Gajos, et al "Designing AI for Trust and Collaboration in Time-Constrained Medical Decisions: A Sociotechnical Lens," May 2021 http://www.eecs.harvard.edu/~kgajos/papers/2021/jacobs21designing.pdf For a broader view of interpretability see Finale Doshi-Velez, Been Kim (2017) "Towards A Rigorous Science of Interpretable Machine Learning." https://arxiv.org/abs/1702.08608

[6] See Been Kim, Finale Doshi-Velez (2021) "Machine Learning Techniques for Accountability" A.i. Magazine, Vol. 42 No. 1: Spring 2021, for a broader discussion of these issues https://ojs.aaai.org/index.php/aimagazine/article/view/7481

[7] See Response from the Harvard's Data to Actionable Knowledge lab, led by Professor Finale Doshi-Velez, to the Agencies on their "Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning," inspectable under FDIC – RIN 3064-ZA24 – https://www.fdic.gov/resources/regulations/federal-register-publications/2021/2021-rfi-financial-institutions-ai-3064-za24-c-043.pdf

[8] See https://privacytools.seas.harvard.edu/project-description?sv_list_box_delta=1481210040&pager_id=1&destination=node/21821&page=0%2C2

[9] See https://privacytools.seas.harvard.edu/datatags

[10] AlgoCount is in Italy to work on "The Public Perception of Algorithms in Society: Accounting for the Algorithmic Public Opinion." See http://algocount.org/

JANUARY 15, 2022

Response to the Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

Abstract

In the context of biometric technologies, the OSTP could consider setting a broad research agenda on "Regulatable" A.i. to make sure AI accountability and progress are not at odds. For biometric A.i. validation, we illustrate two pre-deployment frameworks: (a) an example of a statistical approach to illustrate a broader research agenda on the quantification of values to shape study design, and (b) a sociotechnical lens focused on co-designing Ai systems forcing a re-think of A.i. Explainability research directions. For the latter, the OSTP may consider setting an agenda on how a new wave of 'intelligent' systems can account for the complexity of medical work.

Governance of biometrics technology information suggest a unifying theme: "accountable A.i." revolves around the quantification of values, i.e. presumes accountability has somehow been defined. For example, an AI Model "Check Engine" light can only make sure that AI models do not "fail silently" if it can set accountable standards to monitor negative externalities set by all of us. This makes A.i. accountability depend on the entire society, demanding that all of us contribute our diverse perspective. We suggest to the OSTP that inclusive language, such as "A.i. Explainability for All (XAi4ALL)" research agenda might capture this sentiment"

Harvard John A. Paulson School of Engineering and Applied Sciences, 150 Western Ave, Allston, MA 02134

0. Introduction

0.1. Background: DtAK Lab

The Harvard's Data to Actionable Knowledge (DtAK) lab, led by Finale Doshi-Velez, uses probabilistic machine learning methods to address many decision-making scenarios, with a focus on healthcare applications

0.1.1. PI: Finale Doshi-Velez (She/Her/Hers), the Gordon MacKay Professor of Eng. and Applied Sciences

Professor Finale Doshi-Velez received her Ph.D. in Computer Science from MIT and an M.Sc. in Engineering from Cambridge University as a Marshall Fellow. Prior to joining SEAS, she was postdoc at Harvard Medical School. Doshi-Velez has received an Alfred P. Sloan Research Fellowship, an NSF CiTRaCS postdoctoral fellowship, an NSF CAREER award, and an AFOSR Young Investigator award. In 2019, she was awarded the Everett Mendelsohn Excellence in Mentoring Award by the Graduate Student Council for her mentorship and support of graduate students.

0.1.2. Major Areas: Modeling, Decision-Making, and Interpretability

Probabilistic modeling and inference:

We focus especially on Bayesian models

- How can we characterize the uncertainty in large, heterogeneous data?
- How can we fit models that will be useful for downstream decision-making?
- How can we build models and inference techniques that will behave in expected and desired ways?

Decision-making under uncertainty:

We focus especially on sequential decision-making

- How can we optimize policies given batches of heterogeneous data?
- How can we provide useful information, even if we can't solve for a policy?
- How can we characterize the limits of our ability to provide decision support?

Interpretability and statistical methods for validation:

- How can we estimate the quality of a policy from batch data?
- How can we expose key elements of a model or policy for expert inspection?

0.1.3. Expertise

These comments were created via discussion in the Data to Actionable Knowledge Lab, with particularly engaged suggestions from Weiwei Pan, Isaac Lage, Andrew Ross, Beau Coker, Sarah Rathnam, Sonali Parbhoo and Shalmali Joshi, as well as Eura Shin and Jiayu Yao. **We note here the virtual panel assembled by the OSTP with the convening power of the Center for American Progress last year, in November.**

0.2. Disclaimer

0.2.1. Conflict of Interest Statement: Heavy Reliance on Biometric Data

Our principal investigator, Professor Finale Doshi-Velez and the lab relies substantively on using biometric data to engineer specific applications in two domains: health and wellness. We work in close cooperation with Hospitals among other healthcare professional that use biometric information to make decisions on a daily basis. Finale Doshi-Velez also consults for Ethena, a Compliance Training Platform.

1. Descriptions: Left to Bibliography due to Length Constraints.

2. Validation: Power Constrained Bandit (Illustrating Statistical Approaches) & Decision Support Tools (Sociotechnical Lens)

"Procedures for and Results of Data-driven and Scientific Validation of Biometric Technologies" Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

Given the latest research into technological accountability[11] & fairness[12] we alert the OSTP into the increased recognition of how many kinds of unknowns cannot be "assumed away" or resolved through statistical analysis.[13] They will require even more sophistication from human policy-makers using a socio-technical lens to be potentially operationalized using the A.i. explainability literature. **That said, at DtAK we consider defining an A.i.'s explanation pragmatically**:

> *Explanation is information about the AI/ML provided to the user such that they can make the decision they are trying to make.*

In this sense, an explanation is very context dependent: the explanation necessary to determine whether a Supervisory Technology will enhance safety and soundness (a general-purpose early warning system) may be vastly different than an explanation that embodies machine learning models to help improve the treatment selection process of anti-depressant medication. Below, we will discuss two mechanisms to validate models **before** biometric-data-driven applications are rolled out at scale: (a) an example of a rigorous statistical analysis ('Power Constrained bandits'), (b) a broader and more inclusive approach using a socio-technical lens ('Decision Support Tools').

2.1. Illustration for Statistical Methods using Power Constrained Bandits: An example of a Rigorous Statistical Approach for Mobile Health Applications – potentiality a middle ground between weak assumptions for better personalization, and strong assumptions for robust identification strategy – How to Engineer Study Designs that assess effectiveness of an intervention subject to quantifiable social values? An illustrative example.

Power Constrained Bandits are meta-algorithms[14] that rigorously guarantee that a Micro-randomized trial (MRT) will be sufficiently powered to provide inference about treatment effects (produce generalizable knowledge about a population of users) and minimize regret (improve each user's well-being).[15] We will unpack this definition below in detail, but note here that the validation of our wrapper algorithms rely on the National Institute of Health-funded HeartSteps' project data by Professor Susan A. Murphy and team.[16]

Mobile health applications are gaining more popularity due to easy access to smartphones and wearable devices.[17] In mobile health applications, much of the initial research and development is done via clinical studies.[18] In these safety-critical applications, it is crucial to determine whether or

[11] See for example, Sheila Jasanoff, "Accountability" https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.689.2380&rep=rep1&type=pdf
[12] See for example, Jasanoff 2018 "Helping the world monitor and embrace technological change in a thoughtful way ", https://www.hks.harvard.edu/faculty-research/policy-topics/science-technology-data/helping-world-embrace-technological-change
[13] Broadly on uncertainty of technology, see Jasanoff 2007, "Technologies of humility" https://www.nature.com/articles/450033a
[14] With a certain power constraint, i.e. under the bandit algorithm's environment assumptions, we propose various ways to minimize regret.
[15] Jiayu Yao, Emma Brunskill, Weiwei Pan, Susan Murphy, Finale Doshi-Velez, (2021) "Power Constrained Bandits" https://finale.seas.harvard.edu/files/finale/files/power_constrained_bandit.pdf
[16] See Predrag "Pedja" Klasnja, Susan A. Murphy, Ambuj Tewari, Eric Hekler, Beverly Green Heart Steps https://heartsteps.net/welcome
[17] See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/
[18] For a comprehensively deployed example of this see Harvard's "Digital Phenotyping and Beiwe Research platform" https://www.hsph.harvard.edu/onnela-lab/beiwe-research-platform/

not a treatment has an effect on the health of the patient (i.e. whether or not such an effect exists).[19] This property is known as *power* in the statistical literature: the probability of detecting an effect if it exists.[20]

A popular study design for assessing the treatment effect[21] is the micro-randomized trial[22] in which an automated agent interacts in parallel with a number of individuals over a number of times. At each interaction point, the intervention (or lack of intervention), is chosen randomly according to some ***apriori*** determined probability. However, certain interventions may be more effective in certain contexts for certain people,[23] and this knowledge may not be captured in simple and *apriori* randomization probabilities. Thus, another important goal in mobile health is to personalize these randomized probabilities to each user.[24]

Power Constrained Bandits[25] meet the dual objective in mobile health where we not only want to personalize actions for the users, but we also want to guarantee the ability to detect whether an intervention has an effect (if the effect exists) for the study designers.

> *imagine a mobile app that will help patients manage their mental illness by delivering biometric-data-driven reminders to self-monitor their mental state. In this case, not only may we want to personalize reminders, but we also want to measure the marginal effect of reminders on self-monitoring.*

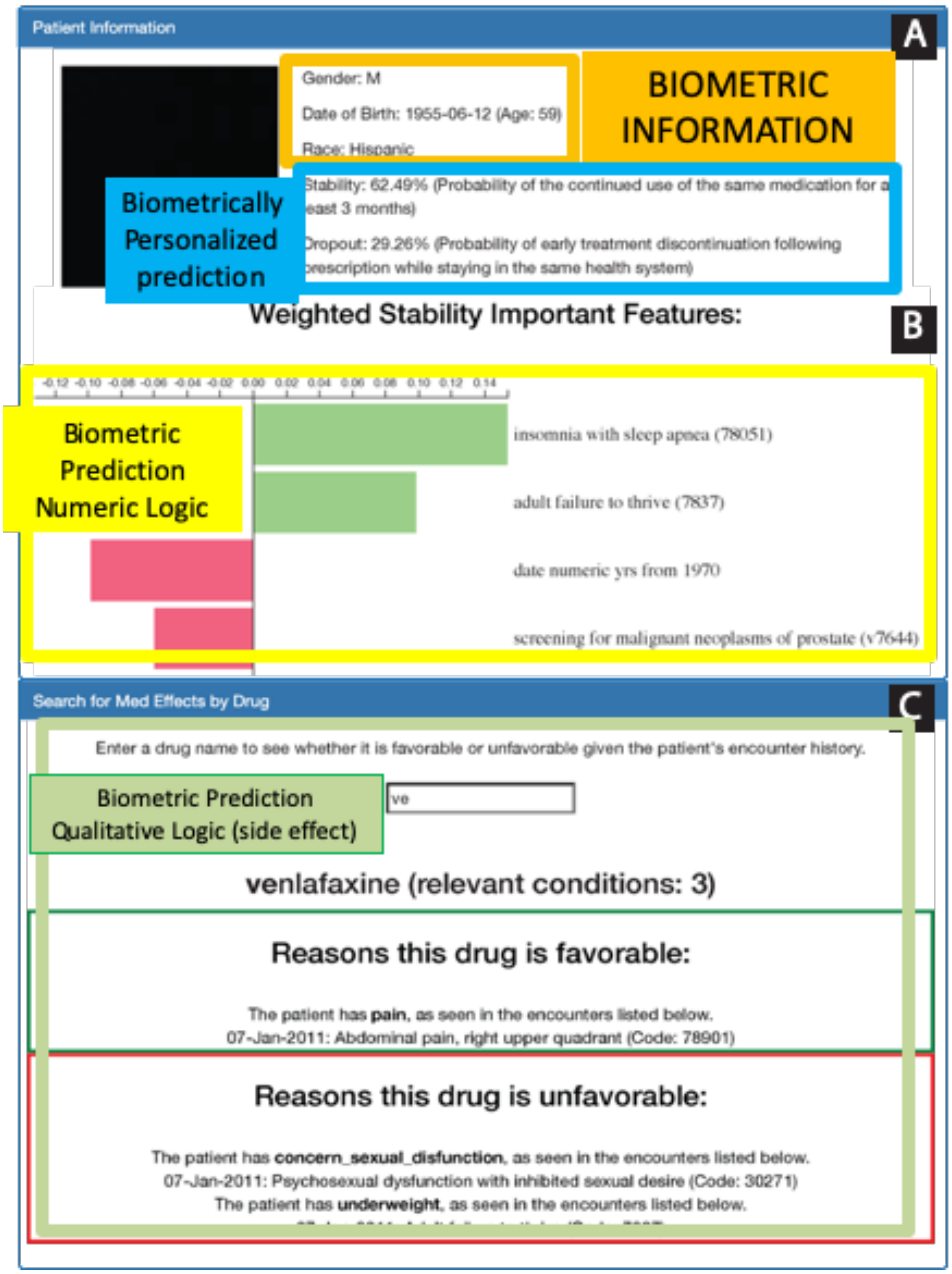
More Broadly, regulators should be aware that there exist algorithms tailored for two competing demands, either it (a) focuses on loose assumptions to better personalize, or (b) forces strong assumptions to be able to make concrete claims on a given intervention's effectiveness that either

- Have principled bounds on regret,[26] which largely come from the Reinforcement Learning (RL) community, or
  - "adding a personalized reminder for a user"
  - may make assumptions that are likely not true, but close enough to result in fast personalization
- Aim to rigorously determine an effect,[27] which have been a focus in the experimental design community.
  - Measuring the "marginal effect of reminders on self-monitoring"
  - must be able to make strong statistical claims:
    - in the face of a potentially non-stationary user—e.g. one who is initially excited by the novelty of a new app, and then disengages—
    - as well as highly stochastic, hidden aspects of the environment—e.g. if the user has a deadline looming, or starts watching a new television series

[19] For a recent overview on this see (2021) "The Power of the Placebo Effect" by Harvard Health Publishing. https://www.health.harvard.edu/mental-health/the-power-of-the-placebo-effect
[20] See Kosuke Imai, (2013) lecture notes "Statistical Hypothesis Tests," page 8. https://imai.fas.harvard.edu/teaching/files/tests.pdf
[21] See Peng Liao, Predrag Klasnja, Ambuj Tewari, and Susan A Murphy. Sample Size Calculations for micro- randomized trials in mhealth. Statistics in Medicine, 35(12):1944–1971, 2016 https://pubmed.ncbi.nlm.nih.gov/26707831/
[22] See Predrag Klasnja, Eric B Hekler, Saul Shiffman, Audrey Boruvka, Daniel Almirall, Ambuj Tewari, and Susan A Murphy. Micro randomized trials: An experimental design for developing just-in-time adaptive interventions. Health Psychology, 34(S):1220, 2015 https://pubmed.ncbi.nlm.nih.gov/26651463/
[23] For an early work on categorization of individuals based on previously disparate biometric markers (in this case Autism and Co-morbidities), see Finale Doshi-Velez, PhD; Yaorong Ge, PhD; Isaac Kohane, MD (2014) "Comorbidity Clusters in Autism Spectrum Disorders: An Electronic Health Record Time-Series Analysis." https://pubmed.ncbi.nlm.nih.gov/24323995/
[24] See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3019312/ for an overview, see https://www.researchgate.net/publication/346540764_When_will_individuals_meet_their_personalized_probabilities_A_philosophical_note_on_risk_prediction for a critique, and for a modern example of creating a "patient outcome prediction tool see https://www.nature.com/articles/s43588-021-00141-9?proof=t2013-2-24 ; for a literature review on medical decision-making see https://www.ipr.northwestern.edu/documents/working-papers/2017/wp-17-21.pdf
[25] Jiayu Yao, Emma Brunskill, Weiwei Pan, Susan Murphy, Finale Doshi-Velez, (2021) "Power Constrained Bandits" https://finale.seas.harvard.edu/files/finale/files/power_constrained_bandit.pdf
[26] For example, Y. Abbasi-Yadkori, P. David, and C. Szepesvari. Improved algorithms for linear stochastic bandits. In NIPS, page 2312–232, 2011 https://papers.nips.cc/paper/2011/hash/e1d5be1c7f2f456670de3d53c7b54f4a-Abstract.html; && Shipra Agrawal and Navin Goyal. "Thompson sampling for contextual bandits with linear payoffs," 2012. http://proceedings.mlr.press/v28/agrawal13.html && Akshay Krishnamurthy, Zhiwei(Steven) Wu, and Vasilis Syrgkanis. Semiparametric contextual bandits. arXiv preprint arXiv:1803.04204, 2018 https://arxiv.org/abs/1803.04204
[27] For micro-randomized trials see Peng Liao, Predrag Klasnja, Ambuj Tewari, and Susan A Murphy. Sample Size Calculations for micro- randomized trials in mhealth. Statistics in Medicine, 35(12):1944–1971, 2016 https://pubmed.ncbi.nlm.nih.gov/26707831/ && Predrag Klasnja, Eric B Hekler, Saul Shiffman, Audrey Boruvka, Daniel Almirall, Ambuj Tewari, and Susan A Murphy. Micro randomized trials: An experimental design for developing just-in-time adaptive interventions. Health Psychology, 34(S):1220, 2015 https://pubmed.ncbi.nlm.nih.gov/26651463/ && JN Kramer, F Kunzler, V Mishra, B Presset, D Kotz, S Smith, U Scholz, and T Kowatsch. Investigating intervention components and exploring states of receptivity for a smartphone app to promote physical activity: Protocol of a micro randomized trial. JMIR Res Protoc, 8(1):e11540, 2019 https://pubmed.ncbi.nlm.nih.gov/30702430/

2.2. **Decision Support Tools ('DST'):** A Sociotechnical Lens to make Antidepressant Medication Treatment Decisions – How the new wave of intelligent systems can account for the complexity of medical work? A potential approach.

As our lab has documented with medical doctors,[28] we will likely require greater attention **not just to Machine Learning methods** or Artificial Intelligence, but also **Explanation Systems** (sometimes referenced as "Decision Support Tools' or DST) built on the recent AI explainability literature. More concretely, these DST can help expose discrepancies between how the model is operating and how people believe it should be acting. For example, a model prediction alone does not expose the treatment selection process---which often might benefit from **input from both doctor and patients**. Put simply, DST can focus on co-designing Ai systems.



Features included in the initial prototype (from top to bottom): (A) a patient scenario with stability and dropout scores, (B) stability score feature importance explanation, (C) personalized treatment recommendations.

From there a discussion with doctors focused on four questions:

(1) Imagine this patient is sitting in front of you, how would you make a treatment decision?

(2) What helped you make a decision?

(3) Did anything detract from making a decision? Or your confidence in the decision?

[28] See Doshi-Velez, Gajos, et al "Designing AI for Trust and Collaboration in Time-Constrained Medical Decisions: A Sociotechnical Lens," May 2021 http://www.eecs.harvard.edu/~kgajos/papers/2021/jacobs21designing.pdf For a broader view of interpretability see Finale Doshi-Velez, Been Kim (2017) "Towards A Rigorous Science of Interpretable Machine Learning." https://arxiv.org/abs/1702.08608

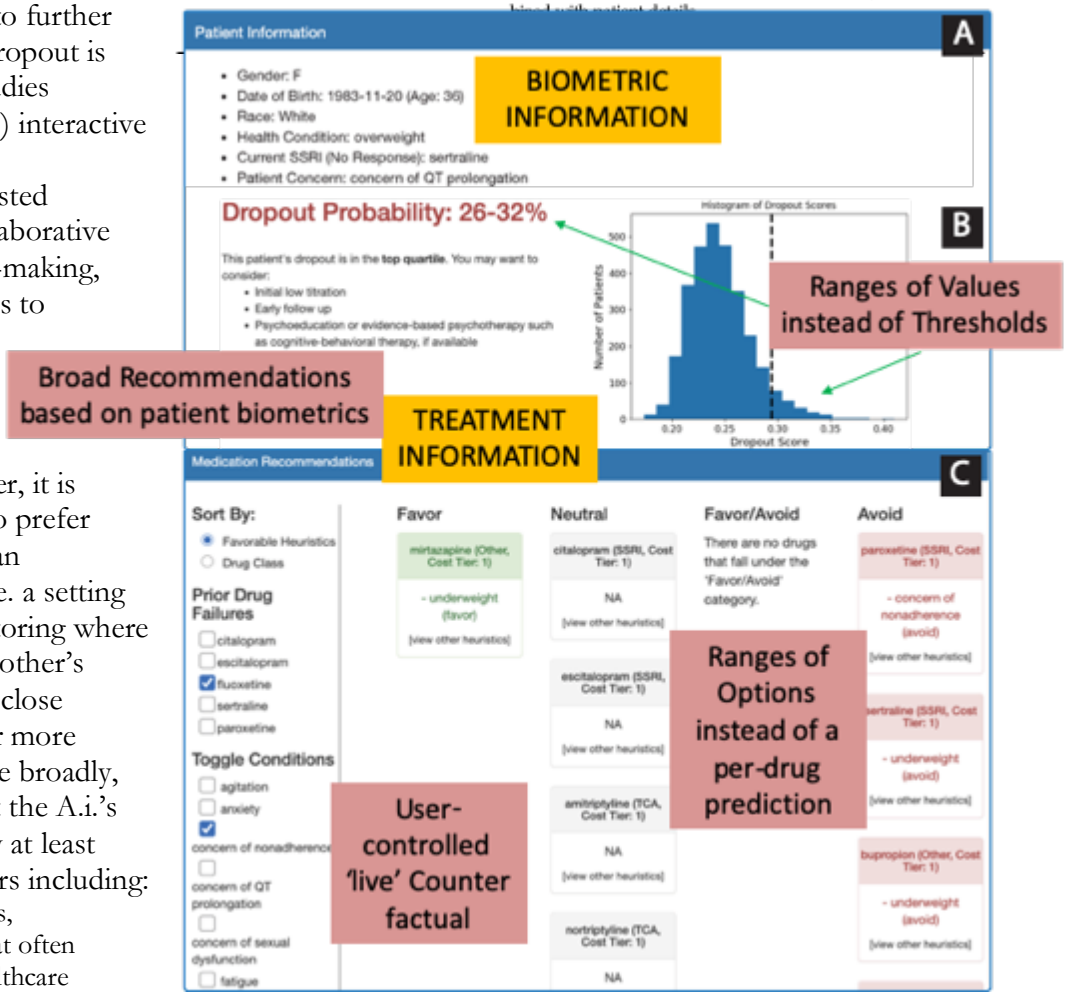
(4) If you were going to design this tool for a colleague, what would they need to make a decision? What would you change?

We identify ways in which DSTs need to engage with the healthcare sociotechnical system, including clinical processes, patient preferences, resource constraints, and domain knowledge. Our results suggest that clinical DSTs should be designed as multi-user systems that support patient-provider collaboration and offer on-demand explanations that address discrepancies between predictions and current standards of care.

Include patient preferences	**Support patient-provider communication, address missing variables** • Make treatment recommendations interactive, so that clinicians and patients may edit the input variables based on changes to a patient's medical history or side effect preferences • When hovering over a treatment, show all potential side effects for that antidepressant, in order to foster communication and education of potential medication effects
Recommend appropriate clinical processes	**Show a path forward, provide actionable information** • For patients with a dropout risk prediction in the top quartile, present recommended next steps based on clinicians' suggestions • Allow for viewing and comparing multiple antidepressant options
Understand system constraints	**Do not require determination of trust at every decision point** • Refocus from model features to model validation process • Present an overview of all model validation steps in a single screen that is accessible from the main interface, but not com-

Features included in the prototype redesign (from top to bottom): (A) patient information, (B) dropout score with links to further information about how dropout is defined and validation studies conducted on the tool, (C) interactive personalized treatment recommendations. Requested changes highlight the collaborative labor of medical decision-making, and the ideal setting seems to not be that the A.i. "models a decision" and "explains/justifies itself to the user" as in our initial mock-up. Rather, it is mutual. Clinicians seem to prefer what some have dubbed an "algorithmic situation," i.e. a setting of potential mutual monitoring where each is accessible to each other's influence; often from the close proximity between two or more ~~individuals~~ entities.[29] More broadly, our research suggests that the A.i.'s co-design is influenced by at least four socio-technical factors including:

i. patients' preferences,
ii. clinical processes that often include multiple healthcare providers,



[29] See Anders Persson (2019) "The development of Goffman's interactional Frame and framing," Routledge https://library.oapen.org/bitstream/id/3e0769f6-f76b-4c1e-b55c-b7b11c8d34c6/9781472482587_text.pdf

iii. the constraints of the healthcare system, and
iv. Existing domain knowledge

We posit that by making these aspects of healthcare central to the design of DSTs, we may develop tools that are capable of supporting the collaborative nature of healthcare, identifying potential adverse events caused by ML predictions, working within time-critical environments, and recognizing conflicting information. However, we do not expect that the sociotechnical factors discussed here represent the full set of sociotechnical considerations that need to be included in AI design (In fact, we highlight in the Appendix an example of recent work by our co-author Professor Krzysztof Gajos that uses a persons' mouse movements to diagnose Ataxia and Parkinson).[30]

Rather, we present this as an initial step in a broader research agenda determining how the new wave of intelligent systems must account for the complexity of medical work.

3. Security: No Comment from our lab.

4. Harms: See (6) Governance, particularly (e), (g) and (h)

5. Benefits: See (6) Governance, particularly (b) and (c)

6. Governance: A.i. Explainability (XAI) for All Agenda – XAi4ALL

Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case. Please note any governance measures that are required by law or by government, including human or civil rights frameworks, or corporate policy, including ethical principles, in cases of deployment, as well as any planned governance measures for planned or current-use biometric technologies

6.1. (a) Stakeholder Engagement: Roadmap for Responsible Machine Learning for Health Care

Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies.

Our proposed roadmap has a comprehensive overview of the barriers to deployment and translational impact. With a view toward accelerating safe, ethically responsible and meaningful progress in ML for health care, we lay out critical steps to consider when designing, testing and deploying new solutions.[31] More broadly, although successful translation requires bringing together expertise and stakeholders from many

[30] See Krzysztof Z. Gajos, Katharina Reinecke, Mary Donovan, Christopher D. Stephen, Albert Y. Hung, MD, Jeremy D. Schmahmann, MD, Anoopum S. Gupta, MD, PhD: (2019) "Computer Mouse Use Captures Ataxia and Parkinsonism, Enabling Accurate Measurement and Detection" Movement Disorders. http://www.eecs.harvard.edu/~kgajos/papers/2020/gajos19computer.pdf

[31] See Jenna Wiens , Suchi Saria, Mark Sendak, Marzyeh Ghassemi, Vincent X. Liu, Finale Doshi-Velez, Kenneth Jung, Katherine Heller, David Kale, Mohammed Saeed, Pilar N. Ossorio, Sonoo Thadaney-Israni and Anna Goldenberg, "Do no harm: a roadmap for responsible machine learning for health care" https://finale.seas.harvard.edu/files/finale/files/do_no_harm-_a_roadmap_for_responsible_machine_learning_for_healthcare.pdf

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Deloitte

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Deloitte.

Public and Private Sector Uses of Biometric Technologies

January 14, 2022

In response to Office of Science and Technology Policy Request forInformation (RFI)

January 14, 2022

Mr. Suresh Venkatasubramanian
Assistant Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: RFI Response: Public and Private Sector Uses of Biometric Technologies

Dr. Suresh Venkatasubramanian,

Deloitte[1] is pleased to submit a response to the questions posed in the Office of Science and Technology Policy (OSTP) Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.

Deloitte applauds OSTP's effort to review the current marketplace and policy landscape related to biometric technologies. Biometrics have a long-standing role in protecting systems and services we rely upon. The use of Artificial Intelligence (AI) has enhanced the efficacy of some of those technologies, and it is important for OSTP to fully understand any unintended consequences of this application of AI.

We support the distinction that OSTP makes between biometric recognition and biometric inference to ensure clarity in the broader marketplace. In this response, we offer: our experiential observations; proposed principles; and recommendations for consideration in our enclosed response prepared by the Deloitte AI Institute for Government. Deloitte's perspective is based on years of working with public and private sector organizations to carefully implement AI-enabled technologies to meet mission and business objectives while protecting privacy and civil liberties.

In the short term, we believe that clear classification of biometric technology use cases, along with the articulation of core AI Risk Management principles are essential. In the medium and longer term, we believe these measures combined with robust governance, broader availability of reliably inclusive data sets, wider use of standardized test methods, strong security and consent-based privacy safeguards, in addition to proactive mitigation of sources of errors and bias can lead to better public policy outcomes.

We would be pleased to have further dialog with OSTP as it continues to explore the concept of an AI Bill of Rights and reviews the responses from this and any future RFIs. Please do not hesitate to contact us, should you have any questions.

Sincerely,

Ed Van Buren
[redacted]
Principal
AI in Government Leader,
Deloitte Consulting LLP

Colin Soutar
[redacted]
Managing Director
Government and Public Sector
Cyber & Strategic Risk Products and Technology Lead,
Deloitte & Touche LLP

[1] As used here Deloitte means Deloitte Consulting LLP and Deloitte & Touche LLP, subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Table of Contents

Company Profile

Company Name	Deloitte	
Headquarters Location	New York City, New York	
Contact Name	Ed Van Buren	Colin Soutar
Contact Title	Principal	Managing Director
Email Address	[redacted]	[redacted]
Phone Number	[redacted]	[redacted]

Executive Summary

Artificial Intelligence (AI) is a powerful tool capable of enhancing U.S. economic prosperity and national competitiveness. AI-enabled automation empowers the government and private sector to achieve progress through enhanced security effectiveness, cost-saving efficiencies, and increased accuracy. In the biometric arena, the impact of AI is already being realized in significant and far-reaching ways, namely by enabling significant advances in performance. In this RFI response, we offer perspectives related to the application of AI to biometric technologies, which may be leveraged to inform an AI Bill of Rights.[2]

In March 2021, we established the *Deloitte AI Institute for Government* to drive the use of AI in a fair and trustworthy way through research, eminence, and applied innovation.[3] We draw upon our deep AI experience for this response, as well as the experience of our **biometric subject matter specialists**, including Colin Soutar[4], who previously helped establish the biometric industry via biometric systems development and deployment in addition to serving in leadership roles and making technical contributions to national (e.g., NIST, INCITS, ANSI) and international biometric standards (e.g., ISO/IEC).[5]

Based on our experience and the latest research, we believe OSTP should embrace core principles as it seeks to develop effective frameworks for the development and use of biometric technologies in both the public and private sectors:

- *Clarity*: biometric technology terminology should adhere to national and international **standards**. Terms such as "**recognition**" and "**inference**" should be clearly defined and deployed in appropriate context to ensure common understanding across stakeholders in the ongoing national dialogue around AI and biometrics. (Response 1)

[2] https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/
[3] https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-launches-ai-institute-for-government.html
[4] https://www2.deloitte.com/us/en/profiles/colin-soutar.html
[5] NIST (National Institute of Standards and Technology; INCITS (InterNational Committee for Information Technology Standards); ANSI (American National Standards Institute); ISO/IEC (International Organization for Standards/International Electrotechnical Commission)

- *Transparency*: Standardized testing is a critical tool for building successful biometric systems. **Inclusive** and **trustworthy** training and testing data is the foundation of fair and accurate biometric solutions. The federal government is uniquely positioned to publish these data assets in a coordinated fashion for broad use by biometric technology developers as well as organizations and third parties wishing to evaluate currently deployed and/or emerging biometric systems. (Response 2)
- *Security:* Individuals have a **right** to understand how their biometric data is collected and used. Organizations developing or implementing biometric technologies should build in security and **consent-based safeguards** up front and ensure **accountability**, for example through procurement requirements. (Response 3)
- *Mitigation:* Like any other technology, biometric solutions do not exist in a vacuum and they are not infallible. Biometric algorithms along with associated sensors, data, users, processes, and operating environments can contribute to errors. Proactively identifying and measuring the **causes of errors** can help mitigate unintended consequences. In addition, AI-enabled solutions should be designed to reduce the potential for **algorithmic bias**. (Response 4)
- *Adoption:* The use of biometric technologies is **widespread** and accelerating in our institutions, the economy, and broader society. This trend is likely to continue as individuals and organizations reap the **benefits** of biometrics, and new innovations come to market. (Response 5)
- *Governance:* Biometric governance should enable **innovation** and guard against potential **misuse** by public and/or private sector entities. A tailored approach designed around clearly defined use cases and core AI risk management principles, such as those championed by Deloitte[6], can yield high quality public policy outcomes. This is consistent with the approach that NIST is taking in the development of their AI Risk Management Framework.[7] (Response 6)

We believe OSTP's inquiry into the state of biometrics in the public and private sectors will continue to foster accurate, successful, fair, and judicious use of this important technology. We are pleased to share our knowledge from our historical and ongoing experience advising government and commercial organizations on the implementation of biometric concepts, technologies, and solutions.

Response 1: Descriptions of use of biometric information for recognition and inference

Biometric technologies are built on decades of research and development in computer vision and pattern recognition. The integration of AI into biometric recognition and inference has yielded unprecedented growth in system accuracy and applications.

Biometric algorithms are generally deployed in two ways: **recognition** or **inference**. In the former, the system is attempting to verify or identify a person based on biometric inputs (i.e., does this sample match this other sample?). In the latter, a system is attempting to detect a specified state, for example: an emotion, signs of fatigue, and so on. It is critical for public and private sector organizations to know the differences so they can select solutions that meet their mission or business requirements. Within the realm of recognition it is also important to be aware of the differences between biometric verification and identification.[8]

Table 1: Differences between Biometric Recognition and Inference

	Recognition	Inference
Application	Verification and/or Identification	Detection
Data	Modalities: Fingerprint, Face, Iris, Voice, DNA, etc.	States: Fatigue, Anxiety, Fear, Deception, etc.
Data Sources	Opt-in Enrollments, Watchlists, Criminal Databases, Training Datasets	Encounter Data, Real-time Samples, Training Datasets
Input	Claim AND Reference Biometric Info	Subject Biometric Info
Decision	Match/Hit OR No Match/No Hit	Detected OR Not Detected

[6] https://www.nist.gov/system/files/documents/2021/09/15/ai-rmf-rfi-0073.pdf
[7] https://www.nist.gov/itl/ai-risk-management-framework
[8] See Response 2 for more detail

As depicted in Table 2, biometric inference and recognition systems are currently deployed across a wide range of use cases including but not limited to[9]:

Table 2 Sample of Current Deployments of Biometric Recognition and Inference

	Context	Goals	User Data Collected (and Purpose)	Impacted Communities
Border Security[10]	International inbound and outbound air travel (e.g., biometric entry/exit)	Fulfilling statutory mandate to biometrically process arrivals and departures, detecting imposters and threats (e.g., terrorists)	Facial, Fingerprints (recognition)	International Travelers
Aviation Security[11]	Domestic airport security checkpoints	Enhancing security, efficiency, and air travel experience	Facial, Fingerprints (recognition)	Trusted Travelers[12]
Law Enforcement	Federal, state, and local investigations	Matching evidence from crime scenes to individuals, developing investigatory leads	Fingerprints, DNA, Facial (recognition)	Suspected Parties
Workforce Vetting[13] **and Human Capital**	Public and/or private sector employers	Ensuring personnel meet employment requirements and are continuously authorized for access to secure facilities and systems	Fingerprints, Facial, (recognition) Keystrokes (recognition and/or inference)	Employees, Contractors [14]
		Providing productivity tools for administrative tasks, detecting signs of stress (i.e., burnout)	Voice (recognition and/or inference)	Employees
Financial Services	Various banking institutions	Combating fraud via speech analysis	Voice (recognition and/or inference)	Account Holders
Citizen Identity[15]	Foreign governments (e.g., India's Aadhaar system)	Enabling financial inclusion especially for remote communities; reduction in fraud, waste, and cost	Fingerprints, Facial and Iris (recognition)	General Population

We believe the **transparent** and consistent classification of recognition and/or inference applications and use cases is critical for ensuring common understanding across **diverse** public and private sector stakeholders with a vested interest in the effective development and governance of biometric technologies.

Response 2: Procedures for and results of data-driven and scientific validation of biometric technologies

Policy makers should enable continuous evaluation of biometric systems using internationally adopted testing standards to ensure they support mission and objectives. The government should consider making authoritative, reliable, and inclusive biometric data sets available for development and testing.

Systems using biometric information are typically tested via methodologies that follow traditional detection theory. These scientific methodologies evaluate performance on any given measurable factor with great

[9] See Response 5 for a more exhaustive list of biometric use cases
[10] https://biometrics.cbp.gov/
[11] https://www.tsa.gov/biometrics-technology
[12] https://ttp.dhs.gov/
[13] https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-security-in-digital-era.html
[14] https://www.commerce.gov/osy/programs/credentialing/hspd-12-credentialing (federal employees/contractors)
[15] https://www.imf.org/en/Publications/FM/Issues/2018/04/06/fiscal-monitor-april-2018

precision. Speed, scale, availability, and system reliability are performance measures used to evaluate biometric systems. As biometric matching is inherently **statistical** – using decision thresholds that accommodate the fact that no two samples from the same individual are identical – system performance is sensitive to testing set size and coverage.

Internationally recognized testing and reporting **standards** offer generalized and standardized procedures to evaluate biometric systems.[16] Organizations such as NIST have also developed authoritative expertise in reliable, independent, and fair assessment of biometric systems.[17] Similarly, DHS Science and Technology Directorate's Biometrics and Identity Management Technology Center evaluates biometric and identity technologies to optimize performance for a variety of operational scenarios and online use cases.[18] The methodologies adopted by these organizations offer trustworthy guidance in understanding performance variation in a variety of factors including operating conditions, human factors, and demographics.

As noted previously, biometric systems are inherently statistical, and their performance ultimately reflects a **trade-off** between two error types: false positive errors and false negative errors (see Table 3 below). In other words, biometric systems are trained to accommodate multiple instances of the same user presenting their biometric sample, while rejecting samples from other users. The data sets and training methods used to train the biometric processes need to ensure the systems will be **inclusive** of all intended users, and that the system has been properly configured for an organization's given mission or business **security requirements**.

Table 3: Types of Biometric Errors[19]

System	False Positive	False Negative
Recognition: Verification	False Acceptance Rate (FAR): proportion of transactions with false biometric claims erroneously accepted.	False Rejection Rate (FRR): proportion of verification transactions with true biometric claims erroneously rejected.
Recognition: Identification	False Positive Identification Rate (FPIR): proportion of identification transactions by capture subjects *not* enrolled in the system for which a non-empty list of candidate identifiers is returned.	False Negative Identification Rate (FNIR): proportion of identification transactions by capture subjects enrolled in the system for which the subject's correct identifier is *not* included in the candidate list returned.
Inference: Detection	Sample from person not exhibiting trait incorrectly determined to exhibit it.	Sample from person exhibiting trait incorrectly determined not to exhibit it.

For testing, it is important to emphasize a **ground truth** and assign expected outcomes to the performed tests to ensure accuracy and fair observation of the system's performance. Different data sets should be used for **testing** the systems and for **training** and **tuning**. An additional consideration is to ensure test data reflects the operational conditions associated with the system. For example, camera images as probes and passport/visa images as gallery samples can be ideal to assess the performance of facial recognition (FR) in a travel use case, but other types of imagery may be best for other use cases. Controlling other factors like illumination can allow the test setup to resemble an **operational scenario** even more closely. Table 4 illustrates common testing methodologies for recognition and inference applications.

Table 4: Biometric Testing Methodologies

Application	Data Sets	Tests
Recognition: Verification	Genuine: Two or more samples from each person Impostor: Samples of non-matching persons	Score distributions from match combinations of genuine and impostor sets. False positive and negative rates at possible score thresholds yield aggregate-based Detection Error Trade-off (DET) curve. DET provides insights into impact of different operating points on security and user experience.

[16] https://www.iso.org/standard/73515.html
[17] https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software
[18] https://www.dhs.gov/science-and-technology/BI-TC
[19] FAR, FRR, FPIR, and FNIR definitions from ISO-IEC 19795-1 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework - WD3 – pages 33 through 35

Recognition: Identification	Probes: Samples, some of which have matching identities in gallery Gallery: Population containing samples from identities including probe	Probes searched against gallery to assess false positive and false negative identification rates, with considerations for rank. Cumulative Match Characteristic (CMC) curve helps assess identification performance by viewing accuracy as candidate list sizes (and ranks) vary. Accuracy is sensitive to gallery size, decreasing with larger galleries.
Inference: Detection	Labeled data sets with ground truth on detection decision	System's ability to make correct binary (detected-not detected) or gradual (least detected-most detected) decision on inferred state evaluated by comparing test outcomes to ground truth.

Given the importance of using reliable and **inclusive** data sets to develop biometric systems and assess their performance (and the significant resource burden for researchers and private businesses to acquire such data sets), the government may consider acquiring and maintaining them. Publicly available portions could be used for development and training of biometric systems, while other portions could be embargoed for subsequent government or **third-party testing** of biometric system performance.

Response 3: Security considerations associated with a particular biometric technology

Individuals have a right to understand how their biometric data is used. Developers and organizations implementing biometric solutions should enhance privacy and security protections by proactively building safeguards to protect users as well as assets and operations.

The security of biometric systems is designed, developed, and evaluated with respect to two categories. The first is security unique to biometric systems, and the second category includes security concerns found in all technical systems including **security of data** in transit, data at rest, and other vulnerabilities.

In 2016-2017, Deloitte supported NIST in developing Strength of Function for Authenticators (SOFA) – Biometrics[20] which leveraged long-standing biometric security principles developed in the late 1990s and 2000s.[21] The SOFA-Biometrics effort outlined security considerations specific to biometrics to include:

- Attempts to override components of a biometric system (i.e., capture device, signal processor, comparator, database, decision engine)
- Attempts to modify information (i.e., biometric template, probe, biometric reference, score, decision) and
- Presentation attacks (e.g., providing **spoofed** biometric data to the sensor)

Defenses against these types of vulnerabilities are becoming increasingly necessary and commoditized with broader use of fully automated, user-centric solutions in a digital environment. Additionally, considering the large quantities of data used by biometric inference systems, the potential vulnerability of the systems that capture, process, and retain this data is another security risk that deserves additional evaluation.

Just as individuals have a right to understand how their biometric data is used and expect **safeguards** built to protect their **privacy** and security, organizations have a responsibility to acknowledge these rights and offer security and privacy in the biometric products and services they offer. It is in the best interest of organizations to strengthen biometric security and privacy controls for their own mission or business success. Standards-based scientific approaches that quantify and classify the strength levels of biometric systems empower organizations to acknowledge the risks associated with biometric information and systems, and make informed design decisions. Vendors are increasingly interested in incorporating standards-based security requirements in their designs. Articulating biometric security requirements during **procurement** can further motivate them to proactively address these issues.

Response 4: Exhibited and potential harms of a particular biometric technology

Biometric errors and their consequences are measurable, mitigatable, and multi-faceted. Data, algorithms, sensors, operational constraints, users, and operational processes are all part of a larger system. Understanding how they are connected is imperative to devising strategies to help mitigate "bias" and errors.

[20] https://pages.nist.gov/SOFA/SOFA.html
[21] Security considerations for the Implementation of Biometric Systems. Colin Soutar. Automatic Fingerprint Recognition Systems. Springer. 2004

Biometric technology developers and organizations implementing biometrics solutions must **continuously** evaluate their systems to ensure they are fulfilling clearly defined objectives. To the best of their abilities, they must identify and mitigate unintended **errors** and their **consequences**. The consequences of typical biometric errors (defined above in Table 2), no matter how infrequent compared to the volume of successful transactions, will vary depending on organization, application, use case, and users involved. Biometric errors can yield negative consequences for both organizations and individuals, as summarized below in Table 5. Both error types may result in unintended harm. Biometric system owners must strike a **balance** between the need to reduce false positives and the need to reduce false negatives based on their specific risk appetite.

Table 5: Consequences of Biometric Errors

	Individual Consequences	Organizational Consequences
False Positive	I have been mistaken for someone else or someone has been mistaken for me	Access has been granted to someone who should not have it (i.e., **vulnerability**)
False Negative	I was denied access to something I should have access to (i.e., **inconvenience**)	Denial of rightful user access resulted in inefficiency and requires resolution
Failure to Acquire	I am unable to use the technology because it cannot acquire my biometric information	An alternative solution or process must be developed and offered to the user

As articulated in Response 2, biometric errors occur due to the inherently statistical nature of the technology. AI has vastly improved the performance of biometric systems, particularly facial detection and FR, however research indicates algorithms that primarily rely on AI may be impacted by how representative their **training** sets are of the general population.[8] If, for example, FR training data sets are overweighted towards younger faces, then algorithms trained on these data sets may perform better on those subjects relative to the general population. Left unaddressed, the use of under-representative data to train AI-enabled biometric solutions could lead to sub-optimal outcomes across a broad range of applications due to **algorithmic bias**.

It is critical to realize not all algorithms are created equal and it is important to "*know your algorithm*." Decision makers across the public and private sectors should strongly consider this when tasked with the responsibility of selecting or designing a holistic biometric solution. While NIST's recurring **benchmark** testing show overall biometric performance continues to improve, certain algorithms still perform measurably better than others.[22] This insight underscores the importance of selecting the right solution for a given use case and the need for **rigorous** testing and evaluation both during initial deployment and on an on-going basis.

Authoritative testing and reporting can only be done using **reliable** data sets, and the federal government is well positioned to make such training sets available through its ongoing engagement with the biometric industry, academia, and interagency partners across the government. This is critical to evaluate performance, understand how it meets the organization's mission objectives and risk tolerance, and ensure even more accurate and **equitable** results across the broadest possible range of use cases.

In addition to algorithmic performance, it is important to account for other variables including **sensors** and the environment in which they operate. Research indicates the specifications of a biometric sensor (e.g., a camera) have significant impact on the quality of the resulting data (e.g., imagery) and subsequently, on the overall performance of a biometric system. Operational constraints and **environmental factors** affecting biometric sample quality (e.g., lighting, occlusions, usability for FR) must be considered when designing a high-performing biometric system.

Lastly, decision makers should consider non-technical aspects of biometric solutions: the people operating them as well as the processes governing their use. Depending on the use case, a biometric process alone may be deemed insufficient for automated decision making, requiring a **human in the loop** to make a final determination. In other use cases, total **automation** may be desirable. In either case, increased emphasis on training – combined with development and procurement of best in breed technology – can lead to better outcomes.

[22] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-facial-recognition.pdf

The causes and consequences of biometric errors are identifiable, measurable, and can be mitigated through holistic system design and rigorous testing. Robust **governance** would incorporate these insights to help the public and private sectors mitigate risks while unlocking the value and benefits of biometric technologies.

Response 5: Exhibited and potential benefits of a particular biometric technology

Biometric technologies can enable enhanced security, efficiency, and user experience. The ongoing integration of biometrics into our institutions, our society, and our economy is likely to continue as individuals and organizations continue to reap value from their use.

Biometric technologies already exhibit a **multitude of benefits** across the public and private sectors. Biometric solutions enable users to authenticate themselves quickly and accurately; they give organizations confidence that critical assets are protected; and they facilitate post-event forensic analysis and investigation. In general, biometric systems are implemented to enhance one or more of the following: **security** (e.g., public safety), **efficiency** (e.g., speed, throughput, staffing), and **experience** (e.g., for the operator, user, customer). Depending on the organization, its specific objectives, and use cases, one or more of these three drivers may be emphasized to a greater or lesser degree in overall system design and deployment.

Biometric technologies are deployed in a **wide variety of use cases**, as outlined in Response 1, and illustrated in Table 6 below.

Table 6: Widespread Use of Biometrics

Economic and Social Sectors	Sample Biometric Use Cases	
National Security	✓ Force Protection	✓ Counter-terror, Counter-intel[23]
Homeland Security	✓ Border and Aviation Security	✓ Immigration Control
Law Enforcement	✓ Investigations	✓ Forensic Analysis
Benefits Access and Distribution	✓ Fraud Prevention	✓ Equitable Distribution
Workplace and Education	✓ Physical and Systems Access	✓ Time and Attendance
Travel and Hospitality	✓ Contactless Travel	✓ Customized Experiences
Citizen Identity	✓ License Issuance (REAL ID)	✓ Passport/Visa Issuance
Healthcare	✓ Biomedical Research	✓ Patient Medical Records
Telecommunications	✓ Mobile Device Security	✓ Application Login
Retail	✓ Theft Prevention	✓ Contactless Payments
Financial Services	✓ Secure Transactions	✓ Fraud Prevention
Automotive	✓ Access and Ignition	✓ Person/Object Detection

Additionally, biometrics play a key role in securing critical **credentials**, including workplace access cards (e.g., PIVs), student IDs, licenses, and passports/visas, wherein issuing authorities rely on biometrics to ensure applicants are who they claim to be. This protects the **integrity** of the credentials, allows verifying entities to **trust** the authenticity of the IDs, and helps combat fraud. Biometrics will continue to secure identities as public and private sector issuing authorities explore the virtualization of physical credentials into products such as mobile driver's licenses (mDL) and other digital travel credentials.[24] Moreover, biometric **multifactor** authentication is an important tool to combat fraud through more secure accounts and transactions.

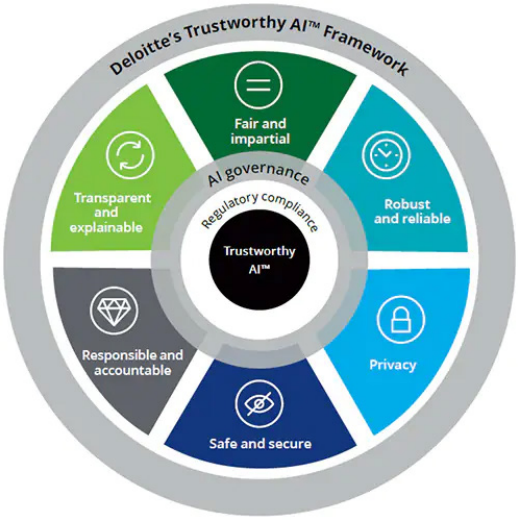
Policy makers should weigh the significant benefits of biometric technologies already deployed throughout our society and the economy as they consider how best to govern their use going forward.

Response 6: Governance programs, practices, or procedures

Biometric governance must enable continued innovation while providing meaningful protection against misuse. A nuanced approach based on core principles and defined use cases may hold the key to effective governance.

[23] https://www.wsj.com/articles/biometrics-smartphones-surveillance-cameras-pose-new-obstacles-for-u-s-spies-11638009002
[24] https://www.iso.org/standard/69084.html

In our experience, there is **no one-size-fits all approach** to governing the use of biometrics. We believe governance programs, practices, and procedures are best designed, with **broad buy-in**, around biometric use cases and the context in which they exist. We also acknowledge the need to maintain balance between **innovation** and the **public interest**.



Core principles can serve as starting point for biometric governance whether it comes in the form of an AI Bill of Rights or other forms (e.g., legislation, regulation, standards). Deloitte published the **Trustworthy AI™ Framework**[25] to guide organizations on how to apply AI responsibly and ethically within their businesses or missions. The framework seeks to provide a common language to help organizations develop safeguards and introduces a multi-dimensional perspective for designing, developing, deploying, and operating AI-powered systems through six considerations. These considerations are congruent with characteristics listed in NIST's proposed AI Risk Management Framework (RMF) and can be readily tailored for the biometric domain:

- *Fair and Impartial*: Organizations should determine what constitutes fairness and impartiality by actively identifying any underlying sources of bias and/or errors within their biometric solutions and implement controls accordingly.
- *Transparent and Explainable*: Organizations should provide the public with clear **notice**, terms, and conditions about the use of biometrics and ensure these are enforced.
- *Robust and Reliable*: Organizations should work to ensure their biometric implementations produce **accurate** and expected results. Procedures for handling errors and anomalies should be developed before they occur and updated as issues are identified.
- *Privacy*: Solutions must be built with **consent** and privacy in mind to protect sensitive data and information about users. Biometric data should only be used for stated purposes, and organizations should ensure user data is not unduly leveraged beyond its intended uses.
- *Safe and Secure*: Biometric solutions must be **safe** and secure to reduce the potential for misuse and risks associated with biometric data theft and exfiltration.
- *Responsible and Accountable*: Organizations should develop policies to establish who is responsible and accountable for system performance. Risks should be anticipated, identified, and communicated clearly to users along with **remedies** (e.g., redress) when incidents occur.

We encourage OSTP to leverage examples in our Trustworthy AI™ Framework as well as security and privacy principles found in U.S. government frameworks, such as the NIST Cybersecurity Framework[26] and the NIST Privacy Risk Management Framework[27], both of which Deloitte helped develop.

Conclusion

The effort undertaken by OSTP to explore a national AI Bill of Rights and to understand the value and limitations of biometric technology represents an opportunity to articulate a practical, nuanced framework for the use of biometrics that enables innovation, secures citizen rights, and provides clarity to industry and implementors across the nation. Clear communication about the complex nature of biometrics is imperative to gain public trust in the use of these technologies and the application of AI to biometrics. Deloitte representatives would be pleased to continue the conversation and share our knowledge from experiences advising and working to implement biometric technologies on behalf of government and commercial clients.

[25] https://www2.deloitte.com/us/en/pages/deloitte-analytics/solutions/ethics-of-ai-framework.html
[26] https://www.nist.gov/cyberframework
[27] https://www.nist.gov/privacy-framework/privacy-framework

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Dev Technology Group

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

RFI Response

Introduction

Per the RFI requirements, we offer the following information to our RFI comments:

#	RFI Requirement
1	**Name of person(s) filing the comment:** • Niroop Gonchikar – Biometric Technical Director • Sanjeev Duggal – Biometric subject matter expert (SME) • Antonio Trindade – Biometric Solution Area Vice President and SME
2	**Name of organization:** Dev Technology Group, Inc.
3	**Respondent type:** Industry
4	**Respondent's role in the organization:** Biometric Solution Area
5	**Number of topics to which we are responding:** 1, 2, 3, 4, & 5

Response to Request for Information

1. Descriptions of use of biometric information for recognition and inference

We provide our various Government clients planning, development, deployment, sustainment, and enhancements of biometric information through mission-critical systems. These teams support the use of biometric information for recognition and interference as shown in the bolded project descriptions below. These projects support positive impacts to communities and national security, such as:

- ✓ Deployment of biometric solutions in support of identification, for the purposes of ensuring safety of personnel interacting with unknown persons
- ✓ Prevent unwanted entry of dangerous or high-risk individuals
- ✓ Verify proof of physical location and reduce unnecessary stressful interactions with law enforcement

As stated above, we support various Department of Homeland Security (DHS) and Department of State (DoS) clients with biometric solutions, including the following:

Enforcement Removal Operations - We provide operations and maintenance, software development, implementation, and modernization for a suite of systems that are used to support immigration-related functions for DHS Immigration and Customs Enforcement (ICE). This suite of systems is used by agents across ICE and supports users throughout DHS and other agencies such as DoS and the Federal Bureau of Investigation (FBI). We migrated all these systems to the cloud, specifically to the Amazon Web Services (AWS) GovCloud environment, and we are currently modernizing these systems to use an event-first and serverless architecture. As a part of our support on this contract, we handle various complex requirements including biometric information for identification. The suite of Enforcement Systems book, process, and manage every one of these subjects and use biometric information for identification. This program is constantly affected by executive orders, changing political and government needs, and information privacy policies requiring the ability to be proactive and deploy changes quickly. Our team also controls the management of fingerprints and mugshots (digital images), as well as various documents (e.g., NTAs) through the EID Arrest GUI for Law Enforcement (EAGLE) and Eagle Direct (ed) Identification Environment (EDDIE) systems. EAGLE is a universal booking system that supports criminal and administrative arrests, with improved biometric capabilities for fingerprint and continued expansion of biometric identification. EAGLE uses

modern system interfaces to communicate biometric information with other federal agencies in pursuit of reliably identifying aliens. EDDIE is a mobile application that provides the ability to capture/collect, transmit, and return search results for biometric information (e.g., fingerprints) from the field.

We have been collaborating to develop an innovative application that will allow ICE to have a completely web-based solution. After analyzing various options, our team recently performed a successful proof of concept using the Electron Library integrated into the Node.js biometric microservice. The solution was successful in connecting the ICE fingerprint scanner into the web-based framework, and this approach will allow ICE to plug and play various peripherals without the need to deploy a desktop application or download drivers as new equipment comes to market.

EAGLE/EDDIE provides high availability for processing individuals, including mobile capabilities for field operations. It integrates with a range of biometric components for increased accuracy in identifying individuals, in addition to other internal ICE applications as well as data sources outside ICE for improved knowledge gained by data sharing. Another example of our digital management services is our work on implementing the Biometric Rest Service (BRS). Several applications in the portfolio require fingerprint and mugshot data from the Office of Biometric Identity Management (OBIM), so our booking team developed a single BRS to interface with OBIM that is utilized by multiple applications to retrieve that data. This **reduced development overhead** by having one system create the service and also **will reduce maintenance** down the road.

Lastly, we have completed many system enhancements on this program and notably two (2) specifically related to biometric data.

1. Completed the removal of ICE system dependencies on IDENT Schema through a series of 13 releases - *Reduced cost, decreased maintenance complexity, streamlined OBIM and biometric data access.*
2. Built a DNA collection interface into EAGLE to allow ERO to collect, process, and share DNA information - *Allows ERO to quickly collect data and share this additional biometric data with the FBI.*

Publicly available documentation on the above referenced systems:

- https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-eid-may2019.pdf

E3 Biometrics (E3B) - We led the design and development of the E3 Biometrics (E3B) module. This module facilitates the capture of biometric information and manages the integration with US-VISIT, FBI, and DOD-ABIS via the JABS Gateway. This web-based application integrated CBP's biometric capture devices from multiple vendors to the application.

Our team led the design and development of the biometrics application within the Office of Border Patrol's booking system for the E3 Biometrics project. The E3 Program supports the Border Patrol and the Office of Field Operation (OFO) missions by centralizing information for activities related to booking, enrollments, and prosecution of illegal aliens

Biometric information is a key element in countering threat anonymity. Current restrictions on data sharing and biometric data transfer limit our nation's ability to identify potential threats. Dev Technology's biometric data sharing platform enables sharing data and improving transparency to achieve near real-time resolution of identity, thereby improving national security.

into one enterprise-wide system and creates standard and repeatable processes across the organization. We provided full 10-print/2-print, photo and iris capture, and submission and vetting of biometric data for the OBP and OFO Secondary Inspections. Additionally, we implemented the Federated Person Query (FPQ) module of the application. This module provides person-centric responses, based on Biographic checks, from a variety of law enforcement systems. In addition, we developed and deployed a mobile E3 Biometrics solution, called E3 Lite, to allow for the capture and processing of Biometrics leveraging a mobile device in the field.

We deployed the E3 Biometrics solution to Border Patrol Stations across the country and maintained multiple interfaces to other systems across DHS and other agencies such as DOD and FBI. Our SMEs led the effort to create an E3B Iris Pilot, working closely with OBIM, DOD, and FBI Next Generation Identification (NGI). This effort required extensive technical collaboration and integration with these government partners, and our established technical relationships enabled us to more quickly complete tasks that required collaboration across DHS. **This solution won the 2014 ACT-IAC Igniting Innovation Award** in the category of High-Risk/High-Reward for an innovation solution to a difficult problem, as described below.

- ***Successful compliance with Service Level Agreements:*** In FY15, we planned, developed, and successfully implemented 18 releases into production. Each release was implemented according to the established schedule, and without defects.
- ***Degree of customer satisfaction or evidence of the same:*** CBP has been highly satisfied with our support of this system as proven by customer satisfaction surveys, high CPAR ratings, and industry awards.

Biometric Data Sharing – Our biometric data-sharing platform is currently operational in support of the Government of Mexico (GOM) for sharing data with DHS. Biometric capture stations are currently deployed at migration stations and airports across Mexico.

The data exchange component is a cloud-ready software application that accepts a 2-way trusted web connection using TLS with client certificate authentication from a potentially lower trust network or environment, and forwards to a secure DHS enclave through VPN tunnels and security appliances. The data exchange can accept multiple biometric data formats and transforming to multiple NIST NIEM and CJIS EBTS based standards for consumption by Automated Biometric Identification Systems (ABIS), allowing biometrics searches and enrollments. The data exchange also allows a response to the submitting entity. Currently, the rules and security around what data is shared back to the submitting entity is controlled by the DHS IDENT automated biometric system, which allows configurable rules-based data sharing back to any specified mission partner, in this case the GOM.

Our team of biometric SMEs was responsible for the following innovations to meet client goals:

- ✓ Biometric Data Sharing Platform - Our solution has effectively extended the southwest US border—from a detection and early warning standpoint—farther south. For example, live scan biometric captures confidently place a subject at the location of capture at a specific time. The biometric data sharing program rapidly identifies persons of interest, understands trends and patterns that can influence approaches in combating exploitation, and informs adjustments to policy. The effect of policy changes can be observed in real time; as subjects make shifts in behavior, we can collect new data points and compare it to previous information.

- ✓ Universal Biometric Client - This is an easy-to-use biometric client that can be deployed as a kit, or out of the box. This client allows the capture of face and fingerprint with the ability to expand to include additional modalities. This client uses industry standards for packaging and transmission of biometric encounter data to be sent to the data exchange component.
- ✓ Encounter Analysis and Reporting Tool - An application for use by USG analysts performs a set of automated operations on real-time incoming biometric transaction events. This includes running searches and checks against law enforcement systems, as well as aggregating additional identifiers to biometrically linked data, and presents a person-centric view of a potential individual of interest. This process can trigger alerts or events to flag for additional investigation or notify relevant support entities of the event.

Compliance Assistance Reporting Terminal (CART) System – Our team supports ICE in automating the repeatable check-in process for subjects on the non-detained docket who are amendable to ERO reporting requirements through new development, deployment, and operations and maintenance of the CART System. CART is a custom hardware and software integrated solution and includes the kiosks, Portal, and Services to be used across all ERO offices that perform this duty. The solution includes a self-serve kiosk that includes a fingerprint scanner and camera to collect biometric information. The system performs back-end database queries, supports business logic, and includes an officer portal, which all integrate with internal and external systems to automate the check-in process.
Our team designed, developed, and deployed this solution under tight timeframes to successfully meet the congressionally mandated deadline. We manage all aspects of the CART Kiosk bundled hardware and software, and successfully tailored our solution to function on the ICE image and accommodate ICE security boundaries, controls, and agents.

2. Procedures for and results of data-driven and scientific validation of biometric technologies

In support of numerous biometric-based programs across the public sector listed in the above section, Dev Technology includes instrumentation for the collection of biometric quality metrics and telemetry. This data includes metrics such as:

- ✓ NIST Fingerprint Image Quality (NFIQ) versions 1 and 2
- ✓ Proprietary quality scores from biometric collection device hardware
- ✓ Biometric collection parameters and metadata such as location / site, capture method, biometric technology operator, or a user supporting a subject's biometric capture
- ✓ Physical environmental conditions

This data collected and provided is secured as Personal Identifiable Information (PII), using the same cryptographic protocols and procedures as the raw biometric data and in accordance with government and NIST-based Federal Information Processing Standards (FIPS).

Using this metadata, we routinely perform analysis both for self-directed as well as in conjunction with government biometric programs to identify anomalies or potential outliers that could contribute to poor biometric matching outcomes. This analysis is provided to the government for further study and correlation with resulting biometric matching outcomes, matching score analysis, and general recommendations or observations that require deeper

investigation. At DHS, we work with and support the Biometric Support Center (BSC) at the Office of Biometric Identity Management (OBIM). The BSC is tasked with providing expert human biometric examination support and in this capacity, they help to disambiguate low confidence automated biometric matches, allowing the automated matching systems to improve both the detection of low confidence matches, as well as shedding light on issues on the collection side.

A few examples of the results of the above analysis include:

- ✓ Identifying biometric operators that require better training on the capture process
- ✓ Biometric capture devices that may require maintenance
- ✓ Vendor product quality issues
- ✓ Physical conditions that can be improved to increase matching accuracies

Additionally, our biometric SMEs have worked with and support both collection and matching and provide unique and cross-program implementation expertise on designing, building, and improving biometric systems. One such effort included a matching accuracy and response time assessment of 8M anonymized biometric sets. Working with other biometric experts, statisticians, and the Government, this was performed in support of evaluating and properly vetting the introduction of new critical matching technologies at DHS.

Our biometric SMEs also participate in biometric improvements across the industry, supporting working groups at The Organization of Scientific Area Committees for Forensic Science (OSAC), as well as speaking at and contributing to biometric conferences.

We strongly believe that biometric technologies, when shown to be implemented properly by experienced industry practitioners that work closely with the public and private sector, have proven benefits and allow the transparency and confidence needed to continue to gain public trust.

3. Security considerations associated with a particular biometric technology

Dev Technology implements and supports systems and biometric capabilities, with the main vulnerability specific to the biometric domain being False Presentation Attacks (FPA). We mitigate this by using the following approaches:

- ✓ Where possible and the business allows, we rely on multiple biometric modalities. Requiring a bad actor to spoof multiple modalities significantly reduces the False Non-Match Rate (FNMR). Our core biometrics are fingerprint, face, and iris. We work closely with vendors and industry to design and implement systems that reduce capture times while preserving capture quality.
- ✓ For any unsupervised or unattended biometric capture systems, incorporating face matching with fingerprint allows using a high match confidence threshold for face with the fallback to fingerprint for insufficiently confident face matches. Additionally, we favor the utilization of NIST-compliant and FBI-validated fingerprint technologies that make use of capacitive and electrical conductivity-based capture sensors. These are more difficult to spoof, as they require presenting false biometrics that also must exhibit electrical characteristics that match human biology.

- ✓ We work with vendors in the industry to pilot and provide feedback to liveness detection and anti-spoofing features, to ensure that we are bringing the best system components and solutions to a system and offering.
- ✓ We recognize it's imperative to assess the risk of a false match vs. a false non-match and adjust thresholds to manage that risk. A system that identifies potential bad actors would have different confidence thresholds for a match than a system that allows physical or resource access based on biometrics. For almost every system, the severity of a mistake in the system is accounted for in the matching thresholds, ensuring that in the unlikely event of an incorrect biometric identification, the mistake is skewed toward the outcome with the least unfavorable consequences. For the 2 dichotomous scenarios, it is a requirement that a human review and act upon the decision that an individual may be a bad actor, and the cost of not identifying that potential individual is greater than the cost of additional investigation or deeper analysis to exonerate a subject from the mischaracterized claims of a biometric system. On the other hand, for a physical / resource access system, a high false match rate (FMR) would inadvertently allow access to a resource that should not have been granted. The thresholds should be skewed toward a higher FNMR with an alternative Multi-Factor enabled authentication capability.

4. Exhibited and potential harms of a particular biometric technology

With advancements in biometric technology and the ubiquity of devices and services that offer biometric capabilities, there is increased opportunity for misconfiguration and poor biometric design and implementation of systems. The previous sections highlight the experience and knowledge needed to build and implement a well-designed, secure, and impartial biometric system. Negativity bias is a well-researched and observed phenomena in human psychology with several National Institute of Mental Health (NIMH) and academic papers on the subject. As a result, the cost of poorly designed and implemented biometrics systems and solutions can exacerbate the existing stigmas against the use of biometrics—particularly in the areas of overuse, misuse, and invasion of privacy, which result in increased resistance to the many benefits that biometrics bring in the areas of automation and security. This outcome is increasingly likely as the barrier to entry for using biometric devices, technology, and capabilities is lowered, requiring a need to better vet biometric system integrators and developers of biometric solutions.

5. Exhibited and potential benefits of a particular biometric technology

A particular biometric that has benefited law enforcement is fingerprinting. Fingerprints are unique, and no two people have the same set. The use of Automated Fingerprint Identification Systems allows law enforcement agencies to quickly, within seconds, identify if a particular fingerprint has been collected previously and linked to a specific person. Fingerprints can be collected for various reasons to include prior arrests, applications for a specific job or benefit, credentialing, and facilitating legitimate travel and trade. Fingerprints also follow an Electronic Biometric Transmission Standards (EBTS) that are published by the National Institute of Standards (NIST), ensuring that an agency collects and records consistent data.

An example of an agency benefiting from fingerprints is the US Border Patrol (USBP). The USBP encounters tens of thousands of individuals crossing the United States border illegally each year. These individuals often travel without valid identification and establishing a person's

true identity may be difficult. Before fingerprints, individuals were encountered multiple times using different identifications and their immigration status could not be verified, resulting in the proper consequence not being applied. With the use of fingerprints, USBP can identify individuals that have been encountered previously, individuals that may be wanted by another law enforcement agency or be identified as a person of interest.

Due to the need for touchless biometric technology for reasons of avoiding transmissible viruses or other infectious diseases, today it is viable to use IRIS and FACE biometrics either individually or in combination to identify subjects. DHS-CBP is successfully using FACE recognition at the land border initiative as well as airports, especially with Global Entry. Other commercial entities such as CLEAR are using IRIS only for enrolled subjects to verify identity at all participating airport locations in the United States. DHS-OBIM has a large FACE and IRIS gallery and continues to build the gallery with the help of USBP and other systems deployed for biometric collections on the US Border. The usability, reliability, and accuracy has now been proven by Commercial and Government entities, so touchless biometric modalities such as FACE and IRIS are a sustainable option.

6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case

Dev Technology is not responding to this question.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Digital Therapeutics Alliance

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Via Email Submission: BiometricRFI@ostp.eop.gov

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Dear OSTP Team,

On behalf of the Digital Therapeutics Alliance (DTA), we are glad to submit this response related to the Office of Science and Technology Policy's Request for Information on biometric technologies.

Digital therapeutics (DTx) rely on a broad range of technologies to generate and deliver therapeutic interventions to patients; this includes the use and integration of biometric technologies and data. As DTx products continue to evolve – through novel therapeutic mechanisms of action, technical components, and treatment delivery methods – DTA remains focused on developing foundational principles and frameworks that underpin DTx product integrity and reliability.

To address OSTP's concerns about the use of biometric technologies in digital technologies – from questions about the validity of the underlying science, to differential effectiveness, outcomes, and harms for different demographic groups – DTA provides a brief overview of DTx industry efforts to develop core principles and standards that relate to product development, manufacturing, deployment, and support methods, with the primary aim of serving and protecting patients.

What is a DTx?

DTx products, a new category of medicine, deliver therapeutic interventions directly to patients using scientifically developed, clinically evaluated software to treat, manage, and prevent diseases and disorders. Digital therapeutics address a wide array of health conditions,[1] with products developed for ADHD, anxiety, asthma, cancer side effect management, diabetes, depression, insomnia, migraine, muscle/movement disorders, opioid and substance use disorders, and PTSD — to name a few. DTx products are used independently, alongside medications, and in tandem with clinician-delivered therapy.

Who is DTA?

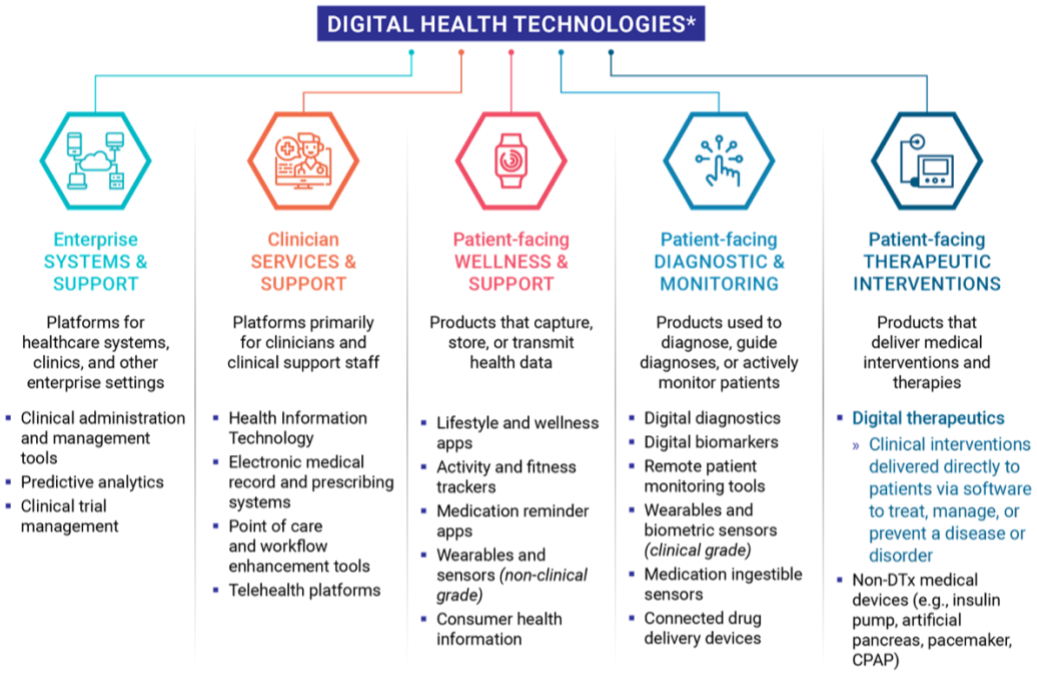
DTA's mission is to help patients, clinicians, payors, and policymakers understand how to identify, assess, and utilize DTx products in everyday settings. As such, DTA works with stakeholders across the healthcare ecosystem to ensure that DTx products are trustworthy and globally accessible care options. Members – including companies across nearly all major healthcare industries and geographic regions – are dedicated

[1] https://dtxalliance.org/wp-content/uploads/2020/03/DTx-Disease-State-Targets_03.20.pdf

to transforming global healthcare by advancing digital therapeutics to improve clinical and health economic outcomes.

DTx in the Digital Health Landscape

It is increasingly clear to healthcare decision makers that products across the digital health ecosystem serve different, but complementary purposes. Depending on a product's intended use and risk, it is subject to increasing degrees of clinical evaluation, regulatory oversight, and real-world data requirements.



Categorizations of the digital health technology ecosystem will continue to evolve. This is a select representation of a broad, diverse ecosystem.

Industry Principles

Considering DTx products' technical nature and direct engagement in patient care (including the generation and utilization of patient-generated data), DTx manufacturers have aligned on rigorous patient-centered core principles (*below*),[2] an industry code of ethics,[3] and product development best practices.[4] As part of their membership with DTA, DTx manufacturers attest to aligning with the following industry principles. Each DTx product must:

1. Prevent, manage, or treat a medical disorder or disease
2. Produce a medical intervention that is driven by software
3. Incorporate design, manufacture, and quality best practices
4. Engage end users in product development and usability processes
5. Incorporate patient privacy and security protections

[2] https://dtxalliance.org/wp-content/uploads/2019/11/DTA_DTx-Definition-and-Core-Principles.pdf
[3] https://dtxalliance.org/wp-content/uploads/2019/11/DTA_DTx-Industry-Code-of-Ethics_11.11.19.pdf
[4] https://dtxalliance.org/wp-content/uploads/2019/11/DTA_DTx-Product-Best-Practices_11.11.19.pdf

6. Apply product deployment, management, and maintenance best practices
7. Publish trial results inclusive of clinically meaningful outcomes in peer-reviewed journals
8. Be reviewed and cleared or certified by regulatory bodies as required to support product claims of risk, efficacy, and intended use
9. Make claims appropriate to clinical evaluation and regulatory status
10. Collect, analyze, and apply real world evidence and/or product performance data

International Efforts

Developed in 2019, DTA's list of Best Practices is currently undergoing review and update by an ISO committee that is focused on developing a DTx-focused Technical Report (TR). The International Organization for Standardization (ISO) is an independent, non-governmental international organization with a membership of 165 national standards bodies. Through its members, ISO brings together experts to develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

This DTx-specific TR will cement an internationally recognized definition of a digital therapeutic, in addition to addressing key standards that DTx products should incorporate to ensure data protection, algorithm integrity, technical rigor, appropriate clinical impact, etc.

This effort will likely build onto another ISO standard published in 2021: ISO/TS 82304-2:2021 *Health software — Part 2: Health and wellness apps — Quality and reliability*. This particular standard provides quality requirements for health apps and defines a health app quality label in order to visualize the quality and reliability of health apps. Covering the entire life cycle of a product, it is intended for use by app manufacturers as well as app assessment organizations in order to communicate the quality and reliability of a health app. Consumers, patients, carers, healthcare professionals and their organizations, health authorities, health insurers and the wider public can use the health app quality label and report when recommending or selecting a health app for use, or for adoption in care guidelines, care pathways and care contracts. Adding a DTx perspective will further improve on this standard.

DTx Industry Efforts

Lastly, DTA is currently working on a *DTx Value Assessment & Integration Guide*, which provides healthcare decision makers with a framework to evaluate the value of and enable the implementation of digital therapeutics in clinical practice. This Guide aims to provide consistent assessment criteria that enhance and refine DTx assessment processes within existing health systems, and includes product evaluation questions related to patient privacy, product security, data governance and storage, regulatory oversight, clinical validation, and real-world implementation.

Thank you for the opportunity to provide commentary on this process. We will be glad to share updates on our international and industry efforts as they further evolve and look forward to any further conversations with your team regarding this and other related efforts.

Sincerely,
Megan Coder, PharmD, MBA
Chief Policy Officer

[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Digital Welfare State & Human Rights Project and Center for Human Rights and Global Justice at New York University School of Law, and Temple University Institute for Law, Innovation & Technology

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Response to Request for Information (RFI)
FR Doc. 2021–21975

January 14, 2022

To the White House Office of Science and Technology Policy:

We are writing on behalf of the Digital Welfare State & Human Rights Project, Center for Human Rights and Global Justice (CHRGJ), NYU School of Law,[1] and the Institute for Law, Innovation & Technology (iLIT), Temple University, Beasley School of Law,[2] as well as a group of international legal experts and civil society representatives with extensive experience studying the impacts of biometric technologies.[3]

We welcome the focus on human and civil rights within the Bill of Rights for an AI-Powered World ("AI Bill of Rights") initiative and the focus on the *impacts* of biometric technologies.[4] Where industry has long pushed for *ethical* principles, this is an opportunity to protect rights through binding regulations, an essential step given the existential threats such technologies pose to human rights, democracy, and rule of law. OSTP should reflect on both the substance of rights and potential barriers for enforcement. This includes striving to distinguish—as many new technology developers fail to do—between the need for innovation, new laws and new rights, and the need to fix what is broken in existing laws, rules, policies, practices, and institutions.

This response provides international and comparative information to inform OSTP's understanding of the social, economic, and political impacts of biometric technologies,[5] in research and regulation. Biometrics fuel automation globally,[6] often at an accelerated, reckless pace, and these concerns transcend both political and geographic boundaries. Other powerful political actors—perceived as both peers and competitors—are attempting to understand and regulate in this area. This is an opportunity for the United States to be a world leader in ensuring that innovation is pursued in a way that safeguards human rights, both at home and abroad.

While we look forward to a consultative and transparent process for the AI Bill of Rights, we also note that the speed with which such technologies are being deployed requires urgent action. OSTP should work to establish immediate checks on the deployment of some of the most high-risk and contested tools, including an immediate moratorium on mandatory use in critical sectors such as health, education, and welfare, allowing time and space for democratic oversight before further intractable harms emerge. Our complete recommendations can be found in Section V.

I. The need for a comprehensive federal government response

There is already significant evidence that use of biometric identification in the United States can lead to harm, disproportionately impacting communities already discriminated against on the basis of, *inter alia*, race, sex, and national origin. For example, facial recognition technology disproportionately misidentifies

---

[1] The Digital Welfare State and Human Rights Project at the Center for Human Rights and Global Justice at NYU School of Law aims to investigate systems of social protection and assistance in countries worldwide that are increasingly driven by digital data and technologies. From NYU, Katelyn Cioffi [redacted], Victoria Adelmant ([redacted]), and Christiaan van Veen ([redacted]) contributed to this response.

[2] The Temple University Institute for Law, Innovation & Technology, pursues research, instruction, and advocacy with a mission to deliver equity and inform new approaches to innovation in the public interest. Contributors: Laura Bingham [redacted], Ed DeLuca [redacted], Sarbjot Kaur Dhillon [redacted] and Bianca Evans [redacted]

[3] This response benefited from invaluable input from a group of international experts with deep knowledge of the impact of AI and biometric identification technologies on human rights, including Gautam Bhatia, Yussuf Bashir (Haki na Sheria Initiative), Olga Cronin (Irish Council for Civil Liberties), Reetika Khera, Matthew McNaughton (Slashroots), Grace Mutung'u, Usha Ramanathan, and Anand Venkatanarayanan.

[4] Eric Lander & Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED, Aug. 10, 2021, https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.

[5] Rashida Richardson & Amba Kak, *Suspect Development Systems Databasing Marginality and Enforcing Discipline*, UNIV. MICH. J. L. REF., Vol. 55 (forthcoming), https://ssrn.com/abstract=3868392. (highlighting "counterproductive siloes between the Global South and Global North")

[6] *Id.*

people of color; use in law enforcement thus perpetuates racial bias, false arrests, and police brutality.[7] Moreover, the Department of Homeland Security's (DHS) transnational network of biometric records, tracking, and automated profiling consistently evades scrutiny, but shows evidence of arbitrary, discriminatory, and harmful practices.[8]

Despite evidence of the harms of biometric technologies, regulation is woefully lacking,[9] with the exception of some cities and states.[10] A significant part of the population is not covered by this patchwork of prohibitions,[11] and while litigation and local regulation provide some oversight, the federal government and its contractors are not held accountable even to these inadequate standards.[12] The absence of, for instance, guidance for development and use of AI by the federal government and its agencies, as well as common binding standards for private actors, risks perpetuating fragmented and insufficient rights protection. Further, the federal government has a vital role to play in regulating *all* biometric technologies, including those which have been in place for decades, such as fingerprint-scanning in the law enforcement and immigration contexts, as well as the extraterritorial application of technologies developed, produced, sold, and promoted by U.S. government agencies and corporations.

Two initial, fundamental concerns with a "Bill of Rights" approach must be highlighted, based on expert comparative legal analysis from several constitutional democracies. First, such an approach, if taken at face value as an effort to amend or modernize textually anchored rights, may exclude structural constitutional questions, such as separation of powers, the scope and quality of judicial review, and standing. Adoption of biometrics and predictive technologies increasingly concentrates power in executive agencies, inviting structural, slow-onset forms of injury.[13] Yet, unlike most constitutional systems, U.S. judicial review of administrative actions is structurally divorced from constitutional law and rights protection. Much relevant technology is predicated on "improving" or "modernizing" the administrative state, but "administrative law in the USA is not concerned primarily with basic rights."[14] Rights, however formulated, therefore risk being effectively unenforceable as executive discretion continues its extra-constitutional expansion.

Second, the absence of a cause of action for indirect discrimination ("disparate impact") that applies generally across different sectors and to state, local, and federal departments, as well as private actors, is concerning in this context. In contrast to proportionality tests applied in the majority of constitutional frameworks,[15] U.S. constitutional balancing tests are rigid and rules-driven, restricting serious scrutiny to the most obvious and intentional instances of racial discrimination.[16] Though disparate impact exists

[7] *See* Joy Adowaa Buolamwini, *Gender shades intersectional phenotypic and demographic evaluation of face datasets and gender classifiers*, 2017, https://dspace.mit.edu/handle/1721.1/114068; Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face recognition vendor test part 3 demographic effects,* NIST IR 8280, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[8] Ryan Calo & Danielle K. Citron, *The Automated Administrative State A Crisis of Legitimacy*, 70 EMORY L. J. 797, 830, 2021, https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj (finding that no-fly algorithms are unable to distinguish names, and that rules are not disclosed under executive and state secrets privileges); Sam Biddle & Maryam Saleh, *Little-Known Federal Software Can Trigger Revocation of Citizenship*, INTERCEPT, Aug. 25, 2021, https://theintercept.com/2021/08/25/atlas-citizenship-denaturalization-homeland-security/; Richardson & Kak, *supra* note 5.

[9] Todd Feathers, *Why It's So Hard to Regulate Algorithms*, MARKUP, Jan. 4, 2022, https://themarkup.org/news/2022/01/04/why-its-so-hard-to-regulate-algorithms.

[10] Facial recognition has been banned or restricted across many cities and several states: *see* Fight for the Future, *Map*, Ban Facial Recognition , https://www.banfacialrecognition.com/map/ (last visited Jan. 13, 2022). *See also* No Biometric Barriers to Housing Act of 2021, H.R. 4360, 117th Cong. (2021–22).

[11] Tom Simonite, *Face Recognition is Being Banned—But It's Still Everywhere*, WIRED, Dec. 22, 2021, https://www.wired.com/story/face-recognition-banned-but-everywhere/.

[12] Calo & Citron, *supra* note 8, at 815 (citing the APA's restrictions on challenging federal agency action).

[13] *See, e.g.*, *id.* at 845; Marielle Debos, *Biometrics and the Disciplining of Democracy Technology, Electoral Politics, and Liberal Interventionism in Chad*, DEMOCRATIZATION 1, Mar. 31, 2021, https://doi.org/10.1080/13510347 2021 1907349.

[14] Vicki C. Jackson & Mark Tushnet (eds.), PROPORTIONALITY: NEW FRONTIERS, NEW CHALLENGES 111, 2017. *See also* David Engstrom et al., *Government By Algorithm Artificial Intelligence in Federal Administrative Agencies*, 2020, https://www-cdn.law.stanford edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf (highlighting lack of public remedies under APA where a private right of action under federal discrimination statutes is "adequate").

[15] Jackson & Tushnet, *Id.*, at 111.

[16] *Id.*

as a theory of liability under some federal civil rights statutes,[17] even here the availability of disparate impact claims is at executive agencies' discretion in their enforcement of federal anti-discrimination laws.[18] In most other jurisdictions, and under international treaties like the Convention on the Elimination of All Forms of Racial Discrimination, ratified by the United States in 1994, the term "indirect discrimination" is used to denote liability for discrimination based on the *effect* of laws and practices.[19]

The limited availability and lax enforcement of disparate impact leaves the equal protection clause gutted and insufficient to deal with AI-enabled biometric discrimination.[20] Without providing for disparate impact claims, rights protections in the U.S. fall beneath international equality standards that the government has pledged to uphold and are not fit for purpose in an automated society which already exhibits structural bias and discrimination.

II. International evidence provides a critical resource

There is now a significant body of evidence that illuminates both the potential benefits and harms of biometric technologies in different contexts.[21] This response reflects input from leading experts who have worked in India, Jamaica, Kenya, and Ireland,[22] where governments, international organizations, and private actors have used a combination of biometrics, data sets, and machine learning to mediate access to fundamental rights.[23] With cities and states in the United States poised to follow suit,[24] this research provides an invaluable resource, allowing for proactive actions that anticipate and mitigate known harms.

Most critically, evidence now extends beyond frequently raised concerns about surveillance and privacy in the context of law enforcement and national security, to encompass concerns about social rights such as health, social security, education,[25] housing, and employment.[26] A recurring finding is that biometrics have potential to generate and exacerbate patterns of social exclusion, as well as direct and indirect discrimination. These technologies thus increasingly affect access, availability, affordability, and quality of fundamental public services.

A. How do AI and biometric technologies generate exclusion and discrimination?

[17] *See Texas Dep't of Hous. & Cmty. Affs. v. Inclusive Communities Project, Inc.*, 576 U.S. 519 (2015). *See* Cass R. Sunstein, *Algorithms, Correcting Biases*, 86 SOC. RES.: INT'L Q. 499, 510, 2019 (noting disparate impact liability presents some of the most important issues for challenging algorithmic discrimination in the future), http://eliassi.org/sunstein_2019_algs_correcting_biases.pdf.

[18] *See, e.g.*, *HUD's New Rule Paves the Way for Rampant Algorithmic Discrimination in Housing Decisions*, NEW AM., Oct. 1, 2020, http://newamerica.org/oti/blog/huds-new-rule-paves-the-way-for-rampant-algorithmic-discrimination-in-housing-decisions. On disparate impact generally, see *Tex. Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc.*, 576 U.S. 519 (2015). *See also Griggs v. Duke Power Co.*, 401 U.S. 424 (1971).

[19] *See* Audrey Daniel, *The Intent Doctrine and CERD How the United States Fails to Meet Its International Obligations in Racial Discrimination Jurisprudence*, 4 DEPAUL J. SOC. JUST. 263, 2011, https://via.library.depaul.edu/jsj/vol4/iss2/3. *See also* EU Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, 2000 O.J. (L 180) 22 (requiring EU Member States to prohibit direct and indirect discrimination on the basis of racial or ethnic origin); *D.H. and Others v. the Czech Republic*, App. No. 57325/00, 47 EUR. H.R. REP. 3, 2008.

[20] *See, e.g.*, Mark MacCarthy, *Fairness in algorithmic decision-making*, BROOKINGS, 2019, https://www.brookings edu/research/fairness-in-algorithmic-decision-making/.

[21] A 2013 survey found at least 230 instances of developmental programs using biometric identification tech. *See* Alan Gelb & Julia Clark, *Identification for Development The Biometrics Revolution*, SSRN J., 2013, http://www.ssrn.com/abstract=2226594.

[22] *See supra* note 3.

[23] Biometrics must be evaluated in conjunction with related algorithms, data sets, and institutional arrangements, sometimes called the 'biometric assemblage'. *See* Mirca Madianou, *The Biometric Assemblage Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies*, 20 TELEVISION & NEW MEDIA 581–599, 2019, https://doi.org/10.1177/1527476419857682.

[24] *See generally*, Mizue Aizeki & Rashida Richardson, eds., *Smart-City Digital ID Projects Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"*, Dec. 2021, https://www.immigrantdefenseproject.org/wp-content/uploads/smart-city-digital-id-products.pdf.

[25] Sally Weale, *ICO to Step in After Schools use Facial Recognition to Speed up Lunch Queue*, GUARDIAN, Oct. 18, 2021, https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk.

[26] *See, e.g.*, Center for Human Rights and Global Justice [CHRGJ] et al., *Chased Away and Left to Die How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,* 2021, https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf; Karthik Muralidharan et al., *Identity Verification Standards in Welfare Programs Experimental Evidence from India,* NBER WORKING PAPER SERIES 26744, 2020, http://www.nber.org/papers/w26744.pdf.; Jean Drèze, *There is an urgent need for safeguards against unfair discontinuation of social benefits*, INDIAN EXPRESS, Apr. 20, 2021, https://indianexpress.com/article/opinion/columns/aadhaar-linking-public-welfare-schemes-pds-system-7280621/; Reetika Khera, ed., *Dissent on Aadhaar Big Data Meets Big Brother,* 2018.

Exclusion can be caused by innate problems with biometric technology. While much recent critique has focused on facial recognition and mass surveillance, the difficulties of mitigating the harmful effects of "lower-tech" solutions[27] such as fingerprinting, should be both a warning and opportunity for learning as "novel," more advanced technologies emerge. As with most biometrics, specific notions of "normality" are built into fingerprinting systems; "hand scanners have particular sizes and shapes, with designated places to put the fingers," and anyone falling outside of this "norm" will struggle to authenticate.[28] Failure rates are significantly higher among people of color as systems are "infrastructurally calibrated to whiteness."[29] Further, as biometric systems are probabilistic and are often designed to tolerate significant exclusion errors, relying on them to definitively identify or verify will inevitably lead to exclusion.[30]

Moreover, while laboratory-based testing of biometric technologies might show relatively high success rates, as was shown in a challenge to a nationwide digital ID system reliant on fingerprint authentication in Kenya, "the real-world data is very different."[31] Environmental conditions, including humidity, temperature, and light exposure, impact the quality of biometric data capture.[32] Biometrics are not immutable, as they can alter over time and degrade with age. Capture and authentication often depend on fragile, expensive hardware, as well as quality internet and electricity. Thus, digital divides—which map onto other disadvantages—can be exacerbated through AI-enabled biometrics.[33]

Consequently, when biometrics are yoked to essential services such as social security or health care, marginalization and exclusion may arise. This in turn results in decreased access to numerous fundamental entitlements, damaging physical and mental health, and impacting dignity. This has been extensively documented in India, home to the world's largest biometric identification system, Aadhaar.[34] Persistent failures to authenticate fingerprints through Aadhaar at the point of service for welfare programs, including food rations depended on by four-fifths of Indian families, has resulted in numerous deaths by starvation, families cut off from rations for weeks, and a system that increasingly punishes the poor.[35] In Uganda, card readers were unable to read older persons' fingerprints or match their biometric profile to an accurate birth date in the national ID database. Although eligible to access certain social protection programs, such as cash transfers, older persons were consistently denied access to life-saving grants because of their inability to identify and authenticate biometrically.[36]

Even where such technologies operate as intended, their use can facilitate other forms of indirect discrimination. They can sit atop existing barriers, while introducing further requirements, and access

[27] Shoshana Amielle Magnet, *Criminalizing Poverty Adding Biometrics to Welfare*, WHEN BIOMETRICS FAIL: GENDER, RACE, AND THE TECHNOLOGY OF IDENTITY 23, 2011.
[28] Sanneke Kloppenburg & Irma van der Ploeg, *Securing Identities Biometric Technologies and the Enactment of Human Bodily Difference*, 29(1) SCI. AS CULTURE 57, 62, 2020, https://www.tandfonline.com/doi/full/10.1080/09505431.2018.1519534.
[29] *See* Shoshana Magnet, *When Biometrics Fail Gender, Race, and the Technology of Identity*, 2011, at 49, https://www.dukeupress.edu/when-biometrics-fail; Simone Brown, *Dark Matter On the Surveillance of Blackness*, 2015, https://read.dukeupress.edu/books/book/147/Dark-MattersOn-the-Surveillance-of-Blackness; Grother et. al, *supra* note 7.
[30] Jeremy Wickins, *The Ethics of Biometrics the Risk of Social Exclusion from the Widespread use of Electronic Identification*, 13 SCI & ENGINEERING ETHICS 45–54, 2007, http://link.springer.com/10.1007/s11948-007-9003-z.
[31] Nubian Rights Forum & 2 others v. Attorney General & 6 others, 2020, eKLR 37 [Kenya], at para. 37, http://kenyalaw.org/caselaw/cases/view/189189/.
[32] *See e.g.*, UNITED KINGDOM GOVERNMENT OFFICE FOR SCIENCE, BIOMETRICS: A GUIDE, June 15, 2018: https://www.gov.uk/government/publications/biometrics-a-guide; Ann Livingston et al., *Upholding the Rights of Children Special Considerations on the Use of Biometrics in Identity Systems*, 2019, https://www id4africa.com/2019/almanac/UNICEF-Ann-Livingston-Kristen-Wenz-Nicola-Richards.pdf.
[33] Silvia Masiero, *Biometric Infrastructures and the Indian Public Distribution System*, S. ASIA MULTIDISCIPLINARY ACAD. J. 11 (2020), https://journals.openedition.org/samaj/6459.This remains a significant issue in the United States, see Emily A. Vogels, *Digital Divide Persists Even As Americans With Lower Incomes Make Gains In Tech Adoption*, 2021, https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/.
[34] Over 1.2 billion people have enrolled in the Aadhaar system. Swetha Totapelly et al., *State of Aadhaar Report*, 2019, https://stateofaadhaar.in/download-reports.php.
[35] *See, e.g.*, Reetika Khera, *These digital IDs have cost people their privacy — and their lives*, WASH. POST, Aug. 9, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/, last visited Jan. 14, 2022; *India's High-Tech Governance Risks Leaving Behind its Poorest Citizens*, ECONOMIST, Oct. 16 2021, https://www.economist.com/asia/2021/10/16/indias-high-tech-governance-risks-leaving-behind-its-poorest-citizens; Ursula Rao, *Biometric Bodies, Or How to Make Electronic Fingerprinting Work in India*, 24 BODY & SOC. 68–94, 2018, https://doi.org/10.1177/1357034X18780983.
[36] CHRGJ et al., *supra* note 26, at 31–33.

becomes contingent on digital literacy, specific forms of personal identification,[37] reliable access to basic ICT services, or fees related to travel, administration, and lost time spent navigating the system. For instance, in India, the use of Aadhaar in public services requires networks of data operators who continuously collect and verify biometric data. Without oversight, such operators become bureaucratic bottlenecks, sites of harassment and intimidation, and an insurmountable barrier to accessing services.[38]

B. Civil death and other cumulative, systemic impacts of biometric systems

Taken individually, instances of exclusion may already constitute indirect discrimination. But the persistence of biometric information also means that the effects of exclusion replicate quickly, locking individuals out of multiple services. In Kenya, the United Nations High Commissioner for Refugees (UNHCR) collected biometric information to distribute food aid during a period of famine. Consequently, many Kenyans who were registered as children are victims of 'double registration': since their biometric data appears in a refugee database, the government denies them national ID cards, restricting access to services including employment, health care, and social security.[39] In Ireland, the Public Services Card (PSC), which includes collection of biometric data, rapidly expanded beyond its original role in the welfare system, with other government agencies requiring it as the sole form of ID.[40] This expansion was introduced without transparency, democratic debate, or adequate review of its necessity and proportionality. The use of biometrics can therefore quickly become *de facto* mandatory, even when not formally required.

Any failure to authenticate or ensure that data is consistent across different systems can therefore lead to "civil death,"[41] where an individual is cut off from *all* fundamental services. This is the case in Pakistan, where the government has unilaterally blocked certain individuals' biometric digital IDs, forcing them into a vetting process to 'prove' aspects of their identity such as citizenship or gender.[42] In Assam, India, the government recently conducted a mass citizenship verification process,[43] placing approximately 2.7 million people on a 'doubtful list' of those whose citizenship is called into question. Many on this list have had their biometric profiles frozen; this means that they cannot use their Aadhaar record to receive health care, access food rations, get a drivers' license, or register a SIM card.[44]

This civil death phenomenon is especially concerning since use of biometric technologies can coincide with entrenchment of structural racism and discrimination. While the broad use of these technologies in public service delivery will ultimately affect everyone, at present harms disproportionately impact already marginalized communities; across many biometric systems, those unable to identify and verify are often those in poor, rural communities, ethnic and religious minorities, women, and older persons.[45] Widespread deployment may thus exacerbate and deepen structural and institutional patterns of harm.[46]

[37] *See* Vivek Maru et al., *Digital IDs Make Systemic Bias Worse*, WIRED, Feb. 5, 2020, https://www.wired.com/story/opinion-digital-ids-make-systemic-bias-worse/.
[38] Vyom Anil & Jean Drèze, *Without Aadhaar, Without Identity*, INDIAN EXPRESS, July 5, 2021, https://indianexpress.com/article/opinion/columns/flaw-in-aadhaar-architecture-uidai-card-enrolment-7389133/.
[39] Haki na Sheria Initiative, *Biometric Purgatory How the Double Registration of Vulnerable Kenyan Citizens in the UNHCR Database Left Them at Risk of Statelessness*, 2021, http://citizenshiprightsafrica.org/wp-content/uploads/2021/11/Haki-na-Sheria_Double-Registration_Nov2021.pdf.
[40] *DPC welcomes resolution of proceedings relating to the Public Services Card*, Dec. 10, 2021, https://www.dataprotection.ie/news-media/latest-news/dpc-welcomes-resolution-proceedings-relating-public-services-card.
[41] Usha Ramanathan, *Aadhaar is Like Drone Warfare Versus Hand to Hand Combat, Profiling Becomes All That More Easier*, BUSINESS STANDARD, Apr. 1, 2016, https://www.business-standard.com/article/economy-policy/aadhaar-is-like-drone-warfare-versus-hand-to-hand-combat-profiling-becomes-all-that-more-eaiser-usha-ramanathan-116033101394_1.html.
[42] Alizeh Kohari, *Life in Pakistan without a digital ID*, CODA STORY, Nov. 3, 2021, https://www codastory.com/authoritarian-tech/pakistan-biometrics-stateless/.
[43] Siddhartha Deb, *They Are Manufacturing Foreigners' How India Disenfranchises Muslims*, N.Y. TIMES, Sept. 15, 2021, https://www nytimes.com/2021/09/15/magazine/india-assam-muslims.html.
[44] *Two Years Since NRC, Lakhs Still Remain in Limbo*, HINDU, Aug. 31, 2021, https://www.thehindu.com/news/national/two-years-since-nrc-lakhs-still-remain-in-limbo/article36201266.ece.
[45] Totapelly et al., *supra* note 34.
[46] Virginia Eubanks, *Automating Inequality*, 9, 2018.

Beyond exclusion, the extensive use of biometrics can also fundamentally affect democracy, the rule of law, accountability and transparency,[47] while entrenching private sector control over public functions.[48] After alleged election rigging in the 2017 Kenyan presidential election, government officials were unable to comply with judicial orders to grant access to election results data tied to a biometric voter registration system, as the vendor's servers were in France.[49] In South Africa, the introduction of biometric technologies into welfare payment systems resulted in one company's disastrous monopoly while weakening the government's power to maintain any control over the welfare system.[50] Use of biometrics can thus augment powerful market-based interests that do not reflect human rights and democratic principles.[51]

III. Comparative efforts to mitigate the exclusionary impact of biometric identification

While a data protection and privacy framework should be seen as a necessary condition to safeguard human rights in the context of biometrics, such measures are not sufficient to combat broader effects. Regulatory efforts that fail to include specific remedies for exclusion nor accessible accountability mechanisms render it extremely difficult to safeguard rights. For instance, India's Aadhaar Act stipulates that children shall not be denied access to any subsidy, benefit, or service as a result of failed biometric authentication, but does not provide any specific cause of action or remedy.[52] Most efforts to regulate the use of biometrics—and AI more broadly—have also failed to adequately engage affected communities in a meaningful, continuous way.[53] In Ireland, this was a core complaint about the expansion of the PSC's scope.

Blocked by the lack of remedies, civil society organizations have resorted to litigation to challenge biometric identification systems. A series of such court cases highlights impacts on equality, dignity, autonomy, health, and social security, and demonstrates some ways in which legal frameworks and norms can be applied to biometric technologies.[54] However, litigation is not an ideal mechanism, and challenges within litigation reflect broader difficulties regulating AI.[55] For instance, biometric identification projects often involve proprietary technology and are implemented quickly and with little transparency; litigants therefore face significant barriers to accessing information necessary to challenge these systems. Judicial timelines also mean that harms may continue, and often replicate and deepen, while awaiting review.

Pushback from civil society and affected communities has also demonstrated the limitations of a purely individual rights framework that does not sufficiently recognize disparate impact; many of the impacts of biometric technology are structural, dispersed, and affect groups collectively. For instance, the legal challenge to the national ID system in Kenya required individual plaintiffs to show that they, as a member of a particular *group*, had been directly disadvantaged through the disparate impacts of biometric

[47] *See* Séverine Awenengo Dalberto & Richard Banégas (eds.), *Identification and Citizenship in Africa Biometrics, the Documentary State and Bureaucratic Writings of the Self*, https://www.taylorfrancis com/books/9781000380033.
[48] *See generally* Linnet Taylor, *Public Actors Without Public Values Legitimacy, Domination and the Regulation of the Technology Sector*, PHIL. & TECH. (2021), https://doi.org/10.1007/s13347-020-00441-4; Julie Cohen, *Between Truth and Power The Legal Constructions of Informational Capitalism*, 2019.
[49] Ken Flottman, *Kenya's IEBC announced 18 months ago that it would finally open its vote tally servers to public, but has failed to do so*, AFRICOMMONS, Aug. 29, 2020, https://africommons.com/tag/france/; Duncan Miriri, *Kenyan opposition leader targets Safaricom staff over election*, REUTERS, Sept. 27, 2017, https://www.reuters.com/article/kenya-election-safaricom-idUSL8N1M81HK; Dalberto & Banegas (eds.), *supra* note 52.
[50] *See e.g.*, Keith Breckenridge, *The Global Ambitions of the Biometric Anti-Bank Net1, Lockin and the Technologies of African Financialisation*, 33 INT'L REV. OF APP. ECON. 93–118, 2019, https://wiser.wits.ac.za/content/global-ambitions-biometric-anti-bank-net1-lockin-and-technologies-african-financialization; Robyn Foley & Mark Swilling, *How One Word Can Change the Game Case Study of State Capture and the South African Social Security Agency, Stellenbosch State Capacity Research Project*, 2018, https://www0.sun.ac.za/cst/publication/how-one-word-can-change-the-game-a-case-study-of-state-capture-and-the-south-african-social-security-agency-sassa/;
[51] Amba Kak, ed., *Regulating Biometrics Global Approaches and Urgent Questions*, 2020, https://ainowinstitute.org/regulatingbiometrics.html.
[52] *Id.*
[53] Christopher Wilson, *Public Engagement and AI A Values Analysis of National Strategies*, GOV'T INFO. Q. 101652, 2021, https://linkinghub.elsevier.com/retrieve/pii/S0740624X21000885.
[54] *See* Nubian Rights Forum, *supra* note 31; *Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors. Writ Petition (Civil) No. 494 of 2012 and Connected Matters* [India] (26 September 2018); Press Release: Civil Society Drags Government to Court Over Requirement to Have National ID Card Before Receiving Covid-19 Vaccine (2021), https://iser-uganda.org/images/downloads/COVID19_vaccine_and_IDs-ISER_Press_Briefing.pdf
[55] *See, e.g.*, Reetika Khera, "The poor are left to themselves," THE HINDU, Sept. 28, 2018, https://www.thehindu.com/opinion/lead/the-poor-are-left-to-themselves/article25074493.ece, last visited Jan. 14, 2022.

technologies.[56] Similar issues have emerged in the United States,[57] where victims of biased surveillance systems are left without constitutional protections.[58] Thus, it is crucial to establish definitions of group harms and indirect discrimination, as well as evidentiary standards for demonstrating disparate impact.

Each application of biometric technology deserves its own legal assessment of harm, as well as of its legitimacy, necessity, and proportionality. However, some have concluded that, on the evidence, such technologies pose such serious risks to human rights and democracy that the potential benefits are outweighed, necessitating a ban on the sale and use of these technologies.[59] Any steps taken by the U.S. government should seriously consider the gravity of these concerns.

IV. An international and comparative perspective is also necessary to reflect the global environment in which such technologies are being developed, used, and regulated

The United States plays a major role in the development and uptake of biometric technologies globally, through foreign investment, foreign policy, and development aid, as well as the activities of U.S. companies. The U.S. government has participated in *mandating* creation of biometric identification systems, such as through UN Security Council Resolution 2396, requiring states to "implement systems to collect biometric data" in order to "properly identify terrorists."[60] USAID provides active support for foreign governments' collection of biometric data, while the World Bank finances the development of biometric systems in dozens of countries.[61] U.S. government actors and companies influence critical decisions in standard setting bodies about specifications for biometric data collection devices and biometric data analysis.[62] Further, the Taliban's seizure of U.S. military biometric devices and data in Afghanistan demonstrates the immense ramifications of U.S. actions abroad.[63] The widespread use of biometric recognition at entry points at the Mexico border[64] further influences other governments around the world to follow suit.[65]

Meanwhile, the United States is one of the largest exporters of biometric surveillance technologies.[66] U.S. company L1 Identity Solutions was instrumental in the introduction of India's Aadhaar system, for

[56] Amnesty International, *Ban the Scan NYC*, https://banthescan.amnesty.org/nyc/, last visited Jan 13, 2022. *See also* Section II.
[57] Mutale Nkonde, *Automated Anti-Blackness Facial Recognition in Brooklyn, New York*, HARV. KENNEDY SCH. J. AFR. AMER. POL., 2019–20. https://pacscenter.stanford.edu/wp-content/uploads/2020/12/mutalenkonde.pdf; Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES, Sept. 24, 2019, https://www nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html.
[58] *United States v. Tuggle*, 4 F. 4th 505, 513 (7th Cir. 2021).
[59] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, Sept. 13, 2021, A/HRC/48/31, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.doc; *Amnesty International and more than 170 organisations call for a ban on biometric surveillance*, June 7, 2021, https://www.amnesty.org/en/latest/news/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.
[60] United Nations Security Council (UNSC) Res. 2396, Dec. 21, 2017, UN Doc S/RES/2396, https://undocs.org/S/RES/2396(2017). *See also* Krisztina Huszti-Orbán & Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists Best Practice or Risky Business?* 2020, https://law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf.
[61] US Agency for International Development (USAID), *Introducing Biometric Data at Refugee Settlements in Uganda*, 2019, https://www.usaid.gov/news-information/videos/introducing-biometric-data-refugee-settlements-uganda; USAID, *Good Governance & Public Administration Strengthening Project (GGPAS)*, 2021, https://www.usaid.gov/kyrgyz-republic/fact-sheets/good-governance-public-administration-strengthening-project-ggpas; *USAID pilots biometrics to track youth health in Kenya*, Identity Week 2015, https://identityweek.net/usaid-pilots-biometrics-to-track-youth-health-in-kenya/.
[62] Joseph N. Pato and Lynette I. Millett, *The Biometrics Standards Landscape*, (National Research Council (US) Whither Biometrics Committee, 2010, https://www ncbi.nlm.nih.gov/books/NBK219888/.
[63] Ken Klippenstein & Sara Sirota, *The Taliban Have Seized U.S. Military Biometrics Devices*, INTERCEPT, Aug. 18, 2021, https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/; Eileen Guo & Hikmat Noori, *This is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban*, MIT TECHNOLOGY REVIEW, Aug. 30, 2021, https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/; Verónica Arroyo & Donna Wentworth, *We Need to Talk About Digital ID Why the World Bank Must Recognize the Harm in Afghanistan and Beyond,* ACCESS NOW, Oct. 14, 2021, https://www.accessnow.org/digital-id-world-bank/.
[64] *See, e.g.*, UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial and Xenophobic Discrimination, Emerging Digital Technologies, and Border and Immigration Enforcement*, 2020, UN Doc A/75/590, para. 47, https://antiracismsr.org/wp-content/uploads/2020/11/A_75_590_Advance-Unedited-Version.pdf. Immigrant Defense Project et al., *Factsheet Freeze Expansion of the Hart Defense*, Apr. 2021, https://justfutureslaw.org/wp-content/uploads/2021/04/HART-Appropriations-2022.pdf; Todd Miller, *More than a Wall*, 2, 2019, https://www.tni.org/files/publication-downloads/more-than-a-wall-report.pdf.
[65] Petra Molnar, *Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up*, 2020.
[66] Steve Feldstein, *The Global Expansion of AI Surveillance*, 2019, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf; Valentin Weber and Vasilis Ververis, *China's Surveillance State A Global Project*, 2021, https://www.nspirement com/2021/09/01/chinas-digital-surveillance.html; Liza Lin & Josh Chin, *U.S. Tech Companies Prop Up China's Vast Surveillance Network*, WALL ST. J., Nov. 26, 2019, https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846;

example;[67] and U.S. companies such as Apple have also normalized the everyday use of biometric authentication.[68] These companies have been largely unfettered by legal or regulatory constraints in their experimentation with biometrics.[69] In large part, such initiatives have been paused only after public backlash and coordinated advocacy have forced companies to change course.[70] Meta's recent decision to shut down its facial recognition system and delete facial templates was explicitly driven by "societal concerns,"[71] but this came after Meta had been unconstrained in creating a database of over one billion faces; the company retains its DeepFace software and can resume use at any point.[72] Further, existing models of self-regulation are insufficient and do not provide meaningful constraints on the development and deployment of biometric technologies.[73]

Reticence in constraining U.S. technology companies' advancements has been driven by a dominant narrative of an "AI arms race" with China.[74] The National Security Commission on Artificial Intelligence (NSCAI) notes that China is setting a "chilling precedent."[75] Indeed, shocking reports detail the Chinese State's use of biometrics to facilitate surveillance and persecution of Uyghurs in Xinjiang.[76]

Yet U.S. government officials lament that technology companies in China can develop AI aided by unconstrained biometric data collection, claiming it is "not a level playing field."[77] This furthers the idea that "global AI leadership" requires low regulation, private sector access to troves of personal data, and expansive security use.[78] The NSCAI urges that the United States "must win the AI competition"[79] and identifies, somewhat uncritically, "surveillance," "clearing of regulatory barriers," and "enormous government stores of data" as factors enabling China "to leap ahead."[80] Viewing the development of AI-enabled biometric technologies through this competitive, national security paradigm risks that law, regulation, and human rights are sacrificed in efforts to "win."[81] The U.S. government must not allow a perceived AI arms race to dictate its approach to regulating biometric technologies.

Further, an arms race narrative simplifies complex realities around regulation in China itself.[82] Growing public controversy around facial recognition, combined with tensions with Chinese Big Tech companies, have led the Chinese government to introduce regulations, including regarding the use of biometric

[67] Unique Identification Authority of India, *Device Drivers,* https://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189
[68] *Face Biometrics Month The Apple Effect and the Mainstreaming of Face Authentication*, FindBiometrics, 2019, https://findbiometrics.com/face-biometrics-month-the-mainstreaming-of-face-authentication-611140/.
[69] Kate Crawford et al., *AI Now 2019 Report*, 2019, https://ainowinstitute.org/AI_Now_2019_Report.html.
[70] *See* Rebecca Heilweil, *Big tech companies back away from selling facial recognition to police. That's progress.*, VOX, June 10, 2020, https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police.
[71] Jerome Pesenti, *An Update On Our Use of Face Recognition*, META, Nov. 2021, https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/.
[72] Rebecca Heilweil, *Facebook is backing away from facial recognition. Meta isn't*. Vox, Nov. 3, 2021, https://www.vox.com/recode/22761598/facebook-facial-recognition-meta.
[73] *See* Ben Wagner, *Ethics As An Escape From Regulation From "Ethics-Washing" To Ethics-Stopping*? in Emre Bayamlioğlu et al. (eds.), *Being Profiled Cogitas Ergo Sum 10 years of Profiling the European Citizen*, 2018, https://www.cohubicol.com/assets/uploads/being-profiled-cogitas-ergo-sum.pdf.
[74] *See* Crawford et al., *supra* note 69; Daniel F. Runde, Romina Bandura, & Sundar Ramanujam, *The United States Has an Opportunity to Lead in Digital Development*, 2021, https://www.csis.org/analysis/united-states-has-opportunity-lead-digital-development; Amanda Macias & Kayla Tausche, *U.S. Needs to Work with Europe to Slow China's Innovation rate, Raimondo says*, CNBC, Sept. 28, 2021, https://www.cnbc.com/2021/09/28/us-needs-to-work-with-europe-to-slow-chinas-innovation-rate-raimondo-says.html.
[75] National Security Commission on Artificial Intelligence [NSCAI], *Final Report*, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.
[76] *See* Maya Wang, *The Robots Are Watching Us, Human Rights Watch*, 2020, https://www.hrw.org/news/2020/04/06/robots-are-watching-us; Olivia Shen, *AI Dreams and Authoritarian Nightmares*, in Jane Golley et al. (eds.), *China Story Yearbook China Dreams*, 2020.
[77] *See* Macias & Tausche, *supra* note 74 .
[78] Crawford et al., *supra* note 69.
[79] NSCAI, *supra* note 75.
[80] National Security Commission on Artificial Intelligence [NSCAI], *Chinese Tech Landscape Overview NSCAI Presentation*, May 2019, https://epic.org/wp-content/uploads/foia/epic-v-ai-commission/EPIC-19-09-11-NSCAI-FOIA-20200331-3rd-Production-pt9.pdf. *See also* Ryan Fedasiuk, *Chinese Perspectives on AI and Future Military Capabilities*, (Center for Security and Emerging Technology, 2020).
[81] Crawford et al., *supra* note 69; Kelsey Piper, *Why an AI Arms Race with China Would be Bad for Humanity*, VOX, Aug. 10, 2019, https://www.vox.com/future-perfect/2019/8/10/20757495/peter-thiel-ai-arms-race-china.
[82] Maya Wang, *China's Techno-Authoritarianism Has Gone Global*, FOREIGN AFFAIRS, Apr. 8 2021, https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global.

technologies.[83] The Supreme People's Court of China has issued regulations requiring companies to obtain consent before collecting and processing facial biometric data.[84] China's recent Personal Information Protection Law mandates data minimization and user consent across the private sector when processing "sensitive personal information" including biometric data. China appears to be taking seriously the need to regulate biometric technologies.

Meanwhile, the European Union (EU) is claiming a leadership role in regulating biometric technologies and protecting human rights. For instance, the EU seeks to prohibit outright some uses of mass biometric surveillance by law enforcement.[85]

The United States should view such attempts not as a ceiling, but rather a challenge to set standards even higher. Indeed, the EU's proposed AI Act has been critiqued for its overly-broad exceptions; unnecessarily restricting prohibition of remote biometric identification to law enforcement; and applying prohibitions only to "real-time" uses rather than continuing or post-hoc uses.[86] Further, the EU's proposed Act gives providers significant discretion to assess the risks of their own technologies;[87] it also fails to confer individual rights to those impacted by AI systems, or to provide for effective remedies where harms occur.[88] We encourage OSTP to look to these parallel efforts and strive to go further still.

The U.S. government must also take account of the far-reaching impacts that its decisions and regulation of U.S. companies already have worldwide: the extraterritorial application of technologies developed, produced, sold, and promoted by U.S. government agencies and U.S. corporations must come into the remit of the AI Bill of Rights.

V. Recommendations

The outcome of this RFI and the AI Bill of Rights should be a comprehensive governance framework, including relevant laws, policies, and plans for implementation, which emphasizes human rights, regulatory oversight, and effective enforcement. In order to achieve this, OSTP should therefore work towards the following recommendations:

1. **Impose an immediate moratorium for critical sectors**: Define, classify, and enact a moratorium on the use of mandatory AI-enabled biometric identification technology.[89] Such identification systems should never be mandatory in critical sectors such as education, welfare benefits programs, and health care, so as to preserve access to fundamental services.
2. **Invoke legal action to address the indirect and disparate impact of biometrics**: Propose and enact legislation that unequivocally applies the disparate impact doctrine, at a minimum in federal equal protection claims regarding the design and use of AI-enabled biometric identification technologies,

[83] *China Rebukes 43 Apps including Tencent's WeChat for Breaking Data Transfer Rules*, REUTERS, Aug. 18, 2021, https://www reuters.com/business/retail-consumer/china-ministry-targets-43-apps-including-tencents-wechat-2021-08-18/; Josh Horwitz, *China Steps up Tech Scrutiny with Rules over Unfair Competition, Critical Data*, REUTERS, Aug. 17, 2021, https://www.reuters.com/business/media-telecom/china-issues-draft-rules-banning-unfair-competition-internet-sector-2021-08-17

[84] Supreme People's Court of China, Provisions on Relevant Issues on the Application of Laws in Hearing Civil Cases Related to the Application of Facial Recognition Technology in Processing Personal Information, July 28, 2021. *See also* Ananaya Agrawal, *China Supreme Court Issues Regulations Against Misuse of Facial Recognition Technology*, JURIST, Aug. 2021, https://www.jurist.org/news/2021/08/china-supreme-court-issues-regulations-against-misuse-of-facial-recognition-technology/.

[85] EU Member States are also taking steps to curb biometric technologies. *See* Koalitionsvertrag Zwischen SPD, Bündnis 90/Die Grüne, und FDP, Mehr Fortschritt Wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 2021, https://cms.gruene.de/uploads/documents/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf.

[86] *See An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement*, Nov. 30, 2021, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf [Hereinafter EU Civil Society Statement]; Nathalie A. Smuha et al., *How the EU Can Achieve Legally Trustworthy AI A Response to the European Commission's Proposal for an Artificial Intelligence Act* (2021), https://papers.ssrn.com/abstract=3899991; Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act.* 22 COMP. L. REV. INT., 2021, 97, https://ssrn.com/abstract=3896852.

[87] Smuha et al., *Id*.

[88] *See* EU Civil Society Statement, *supra* note 86*;* Smuha et al., *supra* note 86.

[89] Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong , 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2052?q=%7B%22search%22%3A%5B%22Facial+Recognition+and+Biometric+Technology+Moratorium+Act+of+2021%22%5D%7D&s=1&r=1.

encompassing their implementation in administering access to public and private services. Such legislation should be designated implementing legislation in line with the ratification of the CERD, affording a private right of action for racially discriminatory effects of the deployment of AI-enabled technologies.

3. **Engage in further review of the human rights impact of biometrics and the components of different legal and regulatory approaches. This should include, *inter alia*:**
    a. Conduct and make public a comprehensive mapping of all federal systems currently or prospectively using biometric identification, including (1) the kinds of information collected, (2) the legal authority for collection and retention, (3) the purposes for which information is used, (4) how the information flows within public agencies, and (5) the impact of collection, retention, and sharing on rights.
    b. Conduct a comprehensive analysis of other countries' and regional bodies' efforts to develop binding legal frameworks to regulate AI-enabled biometric technologies. Distilling key lessons, the U.S. government should go beyond minimal standards to progress the field towards greater recognition and protection of human rights.

4. **Build a comprehensive legal and regulatory approach that addresses the complex, systemic concerns raised by AI-enabled biometric identification technologies, including:**
    a. Commit to adoption of AI-enabled biometrics within administrative agency operations only to the extent that adoption demonstrably furthers the justification for delegated authority. Subject such adoption and use to regular oversight and review.
    b. Establish clear safeguards for experimentation with these technologies, including but not limited to mandating rights-based impact assessments before a biometric technology can be piloted by the government or the private sector, and requiring a high level of justification, as well as suitable precautions, when such technologies are deployed first on marginalized groups such as migrants or welfare benefit recipients.
    c. Address both (and distinguish between) public and private use, individual and group rights, and domestic and international use and data-sharing.
    d. Place meaningful constraints on actions taken abroad. This includes U.S. companies' operations abroad with regard to marketing, sale, or transfer of biometric data and technologies, as well as the U.S. government's actions in spheres including, but not limited to, international development, counterterrorism, defense, and migration.

5. **Ensure that any new laws, regulations, and policies are subject to a democratic, transparent, and open process.** This should include, *inter alia:*
    a. Hold further consultations, proactive outreach to affected communities, and engagement outside of the United States.
    b. Ensure that public education materials and any laws, regulations and policies should be described and written in clear, non-technical, and easily accessible language.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Dignari

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

Subject: Dignari Response to the Office of Science and Technology Policy (OSTP) Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Name of person(s) or organization(s) filing the comment: Dignari, LLC

Respondent type: Industry

Dignari is pleased to submit our response to the OSTP RFI. Dignari is a Women-Owned Small Business (WOSB) that specializes in program strategy, emerging technology, data science, and human-centered design. Our personnel have built and deployed numerous biometrics solutions successfully over the last 25 years, including for key U.S. Federal Government programs including the TSA Transportation Worker Identity Credential (TWIC), TSA Registered Traveler, Department of Homeland Security (DHS) Homeland Security Presidential Directive 12 (HSPD-12), U.S. Customs and Border Protection (CBP) Biometric Entry-Exit Program, General Services Administration (GSA) USAccess, and the DoD Common Access Card (CAC). We continue to provide a full suite of biometric services to our clients and look forward to published results from this RFI and OSTP's continued role in the advancement of policy relevant to biometric technology.

The table below provides our company and GSA MAS contract information for acquiring Dignari services and solutions. We welcome the opportunity to discuss these options in more detail. Dignari's point of contact is Adnan Malik, who can be reached at [redacted] or [redacted]

Dignari Company Information	
Company Name	Dignari, LLC
DUNS	079192182
Contact Name	Adnan Malik
Email	[redacted]
Phone & Fax	[redacted]
Business Address	[redacted]
Contract Vehicles:	GSA Master Award Contract (Dignari Prime): MAS GS-35F-584GA

Sincerely,

[redacted]

Gena C. Alexa
President
Dignari, LLC

Topic 1: Descriptions of use of biometric information for recognition and inference

Dignari personnel have over 25 years of experience with biometric technologies and have found that the use of biometric information falls into two broad categories: (a) for foundational use; and (b) for functional use. In effect, this aligns to the traditional access control constructs of authentication and authorization respectively.

Foundational biometric use most often determines "are you who you claim to be." (e.g., biometrics associated with passports). These systems incorporate varying levels of identity proofing appropriate to operational requirements prior to storage of biometric data. Functional biometric use (e.g., Apple Face ID) is based on some level of established foundational biometric data and is used to determine "are you eligible for a specific service" (e.g., to use an iPhone, to travel, to access a facility, to operate a vehicle), and is offered by both the public and the private sectors. When it comes to establishing root foundational identity within a society, government entities are most often relied upon as the authoritative source of biometric data. These foundational biometrics are in turn often used as seed inputs for derived systems. For example, using a passport photo for identity proofing during employment or benefit program issuance processes.

Each category has challenges and limitations in terms of use. Foundational biometric data, especially in the U.S., is often associated with breeder documents (e.g., birth certificates), however, the lack of universality of documents within a population (e.g., not every citizen owns a passport, lost birth certificates) creates challenges when trying to link biometrics with established industry or enterprise-wide rulesets. Functional biometric use has challenges such as a general mistrust of how the biometric data is used, how it is secured, and how it is obtained by both public and private sector entities. For example, utilizing PII to gain access to a resource, misuse of biometric data, and unknown collection such as automatically tagging people in photos.

Functional use of biometrics has grown rapidly over the last decade and touch almost every sphere of economic and social life, including banking, e-commerce, mobile phones, immigration, and travel. Recent advancements in biometrics, and artificial intelligence in general, have extended the functional use of biometric information to include behavioral or cognitive use. Notable examples include the use of facial biometrics in automobiles to assess the weariness and attentiveness of a driver or sentiment analysis for advertising. Dignari's work has spanned the full spectrum of foundational and functional use-cases of biometric information, crisscrossing the public and private sectors.

Foundational Biometric Use
Dignari has vast experience across multiple U.S. Federal Government clients in the use of foundational biometric information. Many of the systems that we have developed and delivered consist of an enrollment capability where breeder documents and other information is used for identity proofing prior to user account creation and biometric collection.
Planned, developed, or deployed uses
Our developed and deployed uses of foundational biometric data include enrollment systems where users gain access to program benefits or are issued credentials (e.g., federal employee and

contractor badges). Planned use includes referencing or using foundational biometric data to establish identity or to issue derived credentials for expedited and trusted travel uses cases.

Goals of use

Goals of use include initial identity proofing as well as the establishment of foundational biometric data which is authoritative in terms of the given program. This foundational biometric data may then serve as an enabler for functional use later. Foundational biometric data may be collected and stored in the system and serve as foundational for that program or the system may simply reference other authoritative source biometric data repositories at time of use.

Nature and source of the data used

Foundational biometric data typically involves attended collection between an operator and the individual who has opted in to be enrolled. This is to ensure the data is of high quality and trusted at the point of origination into the system. Some of these systems may collect a combination of biometric modalities. For example, ten prints for background investigations, face images for duplicate checks, and iris images for future system flexibility. Foundational biometrics should remain as close to single-sourced as possible. Distribution of copies or different versions of the biometric information may introduce challenges and increase privacy and security risks.

Deployment status (e.g., past, current, or planned deployment)

Dignari personnel have assisted with the implementation of numerous State/Federal/International foundational government biometric systems in the past and continue to support similar implementations today.

Impacted communities

Most of the foundational biometric systems we've implemented have been focused on providing a trusted population with the opportunity to voluntarily provide biometrics to gain access to specific program benefits, such as expedited processing.

Functional Biometric Use

Our experience working with the U.S. Federal government in the functional use of biometrics, includes traveler screening and identity management to improve citizen services and national security. In most cases, functional biometric use is limited to trusted populations or for frequent lower risk travelers who opt-in for added benefits and convenience of expedited processing.

Planned, developed, or deployed uses

Our developed and deployed use of functional biometric data includes several traveler processing systems where users gained access to dedicated lanes and expedited processing. Efficient and frictionless travel experiences are currently being implemented that allow touchless and more sterile biometric processing while improving overall security posture.

Goals of use

The functional biometric systems we've implemented have attempted to make the user experience faster, easier, and less intrusive while also making the system more secure and trustworthy.

Nature and source of the data used

The user experience is varied during functional biometric use. Technologies such as face and iris allow at-a-distance and on-the-move biometric collection while fingerprint typically requires direct contact with devices. Recent advances in contactless fingerprint technology reinforce the idea that industry continues to pursue a balance between convenience and utility. In many cases, sharing benefits across biometric system boundaries enhances the collective ecosystem. As a result, interoperability remains a central tenet with national and international standards bodies continuing to refine relevant standards. Some of our clients have used these industry standards to develop program specific requirements for functional biometric use. For example, establishing face image capture guidelines to include image requirements (e.g., dimensions, quality metrics) and camera placement.
Deployment status (e.g., past, current, or planned deployment)
Dignari personnel have assisted with the implementation of numerous State/Federal/International functional government biometric systems in the past and continue to support similar implementations today.
Impacted communities
Most of the functional biometric systems we've implemented have focused on providing a trusted population with dedicated areas for expedited processing. Impacted communities include travelers and operators of the system, as well as the larger community that relies on the security implemented by the system. Additionally, those who choose not to enroll or who are ineligible to participate are also impacted by their inability to realize potential benefits.

Table 1: Foundational and Functional Biometric Data Use

Topic 2: Procedures for and results of data-driven and scientific validation of biometric technologies

The procedures for and results of data-driven and scientific validation of biometric technologies requires more than just algorithm analysis—it requires an examination across the full spectrum of people, process, and technology. While there is great value in laboratory analysis of algorithms using standardized data sets, normalized procedures, and scientific methods, it is also important to understand the interplay between people, process, and technology in a holistic operational analysis. How does the technology perform given the unique and often unconstrained environments in which it is deployed and how do individuals interact with it? Unfortunately, biometric systems may excel in the lab yet fall flat in production. For example, we recently analyzed face Presentation Attack Detection (PAD) capabilities on mobile phones and our client's unique operational environment (e.g., time of day, indoors/outdoors) was central to our testing. One of the top performing solutions, which could not be spoofed in our lab, failed miserably once it was used outdoors. Understanding real-world scenarios such as this exposed the technology as unusable.

Human factors need to be analyzed when validating biometric technologies. How a biometric sample is collected, and the resultant quality of that sample, is directly related to the experience of the user during capture and the performance of the system. For example, will users know when a biometric collection process has started and ended? Will they clearly understand their role in the process? Will they perform the expected action adequately enough for the collection of a quality sample? For one of our clients, we helped assess multimodal biometric systems deployed in a harsh outdoor environment. The analysis included weekly test increments with configurations that analyzed user behavior while interacting with unique biometric hardware devices across varied

pedestrian traffic flows. The overall experiment ran for 3 months with weekly biometric capture modes (e.g., face only, iris only, face and iris) and a rotation of vendor solutions to ensure data coverage and fairness. These weekly cycles assessed numerous aspects of biometric technology including but not limited to population statistics, traveler demographics, time of day data, weather conditions, device timings, impacts of habituation, subject gaze, occlusions, background faces, image attributes, placement and orientation of hardware, and queue management.

Many of our clients continuously monitor biometric matching performance to not only improve operations but to also improve the underlying algorithm. This has led to a substantial reduction in initial gaps in matching across age, gender, and nationality. Consistent statistical testing bolsters performance thresholds and minimizes the impact of racial or gender bias. There is also a need to conduct manual reviews of data to confirm algorithm performance and to better understand false match and false non-match results.

Participants in the biometrics space should also be encouraged to share data analysis and scientific research to collectively improve the biometrics industry. For example, CBP is partnering with NIST to perform independent analyses of face matching performance including the potential impact of traveler demographics and image quality. In addition, CBP is working with the DHS Science and Technology Directorate to evaluate overall effectiveness of facial algorithms.

Topic 3: Security considerations associated with a particular biometric technology

Unlike other forms of sensitive information (e.g., financial information, health information, login information) that travels the web, biometric information is rather immutable and limited in options and entropy. In addition, in today's age of cloud and edge computing, personal information may be distributed widely and outside the control of the end user. The use of biometric information in today's age requires stronger safeguards in all stages of the data lifecycle (i.e., collection, storage, distribution, in motion, and at rest) to maintain privacy and security. In many instances, biometric data is protected using proven industry data protection methods such as secure transport technologies and encrypted data formats.

Even with these traditional controls, biometric technology poses unique challenges for security. This includes the advent of synthetic identity, spoofing techniques against recognition, and other approaches to defeat the deduplication algorithm commonly used by biometric technology. For example, a common spoofing technique is utilizing someone else's biometric data to perform actions on their behalf or to gain access to systems or facilities. These use cases are not just rudimentary exploits such as the infamous gummy bear fingerprint hack. As AI technology advances, the threats within the biometric space increases exponentially. New attacks may use deep fake video for authentication or employ photo morphing techniques to inject fraudulent root identity data, posing new challenges that traditional IT security approaches can't easily solve. For Presentation Attack Detection (PAD) on mobile devices, there are solutions utilizing both active and passive analysis of the user and their environment. This includes approaches such as eye tracking of dynamic content, background movement analysis, reflectivity, multispectral analysis of the face, and other technologies to determine if the user is live and in person. Traditional biometric systems have required users to perform actions in attended modes (i.e., an operator directly assisting the user during biometric capture), either for security reasons or simply because

the process was unfamiliar. As mobile phones have advanced, biometric operations are now in the hands of the user (i.e., unattended) and evolving into the wild. Remote enrollment systems and similar unattended use cases introduce new attack vectors that will need to be tracked and mitigated. As commercial entities such as Apple, Samsung, and Google embrace biometric use cases, will their implementations be trusted and leveraged for official government business?

Dignari's long-standing work in biometrics across clients has focused on building robust safeguards for security and privacy, using instruments of policy, technology design, data protection, and operational control. We have been involved in several significant technical security and policy roles since CBP inherited the biometric entry/exit mission in 2013. When CBP began testing biometrics at airports in 2016, the Dignari team opened the lines of communication to engage with both internal and external biometric entry/exit stakeholders in cybersecurity, civil liberties, and information privacy to seek input from the community and share facts about the program. Supported by Dignari privacy Subject-Matter Experts (SMEs), CBP coordinated several outreach events with privacy and civil liberties advocates as well as the Privacy and Civil Liberties Oversight Board. In addition, our SMEs engaged Privacy Offices within CBP and DHS Headquarters in drafting multiple Privacy Threshold Assessments (PTA), Privacy Impact Assessments (PIA), Privacy Notices through Privacy Act Statements (PAS), signage at affected facilities, verbal announcements, and tear sheets with frequently asked questions, as well as language for the relevant public websites.

Topic 4: Exhibited and potential harms of a particular biometric technology

One harm that may not garner as much attention is participatory bias. This is where technical, environmental, and/or operational limitations may unintentionally exclude certain populations from taking advantage of biometric technology benefits or worse, introduce extraneous processing or negative experiences for the participant. For example, elderly individuals may not be able to perform necessary capture operations such as placing arthritic fingers on a flat platen. Operational or environmental constraints such as fixed infrastructure, may prevent exceptionally short or tall people from having an optimized facial image captured. Physical disabilities or accessibility issues may prevent someone from interacting with a particular biometric device. Many issues can largely be overcome by solution design and thoughtful analysis in the pilot stage, but awareness is key.

Topic 5: Exhibited and potential benefits of a particular biometric technology

There are many potential benefits of utilizing biometric technology. This section will explore those benefits by user, covering system implementers, government system owners, and end users. By examining the benefits by user, we can identify the success of biometric technology use cases.

For system implementers such as airlines and airports, they have the potential to modernize their processes without unduly burdening their customer. Current processes and infrastructure may be unable to sustain air-travel given the projected increases in the quantity of passengers. A facial biometric system can minimize the burden on existing processes and systems while increasing convenience for the passenger. Unlike fingerprinting or other more intrusive biometric modalities, a facial capture is all that is required to verify one's identity and create a better user experience for

all parties. Additional benefits at the airport could also be enabled for a full curb-to-gate touchless experience while maintaining a more secure and sterile environment for travelers.

For government system owners, overall security can be improved by automatically confirming known identities using biometrics. This minimizes an operators time spent verifying individuals and increases their time to focus efforts on higher risk populations, edge cases, and exceptions. For example, a biometric entry-exit system can effectively combat attempts by foreign national terrorists to circumvent border checkpoints. This is done by providing an accurate way to verify an individual's identity using biometrics and minimizing the unlawful entry using false identity documents. Establishing such a system is crucial to our efforts to respond to the continuing threat of global terrorism. The increasingly sophisticated features in modern passports have led to the increased use of legitimate documents by imposters. Today, those seeking to evade detection by CBP, or other border security services frequently use a non-altered travel document legitimately issued to another person. The best tool to combat this fraud is to biometrically verify that a person who presents a travel document is the true bearer of that document. Using a biometric verification system, CBP can update the border crossing records of foreign nationals and provide greater assurance that the government will be able to identify imposters during future encounters.

For end users there are also benefits of particular biometric technologies. Face recognition systems provide an easy-to-use, more convenient interface that expedites interactions between an individual and the system. As biometrics continue to gain momentum in the private sector, additional benefits are realized such as paying for mobile food orders using Apple Face ID. There are also additional use cases across sectors that open the possibility of benefits for face recognition. From detecting mental stress and depression to helping those with Alzheimer's recognize photos of friends and family, face recognition offers new and innovative ways to interact with the world around us.

Topic 6: Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case

(a) Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;
Stakeholder engagement is critical for any emerging technology implementation, especially biometric technologies. Stakeholders should be viewed across a wide swath of communities, both internal and external. External stakeholders should include those with direct domain knowledge such as industry consortiums, national and international standards bodies, academia, as well as technology product and service providers. It should also include indirect communities who may be impacted or play a role in system implementation such as the public at large, privacy advocates, and the media. Internal stakeholders should cover the gamut of support operations needed to field successful biometric implementations. This includes business/mission owners, program management, acquisition, budgeting, technology implementers, infrastructure and hosting providers, UI/UX designers, security and privacy groups, public affairs, testing

organizations, application developers, and many more. Each must understand the unique aspects of biometric implementations and adhere to overarching security and privacy requirements. Leaning more toward a transparent and collaborative stakeholder engagement model not only keeps everyone informed but it also allows each entity to feel invested in the success of the project. Stakeholders should be engaged at the onset of biometric technology implementation and work together with the delivery team from initial proof of concept, through field pilots, into production, and throughout scaled enterprise operations and maintenance.

(b) Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments

Dignari has significant experience in planning, conducting, and analyzing biometric pilot studies across a range of government sponsors. When conducting pilots or trials it is important to define goals and objectives and to identify measures of success. Understanding what is being tested, and what is hoped to be gained because of the test, should inform how you plan, design, and ultimately conduct each pilot. With this baseline understanding of what is being evaluated, it is then possible to work backwards to define the minutiae of the pilot including evaluation criteria, target populations, deployment locations, pilot phases and duration, and overarching test methodologies to collect relevant data. When utilizing biometric technologies, pilots should be as close to real operations as possible. Users should be representative of a diverse user population and interact with the system consistent with the expected end state. While it may not be possible to fully mimic the end state for each pilot, the goal should remain to be as close as possible. Pilots may be conducted one at a time or incrementally with adjustments to functionality analyzed after each iteration. Regardless of the frequency or duration, each pilot should feed into a larger vision of the organization's biometric operations and inform future work. Additionally, output and findings from the pilots should be shared with relevant stakeholders throughout the process and tracked over time in a centralized and open repository so they may be referenced and used as inputs for future projects.

(c) Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices

Data collection should include processes and procedures related to individual participation. For example, U.S. Citizens who do not wish to have their photos taken during international travel can request alternative processing through government officials or other stakeholders. It's common for most government biometric systems, especially pilot systems, to employ opt-in procedures and alternative processing for those who do not want to participate in the system. These alternate processing guidelines are typically published in standard operating procedures.

To help inform these decisions, biometric system owners should document and publicize intended use of biometric data including retention policies. Many U.S. Federal government biometric programs notify the public using PIAs, System of Record Notifications (SORNs), and through program information such as Frequently Asked Questions readily available via public websites. For example, DHS has published more than 10 PIAs on their Biometric Entry/Exit program to explain all aspects of the program including policies and procedures for the collection, storage, analysis, use, dissemination, retention, and deletion of data.

Data storage and retention should be minimal and focused solely on time frames of valid use within the system and for particular use cases. Foundational biometric data should have documented procedures for data lifecycle management from initial identity creation through deprovisioning and account termination. Functional biometric data, collected at the time of an encounter with the system, should only be stored for specific purposes such as ongoing system performance analysis or evidentiary reasons. For one-to-many identification scenarios, biometric galleries should be limited to the specific target population and ideally remain ephemeral for that particular use.

As an example of proper and tailored data processes and storage, an organization may reduce the retention period of certain protected populations to no more than 12 hours after identity verification and only for continuity of operations purposes. Facial images of other populations within the system may by be retained for up to 14 days in secure systems to support system audits and to evaluate facial recognition performance. Longer term storage to comply with relevant laws and regulations may also be implemented and socialized using SORNs.

(d) Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use

Safeguards and limitations of approved use should be specifically documented and agreed upon by all stakeholders. For example, business requirements should not allow approved partners or biometric vendors to retain the photos they collect under a government process for their own business purposes. The partners must immediately purge the images following transmission to government systems, and the partner must allow audits to ensure compliance. If there are stipulations where images may be used for ongoing analysis, those should be identified, documented, and publicized accordingly with controls in place to anonymize the data as much as possible. If data is to be shared between government organizations for research and analysis, Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) may be necessary to safeguard the data. Strong encryption should be used to transfer the data between the capture device, local or backend matching services, and relying systems, as well as for data at rest. Image data should be minimally stored due to security and privacy reasons. When possible, biometric templates instead of images should be used to limit the possibility of reuse or theft of root biometric data. Only authorized government personnel and authorized representatives of approved government partners should have access to physical devices like cameras. Separation of duties and role-based access control should also be defined for each system component including central data repositories.

(e) Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms)

Performance auditing and post-deployment impact assessments should be standard practice that provide maintenance activities of biometric system implementations. Beyond performance analysis of biometric matching algorithms, it's important to also audit processes and user behavior. This includes analyzing the effects of habituation over time to determine if users are effectively interacting with the system or if something needs to be tweaked before abandonment becomes an issue. System timing metrics should be reviewed at a granular level to understand how long each event takes to identify gaps in performance and opportunities for optimization.

Metrics should be compared to baseline numbers captured prior to deployment and tracked over time to identify anomalies and issues. These analyses should not be performed in a vacuum rather they should be socialized with relevant stakeholders and collectively assessed for future configuration changes or modifications. Additionally, the relevant privacy offices should continually evaluate programs to ensure that all parties maintain required privacy protections.

(f) Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage)

Dignari has performed preliminary research and analysis of potential surveillance camera-based face recognition solutions. This includes using face biometrics to detect and identify individuals as they move through a secure space. While there have been studies in the past such as the NIST Face In Video Evaluation (FIVE)[1], questions remain as to the accuracy of these systems given substandard cameras, suboptimal mounting locations, prevalence of occlusions, and overall poor biometric capture environments. Biometric technologies used in conjunction with surveillance systems also introduces a unique conundrum—if a match isn't detected does that mean the system isn't working or just that a targeted individual wasn't present? For example, a system may be deployed in a public area to check live faces against a watchlist of known criminals. If at the end of a period no criminals are detected, how do you know whether the system malfunctioned or if no criminals happened to walk through the capture zone? There continues to be significant academic research into surveillance-based face recognition capabilities and more generally of face recognition in challenging environments.

(g) Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems

Dignari does not have relevant experience to add for this item.

(h) Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate

In all biometric systems that Dignari has supported, public transparency and notice of use have been central to the ultimate success and acceptance of the biometric technologies. Identification and documentation of how the biometrics of system users will be utilized should be conducted early in the project/program lifecycle and revisited throughout. Many times, this is addressed in PIAs, SORNs, and other open publications. As solutions mature and near piloting or production deployment, public relations efforts should be used to further inform the public of how the biometrics will be used as well as their opportunities for contestation and redress. Signage, tear sheets, and other communication methods should be deployed to areas where biometrics are being actively captured. These should be easy to understand, accessible, and offer information regarding alternate processes available.

[1] https://www.nist.gov/programs-projects/face-video-evaluation-five

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Douglas Goddard

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] Automatic License Plate Recognition (ALPR)
Date: Thursday, October 21, 2021 1:24:54 PM

This technology needs to be controlled. If the government were to enable it on each street corner it would effectively enable the tracking of any vehicle. Most vehicles are tied to a single driver so this would create a citizen-level tracking system.

Additionally, any tracking information stored should come with a steep penalty in case of a data breach. We need to raise the bar for companies that store PII. If they lose that PII to an adversary, they should face significant fines on the order of $10,000 per record, with no cap. Let us make companies think twice before storing PII.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Edgar Dworsky

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Monday, January 10, 2022 2:44:16 PM

For OSTP's inquiry into uses of biometric technologies and the impact on affected populations, I offer you the story of one customer's experience with Spectrum Cable and their Voice ID security system.

In a nutshell, she alleges that without her knowledge and affirmative consent she was opted into the cable provider's Voice ID system which creates a digital voiceprint from her voice, so in future calls less authentication is needed. She says her involuntary enrollment in the program came about despite the company's publicized assurances that the program was "optional" and "completely voluntary."

See her story here:

>https://www.mouseprint.org/2022/01/10/does-spectrum-capture-your-voice-then-secretly-use-it-for-id-purposes/<

What happened to her, and perhaps to other customers, raises the need for better notice and recordkeeping of opt-in acceptances to biometric services, penalties irrespective of financial loss to the victim for violations of stated biometric policies or applicable law, and better disclosure when biometric tools are being used that affect individual consumers.

I offer this information as a consumer advocate, and a former Assistant Attorney General in Consumer Protection in Massachusetts.

--

Edgar Dworsky, Founder & Editor

[redacted]
>http://www.MousePrint.org<

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Electronic Frontier Foundation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

ELECTRONIC FRONTIER FOUNDATION

Comments of the Electronic Frontier Foundation Regarding

Notice of Request for Information (RFI) on
Public and Private Sector Uses of Biometric Technologies

Office of Science and Technology Policy (OSTP)

Document No. 2021-21975

86 Fed. Reg. 56300

Submitted on January 15, 2022

The Electronic Frontier Foundation (EFF) submits the following comments in response to the Office of Science and Technology Policy (OSTP)'s Request for Information (RFI), published at Document Number 2021-21975. These comments will focus on current and proposed uses of DNA technology in immigration and law enforcement. They will respond primarily to Topic 4, "Exhibited and potential harms of a particular biometric technology," although they will also touch on Topic 1, "Descriptions of Use;" Topic 3, "Security Considerations;" and Topic 6, "Governance Programs."

EFF is a non-profit organization that has worked for 30 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. EFF actively encourages and challenges all branches of government to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With more than 30,000 contributing members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

I. Introduction

DNA contains our most private and personal information. Unlike other biometrics that can (or should) only be used for identification, DNA provides "a massive amount of unique, private information about a person that goes beyond identification of that person."[1] Every tiny piece of skin or hair or saliva contains a person's entire genetic code—information that has the capacity to reveal the individual's race, biological sex, likely eye and hair color, ethnic background, familial relationships, behavioral characteristics, health status, genetic diseases, and predisposition to certain traits. Companies are even able to use genetic data to predict what an unknown person might look like today or in the past, which can then be used to generate a composite image of the person.[2] DNA data can also be combined with other data from public records and

[1] *State v. Medina*, 102 A.3d 661, 682 (Vt. 2014) (citations omitted).
[2] *See, e.g.,* Parabon Nanolabs, "The Snapshot DNA Phenotyping Service," https://snapshot.parabon-nanolabs.com/intro#phenotyping; *id*., "Forensic Art Enhancement," https://snapshot.parabon-nanolabs.com/intro#artwork.

social media to create a full picture of a person's life. And unlike a social security or driver's license number, DNA can never be changed. The depth and breadth of information contained in our DNA justifies strong restrictions on its collection and use.

II. DNA Collection and Use Has Expanded as DNA Technology Has Advanced

DNA has been used in criminal investigations for nearly 40 years,[3] and DNA collection is now mandatory from those convicted of or arrested for most crimes. DNA profiles are stored in various local, state, and national DNA databases, including the FBI's Combined DNA Index System (CODIS) database, which contains 14.8 million offender profiles and more than 4.5 million arrestee profiles.[4]

DNA technology has advanced significantly in the last few decades. Where once, a useful forensic sample could only be obtained from blood, semen, or other bodily fluids, today, investigators can detect, collect, and analyze DNA from objects merely touched by a person. Because we cannot help but leave DNA behind on nearly everything we touch, this vastly expands investigators' ability to collect DNA. It also allows investigators to collect DNA from and identify individuals without their knowledge—for example, by collecting DNA from a straw or cigarette they may have used and discarded. The heightened sensitivity in DNA collection technology has also resulted in the collection of trace amounts of DNA from objects, like a door knob or a knife, that may have been touched by more than one person. Probabilistic genotyping software claims to be able to analyze these DNA mixtures and identify unique individuals.[5]

The time it takes to process and sequence DNA has decreased significantly as well. Where once it took labs a month or more to generate a DNA profile, federal and state agencies now have access to Rapid DNA analyzers— self-contained, automated, portable machines that allow non-scientists to process a DNA sample and generate a profile outside a lab in as little as 50 minutes.[6] This allows DNA to be used much like other biometrics—to identify specific individuals on the spot.

Further, the costs of genetic sequencing have decreased so significantly that DNA

---

[3] Ian Cobain, *Killer breakthrough—the day DNA evidence first nailed a murderer*, The Guardian (June 7, 2016) https://www.theguardian.com/uk-news/2016/jun/07/killer-dna-evidence-genetic-profiling-criminal-investigation.
[4] CODIS - NDIS Statistics, FBI (Oct. 2021) https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics.
[5] Hannah Zhao, *How Your DNA—or Someone Else's—Can Send You to Jail*, EFF Deeplinks Blog (May 14, 2021) https://www.eff.org/deeplinks/2021/05/how-your-dna-or-someone-elses-can-send-you-jail.
[6] *See* U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Rapid DNA Operational Use DHS/ICE/PIA-050 2 (June 25, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-rapiddna-june2019_1.pdf.

collection and analysis have expanded far beyond use for health, research, or criminal justice purposes. DNA profiles used for criminal justice purposes have typically contained 13-20 short-tandem repeat (STR) DNA markers, which are specifically chosen from non-coding (and thus less revealing) segments of DNA. But as costs related to DNA processing have decreased, police are beginning to access more information from DNA samples. It is now possible to create a genetic profile made up of more than half a million single nucleotide polymorphisms (SNPs) that span the entirety of the human genome for just $99 or less.[7] This has led to the rise of consumer genetic testing, the portability of genetic data, and the growth of consumer genetic databases that offer to connect people to long lost relatives and provide insights into health, frequently for no cost at all.[8] These sites and databases have already been used by the police in hundreds of investigations to identify people who are genetically related to unknown DNA samples and to identify a sample's donor, even when that donor has not entered their own genetic data into the consumer database.[9]

As the costs associated with DNA collection and processing have decreased, federal and state agencies have increased their reliance on DNA. For example, DNA use for immigration-related purposes has expanded, despite a lack of supporting statutory or regulatory authority.[10] In 2019, the U.S. Department of Homeland Security (DHS) began a program to use Rapid DNA on migrant families at the U.S.-Mexico border to identify and prosecute individuals who are not related through a biological parent-child relationship. The program began as a three-day pilot program at two locations and quickly expanded to a 10-month program at seven locations.[11] DHS later extended this contract for up to five years.[12] Although DHS claimed that the testing was voluntary, refusal to submit to testing could factor into a decision of whether to separate parent from

---

[7] *See, e.g.*, Ancestry, https://www.ancestry.com/dna/.
[8] *See, e.g.,* GEDmatch, https://www.gedmatch.com/.
[9] *See, e.g.*, Megan Molteni, *The Future of Crime-Fighting Is Family Tree Forensics*, Wired (Dec. 26, 2018), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.
[10] Jennifer Lynch et al., *Comments of the Electronic Frontier Foundation Regarding Notice of Proposed Rulemaking on the Collection and Use of Biometrics by U.S. Citizenship and Immigration Services* at 31–34, EFF (Oct. 13, 2020) https://www.eff.org/document/eff-comments-dhs-proposed-rule-collection-and-use-biometrics-october-2020.
[11] Chris Burt, *Rapid DNA testing at U.S. border extended and criticized*, BiometricUpdate.com (Aug. 7, 2019), https://www.biometricupdate.com/201908/rapid-dna-testing-at-u-s-border-extended-and-criticized; Mark Albert, *ICE warns of privacy from DNA checks of border-crossing migrants*, WCVB5 (June 26, 2019), https://www.wcvb.com/article/ice-warns-of-privacy-risks-from-dna-checks-of-border-crossing-migrants/28199494#.
[12] Cal Biesecker, *ICE Awards Bode Contract for Rapid DNA Testing on Southwest Border*, Defense Daily (Mar. 31, 2020), https://www.defensedaily.com/ice-awards-bode-contract-rapid-dna-testing-southwest-border/homeland-security/.

child in immigration detention.[13] And in a 2020 Notice of Proposed Rulemaking (NPRM), DHS proposed extending its regulatory authority to mandate DNA collection "for any benefit request where [a genetic] relationship must be established."[14] DHS would have applied this rule to prospective immigrants and U.S. persons alike, potentially increasing the number of people subject to mandatory DNA collection from zero to an estimated 805,493 each year.[15] Of those, approximately 336,650 would have been U.S. citizens.[16] DHS proposed retaining "partial DNA profile" data that would have genetically linked family members in the database.[17] In the NPRM, DHS left open the possibility that it could, at its own discretion, share DNA test results and DNA profiles with other agencies, including law enforcement agencies.[18]

III. DNA Collection Presents Unique Threats to Privacy

In the past decade, law enforcement and immigration authorities have been working to normalize biometrics collection and expand the collection of DNA from more and more individuals caught up in the criminal justice and immigration systems with little evidence that doing so solves or prevents crimes or immigration violations.[19] By vastly expanding the amount of DNA collected and added to national, state, and local DNA databases, however, these efforts are bringing us closer to a regime of DNA collection from the entire population without any public or legislative debate on the serious attendant threats to privacy and civil liberties.

A. DNA Can Reveal More Sensitive and Private Information Than Other Biometrics

DNA collection threatens privacy because each DNA sample contains a person's

---

[13] Saira Hussain, *ICE's Rapid DNA Testing on Migrants at the Border Is Yet Another Iteration of Family Separation*, EFF Deeplinks Blog (Aug. 2, 2019), https://www.eff.org/deeplinks/2019/08/ices-rapid-dna-testing-migrants-border-yet-another-iteration-family-separation.
[14] *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338, 56364 (proposed Sept. 11, 2020).
[15] *Id.* at 56380. DHS noted that it "currently accepts DNA test results for 11,383 beneficiaries" each year. However, none of these submissions are mandatory.
[16] *Id.* at 56380.
[17] Lynch, *supra* n. 10, at 18–19.
[18] 85 Fed. Reg. at 56353; *see also* Proposed 8 C.F.R. pt. 103.16(e).
[19] *See, e.g.*, Bill Farrar, *Proposal to Expand Mandatory DNA Collection in Virginia Raises Serious Privacy and Due Process Concerns*, ACLU Free Future Blog (Jan. 8, 2018), https://www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/proposal-expand-mandatory-dna-collection; Jason Silverstein, *The Dark Side of DNA Evidence*, The Nation (Mar. 27, 2013) https://www.thenation.com/article/dark-side-dna-evidence/ (reporting that, "[i[n 2011, Maryland police collected 10,666 DNA samples; only nineteen led to an arrest.").

entire genetic code. This not only can reveal a person's propensity for various diseases like breast cancer or Alzheimer's and can predict traits like addiction and drug response, but can also identify family members and ancestors, predict a person's appearance, and may reveal much more information in the future as scientific knowledge advances.

DNA profiles, which contain less data than a full DNA sample, still present privacy threats. One study—conducted when the FBI's CODIS database relied on just 13 loci—found that the STR profiles in CODIS can identify information about individuals' ancestry, which may, in turn, be used to reveal information about their phenotypic traits (i.e., physical appearance) based on assumptions about race and ethnicity.[20] Another study suggested that the profiles maintained in CODIS can now be matched to SNP profiles in other publicly accessible databases, suggesting that DNA profiles stored in government databases could be used to identify anonymized genomes from health-research databases or other sources.[21]

Data aggregation—combining genetic profiles with other government-maintained or publicly available data—increases these privacy risks. In 2012, researchers used genetic genealogy databases and publicly-available information to identify nearly 50 people from just three original anonymized samples.[22] More recent research shows that 60% of white Americans can already be identified from a genetic genealogy database representing just 0.5% of the U.S. population.[23] While the FBI's CODIS database does not store any names or personal identifiers with DNA profiles, and the FBI keeps DNA separate from other biometric data,[24] DHS proposed storing DNA information in an immigrant's "A-file," along with all other biometric and biographic information.[25] This

---

[20] Bridget Algee-Hewitt et al., *Individual Identifiability Predicts Population Identifiability in Forensic Microsatellite Markers*, Current Biology (Mar. 17, 2016), https://doi.org/10.1016/j.cub.2016.01.065.
[21] Michael D. Edge et al., *Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets*, Proceedings of the National Academy of Sciences (May 15, 2017), https://doi.org/10.1073/pnas.1619944114; Lindzi Wessel, *Scientists concerned over US plans to collect DNA data from immigrants*, Nature (Oct. 7, 2019), https://www.nature.com/articles/d41586-019-02998-3.
[22] Melissa Gymrek, et al., *Identifying Personal Genomes by Surname Inference*, Science (Jan. 18, 2013) https://www.science.org/doi/10.1126/science.1229566.
[23] Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, SCIENCE (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white (This same research shows that once just 2% of the U.S. population has uploaded DNA, 90% of white Americans would be identifiable.).
[24] *See* FBI, Frequently Asked Questions on CODIS and NDIS, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.
[25] 85 Fed. Reg. at 56347.

would make DNA data and relationship information easily accessible to other users of those databases.

B. Collecting Data on Genetic Relationships Threatens the Privacy Interests of Whole Communities

Consumer genetic databases now make it possible to map generations of family members using the genetic information of a relatively small number of individuals who opt in to sharing their own data. As noted above, police are increasingly accessing this information in criminal investigations. Familial searches through non-criminal data have been hotly debated within the American public, with many people choosing to opt-out of these searches where they can.[26]

In 2020, DHS proposed collecting genetic data that would have allowed it to similarly map family relationships.[27] This would have made familial DNA searches accessible to any agency or user who had access to DHS's database and a law enforcement- or immigration-related need. DHS proposed to do this with no public debate and no congressional oversight. But collecting genetic relationship data from immigrants and U.S. persons would have allowed the federal government, in the near future, to map whole generations of family members, and by extension, whole immigrant communities. Agency action like this further compounds threats to individual privacy and autonomy and violates societal norms.

In 2008, the United Nations High Commissioner for Refugees (UNHCR) recognized that DNA testing "can have serious implications for the right to privacy and family unity," and should be used only as a "last resort."[28] UNHCR noted that, if DNA is collected, it "should not be used for any other purpose than the verification of family relationships" and that DNA associated with the test "should normally be destroyed once a decision has been made." Proposals such as DHS's have failed to meet even this bare requirement.

IV. Government-Mandated DNA Collection Exacerbates Racial Disparities and Harms Vulnerable Populations

Expanding the collection of DNA will exacerbate racial disparities that are already present in existing DNA databases and harm vulnerable populations. In 2011, it was estimated that Black individuals made up 40 percent of profiles in CODIS (despite representing only 13.4% of the U.S. population), and that it was possible, even with

---

[26] Heather Murphy, *Why a Data Breach at a Genealogy Site Has Privacy Experts Worried*, N.Y. Times (Aug. 1, 2020), https://www.nytimes.com/2020/08/01/technology/gedmatch-breach-privacy.html.
[27] *See, e.g.*, 85 Fed. Reg. at 56341.
[28] UNHCR Note on DNA Testing to Establish Family Relationships in the Refugee Context, 1, 5(2008) *available at* https://www.refworld.org/pdfid/48620c2d2.pdf.

limited CODIS profiles, "to use the database to identify up to 17 percent of the country's entire African-American population."[29]

Several recent proposals to expand DNA collection have been aimed squarely at immigrants and refugees. In March 2020, the U.S. Department of Justice finalized a regulation that allowed for DNA collected from immigrant detainees to be entered into CODIS—leading to the addition of up to 750,000 new DNA profiles a year.[30] This will undoubtedly further skew the racial disparities in CODIS, given that in 2018, 43 percent of immigrant detainees were from Mexico and an additional 46 percent were from Guatemala, El Salvador, or Honduras.[31] DHS's 2020 proposal similarly threatened to disproportionately impact communities of color, both among U.S. persons and immigrants.

V. Government DNA Collection Puts Innocent People at Risk of Being Accused of Crimes They Didn't Commit

The overcollection of DNA puts individuals at risk of being identified for a crime they did not commit, merely because their DNA already exists in a government database. This is so because we shed DNA constantly and because forensic tools are so sensitive that they can detect DNA on almost any surface, even if it is only a trace amount. DNA may be found not only on items that a person has touched, but also on other items with which the person never came into contact—a phenomenon known as "secondary transfer."[32] This means that crime scene samples can contain DNA from someone who was never at the scene or who was there or touched something transported to the crime scene long before the crime was ever committed. In California, a man spent five months in jail after a database search linked his DNA to DNA found on the fingernails of a murder victim—although the man was in the hospital when the murder occurred.[33] Prosecutors believe paramedics may have transferred his DNA to the murder victim when they responded to the crime scene hours after dropping him off at the hospital. He never

---

[29] Silverstein, *The Dark Side of DNA Evidence*, supra n. 19; *Quick Facts*, Census, https://www.census.gov/quickfacts/fact/table/US/RHI225219#RHI225219.
[30] DNA-Sample Collection from Immigration Detainees, 28 CFR Part 28, https://www.federalregister.gov/documents/2020/03/09/2020-04256/dna-sample-collection-from-immigration-detainees.
[31] Emily Ryo & Ian Peacock, *The Landscape of Immigration Detention in the United States*, American Immigration Counsel (Dec. 2018), at 2, https://americanimmigrationcouncil.org/sites/default/files/research/the_landscape_of_immigration_detention_in_the_united_states.pdf.
[32] Katie Worth, *Framed for Murder by His Own DNA*, Wired (Apr. 18, 2019), https://www.wired.com/story/dna-transfer-framed-murder/.
[33] Henry Lee, *How Innocent Man's DNA Was Found at Killing Scene*, SF Gate (June 26, 2013), http://www.sfgate.com/crime/article/How-innocent-man-s-DNA-was-found-at-killing-scene-4624971.php.

would have been linked to the crime if his DNA had not already existed in a government database.[34] Given this, researchers have recognized that "[a] DNA hit does not show that the subject is the offender and there are many reasons why the DNA of an individual may be found at a crime scene."[35] Nevertheless, this has not stopped prosecutors from arresting someone solely based on a DNA hit.

VI. Government-Mandated DNA Collection Must Take Account of Reliability, Accuracy, and Security Issues

DNA analysis is far from infallible, and faulty DNA processing has threatened people's civil liberties. In 2015, for example, a San Francisco crime lab analyst repeatedly made assumptions about poor-quality, incomplete genetic evidence, falsely linking a DNA profile to a defendant and potentially causing errors in as many as 1,400 other cases.[36] Similarly, the Washington D.C. Crime Lab lost its accreditation several times for its error-prone DNA analyses.[37] And just this month, the Virginia Attorney General announced the Virginia Beach Police Department used forged DNA reports to get confessions.[38]

Accuracy and reliability challenges have continued, even as technology has advanced. In 2017, the Swedish National Forensic Centre published a report detailing serious problems with certain Rapid DNA analyzers, finding that "36% of the runs had

---

[34] This is not an isolated occurrence. In another case, the main contributor of DNA found on the murder victim's underwear had been dead for two years before the murder was committed. Erin E. Murphy, *How DNA Evidence Incriminated an Impossible Suspect*, The New Republic (Oct. 26, 2015) https://newrepublic.com/article/123177/how-dna-evidence-incriminated-impossible-suspect.

[35] Aaron Opoku Amankwaa & Carole McCartney, *The effectiveness of the UK national DNA database*, 1 Forensic Science International: Synergy 45, 49 (2019), https://www.sciencedirect.com/science/article/pii/S2589871X19300713.

[36] Jaxon Van Derbeken, *Technician, boss in SFPD lab scandal flunked DNA skills exam*, (March 30, 2015) https://www.sfgate.com/bayarea/article/Technician-boss-in-S-F-police-lab-scandal-6169230.php.

[37] Keith L. Alexander, *National accreditation board suspends all DNA testing at D.C. crime lab*, Wash. Post (April 27, 2015) https://www.washingtonpost.com/local/crime/national-accreditation-board-suspends-all-dna-testing-at-district-lab/2015/04/26/2da43d9a-ec24-11e4-a55f-38924fca94f9_story.html; *see also e.g.,* Ate Kloosterman, et al, *Error rates in forensic DNA analysis: definition, numbers, impact and communication*, Forensic Sci Int Genet. (Sept. 2014) https://pubmed.ncbi.nlm.nih.gov/24905336/.

[38] Deepa Shivaram, *Virginia Beach Police used forged DNA reports to get confessions, investigation finds*, NPR (Jan. 13, 2022) https://www.npr.org/2022/01/13/1072766152/virginia-beach-forged-evidence-investigation.

problems or errors effecting two or more samples."[39] This resulted in a 23% failure rate, even with higher quantity samples.[40] Notably, many local, state, and federal agencies that use Rapid DNA systems have provided no statistical or peer-reviewed studies as to their accuracy. There have been similar problems with newer high-sensitivity testing of trace amounts of DNA and mixtures. Independent examination of the source code of probabilistic genotyping software has revealed mistakes and flaws that call into question the accuracy of these tools and their suitability for the criminal justice system.[41]

VII. Laws and Regulations Have Not Kept Pace as DNA Advances

Laws have not kept up with advances in DNA technology. The most recent Supreme Court case to address DNA collection was decided nearly a decade ago. In *Maryland v. King*, the Court upheld, by a slim majority, the warrantless collection of DNA from arrested persons, holding that a DNA swab did not violate an arrestee's expectation of privacy.[42] The Court solely addressed the collection of DNA from a specific class—arrestees—and limited its analysis to the minimal physical intrusion of the cheek swab and data contained in a CODIS profile. However, this hasn't stopped police and immigration authorities from citing *King* to justify everything from warrantless collection of DNA from free people without their knowledge and immigrants who are not subject to arrest warrants to searches through consumer DNA databases.

It is possible, given what we now know about DNA and how much it can reveal, that the Court would decide the case differently today. For example, in a more recent case, the Court held the Fourth Amendment did not allow the warrantless collection of a blood sample from an allegedly intoxicated driver because "blood tests are significantly more intrusive [than breath tests]."[43] This was true even though the police used only the limited blood alcohol information contained in the sample.

There have been some efforts to regulate DNA collection and search by statute or agency policy, particularly with respect to familial searches. The FBI has disclaimed association with familial searching as a matter of policy,[44] while Maryland and the District of Columbia have banned them through statute, citing concerns that "genetic

---

[39] Swedish National Forensic Centre, *Experiences from operating the RapidHIT® System* 3 (2017), https://nfc.polisen.se/siteassets/dokument/informationsmaterial/rapporter/nfc-rapport-2017-02_experiences-from-operating-the-rapidhit-system.pdf.
[40] *Id.*
[41] *See, e.g.,* Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. Times (Sept. 4, 2017) https://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques.html.
[42] 569 U.S. 435 (2013).
[43] *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2184 (2016).
[44] *See* FBI, *supra* n.25 (noting "familial searching is not currently performed at NDIS.").

surveillance" would largely target people of color.[45] Montana now requires a warrant for familial and partial match searches through its state DNA database.[46] Other states, such as California, that expressly allow for familial searching limit its use to unsolved criminal investigations where the crime is serious and "has critical public safety implications."[47]

Few rules have been put in place to govern other police practices such as searches of consumer genetic genealogy databases and the collection of DNA with or without a person's knowledge or consent. Montana and Maryland are the only two states that require a warrant to search genetic genealogy databases.[48] Maryland's law also places limits on law enforcement's ability to collect DNA from someone without their knowledge. And after reports that a police agency was collecting DNA from juveniles based on dubiously obtained "consent," California passed a law limiting the practice.[49]

VIII. CONCLUSION

We hope these comments assist OSTP in understanding the threats that continued government expansion of DNA collection and use pose to privacy and security, including particular harms to communities of color and immigrants.

If you have any questions, please contact Jennifer Lynch at [redacted].

Sincerely,

Jennifer Lynch
Saira Hussain
Electronic Frontier Foundation

---

[45] Maryland Public Safety Code § 2-506(d); DC ST§ 22-4151(b); James Rainey, *Familial DNA puts elusive killers behind bars. But only 12 states use it* (April 18, 2018) NBC News https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711.

[46] Jennifer Lynch, *Maryland and Montana Pass the Nation's first Laws Restricting Law enforcement Access to Genetic Genealogy Databases*, EFF Deeplinks Blog (June 7, 2021), https://www.eff.org/deeplinks/2021/06/maryland-and-montana-pass-nations-first-laws-restricting-law-enforcement-access.

[47] *See, e.g.*, California Dep't of Justice DNA Data Bank Program, Memorandum of Understanding Familial Searching Protocol, https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/fsc-mou-06142011.pdf?.

[48] *See supra* n. 46.

[49] Jamie Williams, *San Diego Police Target African American Children for Unlawful DNA Collection*, EFF Deeplinks Blog (Feb. 15, 2017) https://www.eff.org/deeplinks/2017/02/san-diego-police-targets-african-american-children-unlawful-dna-collection; Cal. Welfare and Institutions Code §625.4.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Electronic Privacy Information Center,
Center for Digital Democracy, and
Consumer Federation of America

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

[redacted]
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

joined by the

Center for Digital Democracy and Consumer Federation of America

to the

Office of Science and Technology Policy

Regarding the

Public and Private Sector Uses of Biometric Technologies

January 15, 2022

The Electronic Privacy Information Center ("EPIC") submits the following feedback to the request for information by the Office of Science and Technology Policy ("OSTP") on the public and private sector uses of biometric technologies.[1] We submit these comments to 1) stress the importance of robust, timely, and transparent impact assessments to mitigate the privacy and human rights risks of biometric technologies; 2) highlight the need for rigorous impact assessments that broadly consider the potential impact and apply to all biometric technologies; and 3) articulate key factors impact assessments should consider.

EPIC is a public interest research center in Washington, D.C. that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.[2] EPIC has a long history of promoting transparency and accountability of the technologies used in the private and public sectors.[3]

EPIC has a particular interest in promoting transparency and accountability regarding the use of biometric technologies and has consistently advocated for the need for safeguards related to the use

---

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56,300 (Oct. 8, 2021), https://www.govinfo.gov/content/pkg/FR-2021-10-08/pdf/2021-21975.pdf.
[2] EPIC, *About EPIC* (2022), https://epic.org/about/.
[3] EPIC, *Algorithmic Transparency* (2018), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System* (2018), https://www.epic.org/algorithmic-transparency/crim-justice/; Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet*, United Nations Educational, Scientific and Cultural Organization ("UNESCO") (Mar. 15, 2018), 5-6, https://epic.org/internetuniversality/EPIC_UNESCO_Internet_Universality_Comment%20(3).pdf.

of biometric technologies as well as the need to ban certain technologies or specific uses of those technologies. EPIC, through the Public Voice coalition, gathered support from over 100 organizations for a declaration calling for a moratorium on the further deployment of facial recognition for mass surveillance.[4] More recently, EPIC joined an open letter calling for a global ban on biometric recognition tools used for mass and discriminatory surveillance.[5]

I. Robust, timely, and transparent impact assessments are necessary to mitigate the privacy and human rights risks of biometric technologies.

Like all systems that collect and process personal data, it is imperative that biometric technologies only be introduced—if at all—after a robust and transparent review of the resulting risks to privacy and human rights. The process of evaluating technologies before their potential use is known as an impact assessment (or risk assessment).[6] An impact assessment is an analysis of how personally identifiable information will be collected, processed, stored, and transferred.[7] Properly executed, an impact assessment forces an entity to identify privacy and human rights risks of a proposed technology or application of a technology; to determine how and if those risks should be mitigated; and to make an informed decision whether the technology or application can be justified in light of its impact.[8] Impact assessments are mandated by numerous legal frameworks, including the E-Government Act of 2002,[9] the European Union's General Data Protection Regulation,[10] and the California Privacy Rights Act of 2020.[11]

It is essential that impact assessments for biometric technologies operate as true decision points and not as box-checking exercises used to legitimize foregone conclusions. As Professor Gary T. Marx writes, the object of a privacy risk assessment is to "anticipate[] problems, seeking to prevent, rather than to put out fires."[12] Accordingly, an impact assessment "is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project."[13] Moreover, an impact assessment "is not a time-restricted activity that is limited to a particular milestone or stage of the information system," but rather "shall continue throughout the information system and PII life cycles" and must be updated whenever circumstances "alter the privacy risks

[4] https://thepublicvoice.org/ban-facial-recognition/.
[5] Access Now et al., *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance* (2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.
[6] EPIC, *Privacy Impact Assessments* (2021), https://epic.org/issues/open-government/privacy-impact-assessments/.
[7] *Id.*
[8] *Id.*
[9] E-Government Act, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921–23 (Dec. 17, 2002) (codified at 44 U.S.C. § 3501 note).
[10] Commission Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119).
[11] Cal. Civ. Code § 1798.185(a)(15).
[12] *Privacy Impact Assessment* at v (David Wright & Paul de Hert, eds., 2012).
[13] *Id.* at 5–6; *see also* Office of Mgmt. & Budget, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf ("Agencies shall conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle.").

associated with the use of such information technology."[14] At all stages of this process, one realistic outcome of an assessment must be an institutional decision to substantially modify or abandon a proposed use of biometric technology based on the privacy and human risks it would pose.

Indeed, some forms of biometric technology—those who core functionality rests on invasive, nonconsensual, and unaccountable processing of biometric data—could not survive a robust impact assessment at all. For example, the privacy and human rights risks of emotion recognition systems cannot be justified or mitigated in view of the accuracy, bias, and privacy risks they carry.[15] So too with mass biometric surveillance tools,[16] including face surveillance.[17] It is essential that impact assessments be conducted early and with sufficient bite to prevent such biometric technologies from being deployed in the first place.

In many cases, an impact assessment also serves to inform the public of a data collection or system that poses a threat to privacy and human rights.[18] Requiring the prompt disclosure of impact assessments for biometric technologies will help ensure that each institution conducts a sufficiently rigorous evaluation of privacy and human rights risks; force the institution to justify the decision to introduce a given biometric technology; place the public on notice of the technology and how it will be used; and enable individuals and policymakers to respond to the technology before it deployed.

II. Impact assessments should apply to all biometric technologies and broadly consider the impact of the technology with thorough and detailed analysis.

Impact assessments should be triggered in all instances where biometric technologies are or will be used. Current implementations of biometric technologies should not be grandfathered in and thus allowed to avoid the requirement for an impact assessment. Similarly, seemingly non-controversial implementations of biometric technologies should not be exempt from an impact assessment requirement. A requirement for an impact assessment should avoid loopholes and exemptions that allow certain biometric technologies to avoid an assessment. A broad requirement that applies to all biometric technologies, including current as well as seemingly non-controversial biometric technologies, is more likely to identify potential issues.

The impact assessment requirement should extend to both the public and private sectors. Both government entities and private companies use biometric technologies and will no doubt look to expand their use of these technologies. Both sectors use biometric technologies in ways that create privacy, civil liberties, and human rights risks; disproportionately impact marginalized communities;

[14] Office of Mgmt. & Budget, *supra* note 13, at 10.
[15] *See* EPIC, *Feedback from: The Electronic Privacy Information Center (EPIC)*, European Commission ¶ 3 (Aug. 6, 2021).
[16] *See, e.g.*, Access Now, EPIC, et al., *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance* (2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.
[17] *See* EPIC, *Ban Face Surveillance* (2022), https://epic.org/campaigns/ban-face-surveillance/.
[18] *See, e.g.*, E-Government Act § 208(b)(1)(B)(iii) (requiring the publication of impact assessments by federal agencies).

and create opportunities for abuse.[19] The obligation to conduct an impact assessment should fall on all entities that use biometric technologies, including those entities that merely use a service that involves a biometric technology provided by a third party. For example, each law enforcement agency that uses the controversial facial recognition service provided by Clearview AI should be required to conduct an impact assessment in addition to Clearview AI itself.[20] Similarly, each airline and airport that uses the Traveler Verification Service that identifies travelers through facial recognition system managed by Customs and Border Protection should be required to conduct their own impact assessment before using the service.[21]

An impact assessment should be a thorough examination of the biometric technology at issue and include a serious analysis of the potential impact of the technology prior to its potential implementation. Too often an assessment requirement lacks teeth and becomes merely a lower priority box to check—one that is frequently checked after the fact instead of prior to the implementation of the biometric technology. This has often been the case with the privacy impact assessment requirement of the E-Government Act of 2002, particularly as it applies to the use of facial recognition technology.

The E-Government Act of 2002 requires government agencies to conduct a privacy impact assessment ("PIA") prior to "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form."[22] Despite this requirement, PIAs are often conducted after the fact if at all. Additionally, PIAs tend to narrowly construe the potential issues the technology raises and focus on justifying the technology instead of an honest analysis of its impact and whether the technology should be implemented.

For example, Immigration and Customs Enforcement ("ICE") began using the facial recognition services of Clearview AI almost a year prior to the completion of a relevant PIA in May 2020.[23] It's clear from the documents obtained by EPIC through the Freedom of Information Act that the DHS Privacy Office, which is generally responsible for making sure PIAs are conducted, was not initially aware that ICE was using Clearview, only asking to be briefed on its use in December 2019.[24]

---

[19] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *see also*, Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html;

[20] Clearview AI is a controversial facial recognition service that scrapes billions of photos from websites to create a massive biometric database used by hundreds law enforcement agencies. *See* Ryan Mac, Caroline Haskins, *et al.*, *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, Buzzfeed News (), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

[21] As part of the Biometric Entry-Exit program that uses facial recognition to verify the identity of travelers entering and leaving the country, Customs and Border Protection created the Traveler Verification Service, which can also be used by airlines to verify a traveler's identity during, for example, baggage check.

[22] E-Government Act § 208(b)(1)(A)(i).

[23] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's Walmart, and the NBA* (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[24] Email re: Clearview PTA (December 3, 2019) (obtained through the Freedom of Information Act), https://epic.org/wp-content/uploads/2022/01/EPIC-20-03-06-ICE-FOIA-Email-Clearview-PTA.pdf.

The PIA conducted by DHS regarding ICE's use of facial recognition services, specifically Clearview AI, lacks a meaningful assessment of the risks of a facial recognition database of billions of images indiscriminately scraped from the internet. The focus of the facial recognition services PIA is on ICE's handling of the photos the agency submits to Clearview AI or other providers of facial recognition services for searches and the results the agency gets back. The few impacts that the facial recognition services PIA does mention that are specifically created by Clearview AI's facial recognition database are chalked up as a "risk [that] is not mitigated" and more or less left at that. These unmitigated risks appear to serve no role in determining whether ICE should use such a service. Indeed, the facial recognition services PIA is not focused on whether Clearview should be used only on what the agency is doing to mitigate the narrow set of risks ICE is willing to address.

Another issue federal government PIAs tend to ignore, particularly with the use of facial recognition, is the disproportionate impact and racial bias inherent in these systems. For example, the Federal Bureau of Investigation conducted a PIA for its Next Generation Identification ("NGI") database that contains various biometric modalities, including images for facial recognition.[25] The images in the database that are used in facial recognition searches come from mugshots. It is well known that the criminal justice system disproportionately arrests and incarcerates Black people. Consequently, Black people are over-represented in NGI database of facial recognition photos. Additionally, facial recognition systems tend to be the least accurate on Black people. The PIA does nothing to address the issues created by using a system that has historic racial bias built into it. It is imperative that an impact assessment requirement necessitate the broad consideration of the impact of the biometric technology and thorough evaluation of the issues the technology raises.

III. Impact assessments should, at a minimum, consider several key factors related to the collection, use, dissemination, and retention of biometric data.

Although impact assessments should not be one-size-fits-all box-checking exercises, there are certain essential factors and categories an impact assessment must address. When assessing the impacts of biometric systems, the data at issue will always be sensitive.

Impact assessments must be sufficiently detailed and should consider several factors related to the collection, use, dissemination, and retention of biometric data.[26] The assessments should be able to generally indicate what type of regulatory intervention is appropriate for a given system.

Both the content and process of the impact assessment tool are hugely impactful. The assessments must be published, performed by someone with the requisite access and understanding of a given tool, and be legitimized through threats of fine or disgorgement if the assessment registers sufficient risk or is done inadequately.[27]

---

[25] FBI, *Privacy Impact Assessment for the [Next Generation Identification-Interstate Photo System*, (Oct. 29, 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

[26] *See* Dillon Reisman, Jason Schultz, Kate Crawford, Meredith Whitaker, *Algorithmic Impact Assessments: A practical framework for public agency accountability,* AI Now Institute (April 2018), https://ainowinstitute.org/aiareport2018.pdf.

[27] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021).

EPIC urges that impact assessments address the following minimum factors to prevent mission and function creep, needless over-collection of biometric data, and non-consensual processing of data:[28]

- Mission and function creep:[29] The stated purpose of the system, the allowable uses of the system, and the justification for adopting the system.
- Needless over-collection of data:[30] Information about the data collected for or by a system, including but not limited to the purpose for collection and the source(s) of the data.
- Lack of consent:[31] Information about data collection methods, including the scope of consent obtained (if any) and limitations on scraping.
- Failure to minimize:[32] Information about the management, retention, deletion, and transfer of data.
- Lack of transparency:[33] Information about the logic and development of a system.
- Lack of due diligence:[34] Initial tests regarding the accuracy and propriety of a system and information about ongoing tailored testing of a system. In addition to accuracy and propriety, audits and impact assessments must center civil rights, specifically testing for disproportionate impact based on race or other protected classes.
- Lack of accountability:[35] Any appeal procedures or harm mitigation strategies employed and information about key players, including the developer of a system, the user of a system, and the evaluators of the system.

In a growing number of countries, automated decisionmaking systems—including those that process biometric data—are required to undergo impact assessments. In Canada, for example, businesses input information about automated decisionmaking systems into a standardized survey, which allows for the evaluation of system based on design attributes, the sensitivity of data processed, and the system's connection to areas requiring additional considerations and protections.[36] This type of form could be used to collect and ensure uniform reporting of key information about biometric technologies and systems. The Canadian assessment asks each business to evaluate the stakes of the decisions that a system makes, the vulnerability of subjects, and whether the system is a predictive tool.[37] The tool also allows for multiple answer options and detailed explanations of responses. In

[28] *See* EPIC's comments on the California Privacy Rights Act (particularly the "scope of risk assessments" section, https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020/.
[29] *See, e.g.*, Arif Kornweitz, *A New AI Lexicon: Function Creep*, AI Now Institute (Aug. 4, 2021), https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-function-creep-1c20834fab4a.
[30] *See, e.g.*, Olivia Solon, *Facial Recognition's dirty little secret: millions of online photos scraped without consen*t, NBC News (Mar. 12, 2019), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] Necessary in large part because of demonstrated lack of accuracy and bias. *See, e.g.* Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Fairness Accountability and Transparency Conference (Feb. 2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[35] *Id*.
[36] Canada Digit. Servs., *Algorithmic Impact Assessment* (2021), https://open.canada.ca/aia-eia-js/?lang=en.
[37] *Id*.

some cases, the Canadian tool requires a business to identify the downstream processes of a system. This includes asking (1) whether the system will only be used to assist a decision-maker; (2) whether the system will be making a decision that would otherwise be made by a human; (3) whether the system will be replacing human judgment; (4) whether the system will be used by the same entity that developed it; and (5) for details about the system's economic and environmental impacts.[38]

Although impact assessments can't be the sole regulatory mechanism governing biometric systems, robust impact assessments *combined* with a system of governance that incorporates oversight and protects privacy and human rights can help regulators manage the risks that biometric technologies pose.

IV. Conclusion

We thank OSTP for the opportunity to comment on the use of biometric technologies and urge the agency to push for a meaningful impact assessment requirement as described in this comment. We look forward to working with OSTP in the future on these issues.

Respectfully Submitted,

[redacted]
Jeramie Scott
EPIC Senior Counsel

[redacted]
John Davisson
EPIC Senior Counsel

[redacted]
Ben Winters
EPIC Counsel

[38] *Id.*

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

FaceTec

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Introduction - FaceTec, Inc. (a Delaware Corp.) is the leading global provider of 3D Liveness and 3D Face Matching software for remote identity verification platforms. FaceTec's technology is currently used by U.S. federal and state governments, numerous foreign/sovereign governments, as well as hundreds of commercial entities to verify, enroll and reverify (authenticate) citizens, customers, and users. Examples include the Colorado Mobile Driver License, the Utah Mobile Drivers License, the U.S. Department of Homeland Security Mobile Trusted Traveler-related programs, the Canadian Parliament Remote Voting Verification System, and the United Arab Emirates Digital Dubai project.

Over 350,000,000 people on six continents have proven their Liveness remotely with FaceTec on smartphones, tablets, and webcams (including low-end & low-res devices), and with no observable age, gender, or skin tone bias. In 2022, FaceTec will enable well over 500,000,000 distinct 3D liveness checks globally.

To ensure real-world security, FaceTec operates the world's first-and-only persistent $100,000 Spoof Bounty Program, incentivizing hackers to attempt to beat its biometric security platform. It has successfully defended against over 105,000 bounty program attacks over the last 25 months, providing unmatched insight into the methods required to rebuff the most sophisticated threats to remote access management, identity proofing, and biometric verification systems.

We are proud to contribute a response. The White House Office of Science & Technology Policy RFI asked six broad questions. FaceTec's answers follow, with the questions the information pertains to listed in the header of each section.

Thank you.

1) Biometric Overview (Questions #1, #2, #5)

Biometrics is the measurement of data, usually digital, that was collected from unique personal physical attributes and can be compared to other like-kind biometric data. There are many biometric modalities, including fingerprints, face images, iris images, retina images, blood vessels images, voice recording, signature, behavioral, and DNA, among others. Biometric data can be used in several ways but is typically used in one of two ways, personal ***Identification***, and legal identity ***Verification***. Any biometric data can potentially be used for identification but only some biometric data can be used to verify a person's legal identity, and even fewer are effective at verifying a person's legal identity remotely. Moreover, biometric systems are designed for the collection of the biometric data, which to the subject, may be ***Voluntary*** or ***Involuntary***. The differences are not well understood by the public or media, and that is why education about this topic is critical to making informed policy decisions.

Identification is the process of connecting known data to unknown data from an individual, so that the identity of the subject can be known, or at least estimated with a probability. Identification answers the question "who is this person?". Identification functions compare the yet unknown biometric against a dataset of existing or known biometric data that has been bound to identity details, like name, for example. The software determines if a match or even multiple matches exist to any known identities at the given match confidence level. The process is often called a "one-to-many" match, or 1:N, and data collection for it can be voluntary or involuntary. There are many applications of 1:N matching. Law enforcement agencies "identify" involuntary suspects by comparing the suspect's fingerprints to databases of existing known criminal prints. Today, some government and commercial organizations collect biometric data (usually face images or video frames) from subjects, without permission, to be compared against criminal databases, simply to determine if there is a possibility that a criminal is present. Many believe this application raises privacy concerns. Conversely, employers screen voluntarily collected biometric data from job applicants using a similar software method to uncover potential criminal history during the job application process. In this case, the applicant volunteers to be compared to others in the database, eliminating privacy concerns. Additionally, stakeholders, like banks and e-commerce vendors, use identification and one-to-many matching to mitigate

identity theft-related frauds. Therefore, ethical ramifications of biometric systems hinge largely on the specific application and the voluntary or involuntary nature of the subject person's enrollment.

Verification is the comparison, for the purpose of confirmation, of two pieces of data that are presumed to be known. The stored, trusted biometric data of a vetted individual that has been bound to a legal identity, and the live biometric of a person claiming to be that individual. Verification answers the question for the relying party, "Are you who you say you are?" Verification is normally a voluntary action and is often referred to as a "one-to-one" match. Biometric verification is utilized in access control systems, like attempting to log in online after the enrollee's identity is established. Biometric Verification is becoming pervasive in remote and unsupervised networks, like the internet. The COVID pandemic highlighted the importance of remote user verification, as identity theft and online fraud exploded. The marketplace for verification applications that run on devices the general public already owns, is huge. When devices like PCs, laptops, and smartphones can be used as legal identity verifiers, identity theft and online fraud can be stopped almost completely.

2) Biometric Viability (Questions #1, #2)

Any biometric data can be used for either identification or verification. Fingerprints, handwriting, and DNA have long been used in law enforcement, because of their latency potential. Additionally, very many large government databases exist, containing face images. Police mugshots, driver license photos, passport photos, national ID card photos, and other credentialing applications are ubiquitous and rely on face image data almost exclusively. To follow, extensive academic research on fingerprint and face biometrics exists. The U.S. National Institute of Standards & Technology (NIST), along with many other research entities, have researched fingerprint and face biometrics for decades. Moreover, human beings have evolved to communicate by seeing, talking, and listening. Thus, the natural human interface, to computer systems, follows natural human evolution, including face and voice.

The existence of such infrastructure has several implications. First, there is a limited business case supporting the development of biometric modalities, beyond

face, voice, fingerprint, DNA, and signature. Second, substantial academic research exists for these established modalities, while limited research data exists for alternative biometric technologies. Given all this, it's likely that fingerprints, signatures, DNA, and face biometrics will remain the standard biometrics in law enforcement and forensic investigation, while face and voice biometrics will remain the standard modalities for commercial and civilian applications.

3) Probabilistic Biometric Match Outcomes (Questions #2, #4)

Biometrics can make two basic errors: False Match (FM), also known as **False Accept**, and False Non-match (FNM), also known as **False Reject**. False Accepts occur when the system mistakenly matches biometric data from different people. False Reject occurs when the system fails to make an appropriate match to the person who did provide both biometric data samples. A False Accept error could identify someone as someone they are not, setting the stage for a wrongful conviction or granting unauthorized access. A False Reject could fail to identify or verify someone, setting the stage to erroneously deny authorized access to privileges. Any of these errors could result in potentially catastrophic outcomes for individuals and society. Importantly, vendors with inferior technologies often tweak or skew their technology to minimize either False Accept or False Reject to artificially generate more impressive results in certain tests. Therefore, a better measure of a biometrics performance capability describes both False Accept and False Reject, relative to one another. Further, recent breakthroughs in face biometrics have substantially raised its potential utility beyond any other.

No biometric can ever be 100% accurate, because it is a derivative of the original biological human. Therefore, biometric matching relies on statistical probabilities. Biometric match results are probabilistic. To follow, increasing the amount of data, measured in a biometric match, increases the potential match accuracy and confidence. Regarding face liveness and biometric matching, there are two-dimensional systems (2D) and three-dimensional systems (3D). While 2D matching systems measure data from X, Y coordinates only, gathered from the 2D face image, 3D systems capture orders of magnitude more data, by measuring data from X, Y, and Z coordinates, as well as the 4th dimension, time, in some cases. Thus, 3D systems provide inherently and substantially higher potential Liveness and match confidence than any 2D system. This is why Apple adopted 3D for its

FaceID face authentication technology for the iPhone. Moreover, 2D face systems are subject to distortions in the image data that can confuse the matching algorithms and result in False Accepts, False Reject, and bias towards skin tone, age, and gender. Face distortions in 2D photos limit the potential biometric match confidence of 2D face matching systems. However, 3D face liveness and matching systems are not negatively impacted by perspective distortion, raising their match confidence levels far beyond 2D capabilities. FaceTec reports a false accept error rate of 1 per 12.8 million attempts, with a 1% false reject rate, orders of magnitude more confidence than 2D systems, and even more accurate 3D face matching algorithms are coming in 2022.

4) AI, Machine Learning and Bias (Question #4)

While biometrics have been researched and utilized for decades, AI used in conjunction with biometrics is relatively new. With that, the industry has observed some bias in AI-driven biometrics that can be corrected by ensuring correct system design and utilizing improved face biometric technologies.

There may be numerous sources of bias, but today, there are two largely recognized sources of such bias. The first regards AI itself and the training sets that are used to enable machines to “learn”. If the training sets are not sufficiently diverse, the AI will effectively learn to favor the perspective color of the training set. Thus, to advance inclusivity and mitigate skin color, gender, and age-based bias, the training set must be sufficiently diverse.

Second, 2D systems routinely gradient levels of light reflection, refraction, and contrast. Importantly, darkness is not a color, but the absence of light of any wavelength. Darker skin is darker because it absorbs more visible light wavelengths, rather than reflecting them to the sensor. So, 2D systems that rely on light reflection receive less data as the skin tone darkens. Thus, as quantities of light data fall with darker skin the potential for match accuracy is diminished. Similar biases can occur when a subject is wearing makeup, and with young children who have fewer unique characteristics on the skin, and thus any 2D system’s potential accuracy and confidence is less than a well-executed 3D system because with 2D there is simply fewer data to measure for all users, but that will negatively affect some users more than others

Conversely, 3D face liveness and biometric matching systems do not rely exclusively on gradient levels of light reflection, refraction, and contrast. Rather, 3D systems rely on the actual physical shapes of the face and related attributes. Thus, 3D does not present measurable bias, regarding skin tone, gender, and age.

5) Liveness, Spoofing, Honeypots, and Spoof Bounty (Questions #2, #3)

Liveness detection is a process to determine if a computer is interfacing with a live human, in real-time, and is most valuable in remote and unsupervised identity verifications. Liveness determines if it is a real, living person, while biometric matching determines if it is the correct, real person. Liveness detection mitigates many forms of presentation attacks, including photo presentations, deepfake videos, or mask replica presentations. Additionally, liveness must mitigate "camera bypass attacks", where hackers attempt to bypass biometric systems completely by injecting video images into the system that replace the legitimate images that would have been captured by the camera. Biometric spoofing and bypass attacks have become very sophisticated, as these examples demonstrate, https://liveness.com/#VendorsSpoofed.

Without robust liveness detection, biometric matching would be increasingly vulnerable to these remote fraud attacks. Therefore, biometric liveness detection should be considered a required, and primary, first line of defense to mitigate identity-related attacks.

There are various types of biometric liveness defense:

- **Active Liveness** commands the user to successfully perform a movement or action like blinking, smiling, tilting the head, and track-following a bouncing image on the device screen. Importantly, instructions must be randomized and the sensor/system must observe the user perform the required action. Active Liveness methods can stop unsophisticated fraudsters, but they will not stop knowledgeable hackers without many additional layers of security, that most active Liveness vendors do not possess.
- **Passive Liveness** relies on involuntary human traits like eye saccades, pupil dilation, skin texture, hair texture, reducing user friction, and session abandonment. Passive liveness only asks the user to "be themselves" and

thus, what a fraudster must do to successfully attack the system is more difficult to ascertain. This forces attackers to guess about what attack vector to use. When Passive Liveness is paired with 3D face data and camera feed security assurance it can determine if the biometric data is first-generation captured just moments before the analysis takes place, and not a presentation attack or injection of data that was previously collected. Significantly higher security levels can be achieved when the face images are captured securely with a verified camera feed, and the image data is verified to be captured in real-time by a device Software Development Kit (SDK). Under these circumstances, both liveness and match confidence can be determined concurrently from the same data, mitigating many potential vulnerabilities.

- **Multimodal Liveness** utilizes numerous liveness modalities. This often requires the user to "jump through hoops" of numerous active liveness tests and increases friction and session abandonment.
- **Liveness & Three-Dimensionality**. A human must be 3D to be alive, while a mask-style artifact may be 3D without being alive. Thus, while 3D face depth measurements alone do not prove the subject is a live human, determining that a spoof artifact two-dimensionality proves the subject is not alive. Regardless of camera resolution or specialist hardware, three-dimensionality provides substantially more usable and consistent liveness data than 2D, dramatically increasing accuracy, highlighting the importance of 3D depth detection as a component of stronger liveness detection.

More information on biometric spoofing and liveness is available at Liveness.com.

Today, there is much debate about the security implications of using biometrics. Some observers describe potentially catastrophic implications of moving biometric data from one device to a database and storing such data in a centralized database. A biometric honeypot is a concept describing the possibility that a centralized biometric database could be breached and its contents stolen. This could potentially compromise the victims' identities from that point forward. These fears can be mitigated relatively easily by utilizing properly designed cryptographic security systems. More effectively, however, if that biometric data was stored in an altered format, such that it could not be used to steal an identity, the hacker's motivation to breach the database and steal the biometric data disappears.

An identity verification system should be designed to accept only concurrently captured liveness and matching data within the same data flow. After liveness is confirmed, liveness data should be deleted. With that, the remaining matching data, lacking the required liveness data, would be rejected by the identity verification system upon resubmission. This would render the remaining biometric data unusable by a hacker, mitigating or even eliminating honeypot risk.

Conversely, designing identity management solutions to minimize the use, or even avoid biometric data creates significant vulnerabilities that have enabled some of the most notorious data breaches, including the Solarwinds breach. That vulnerability is known as "The PKI Fallacy". More about the PKI Fallacy is found here: https://youtu.be/Cp8EvCduvLU.

Industry standards, like those developed by the International Organization for Standardization (ISO) and The National Institute of Standards and Technology (NIST), might not address the most current types of spoof attacks. This is because, while hackers and cyberattack vectors evolve in real-time, utilizing the most current available technologies and techniques, technology standards must remain fixed for long periods. ISO standards, for example, once ratified, cannot be changed for five years. Thus, an ISO standard for Biometric Liveness, Presentation Attack Defense (PAD), and anti-spoofing capabilities could be several years old and remain mandated by various stakeholders. Moreover, certification laboratories, like iBeta, are frequently bound to certify vendor compliance and conformity to PAD-related standards that are not capable of defending against the most current spoof attack vectors, like deepfake puppets and bypass attacks. Despite this, many vendors today market such certification as evidence of their ability to defend against the most modern attack vectors. It is likely their customers, which may include government agencies, do not know their defenses are incapable of defending against attacks beyond an outdated standard.

Consequently, FaceTec has developed a $100,000 Spoof Bounty Program (www.spoofbounty.com) that invites hackers to attempt to penetrate the FaceTec 3D Face Liveness software. To date, FaceTec has defended against over 105,000 attacks over the last 25 months. FaceTec systems were spoofed only two times, allowing FaceTec to close those vulnerabilities while providing FaceTec with invaluable data to understand the most current spoof attacks. Consequently,

FaceTec routinely consults with and educates government and large enterprise stakeholders around the globe.

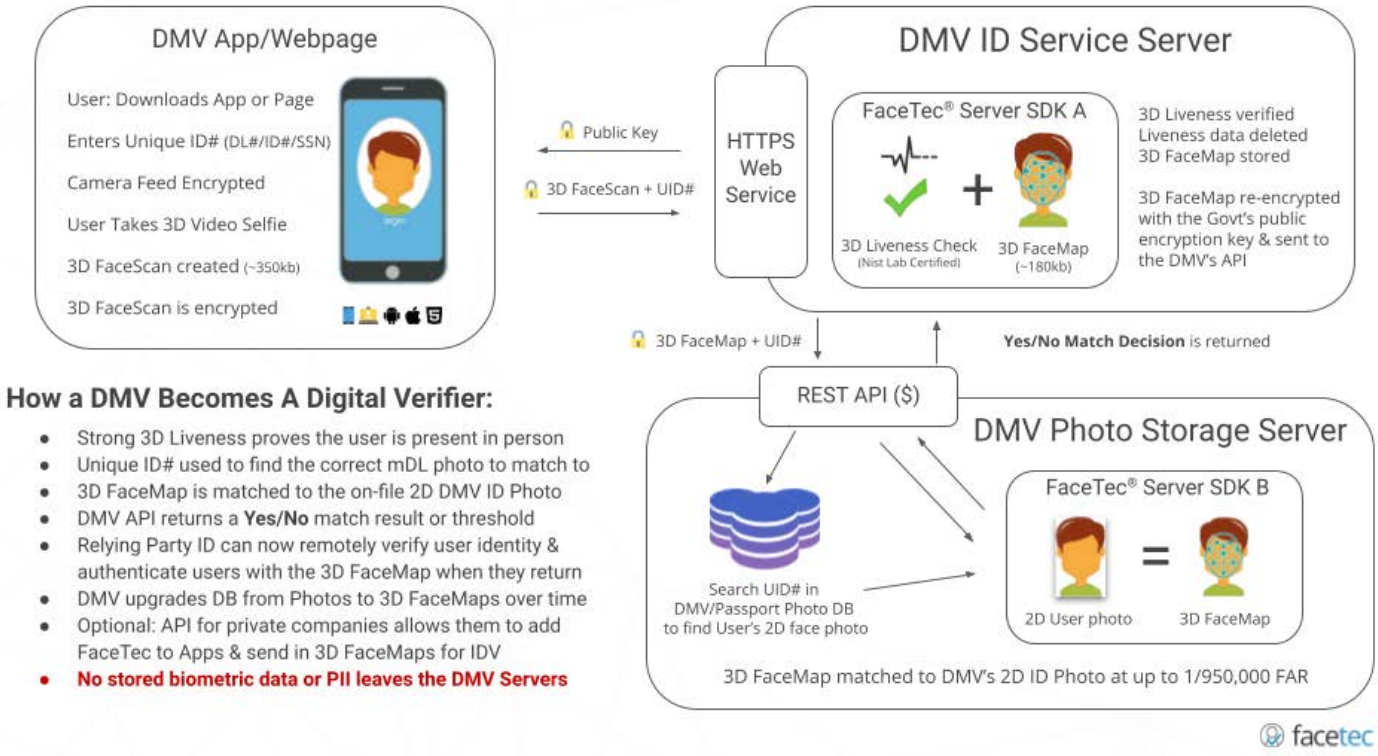
6) Government Trust Anchor (Questions #3, #5)

"You are who the government says you are". Birth certificates, social security cards (numbers), driver licenses, passports, Medicare and Medicaid cards, national IDs, among others, are government-sponsored, identity-related documents that we use to proclaim who we are in society. With that, government-sponsored identities represent the "anchor of trust" for society's identity verification needs. It makes sense that the government represents the best source of information to be used in identity management schemes, and is best suited to "vouch" for citizen identities.

Devices are not humans and humans are not devices. By binding a privilege credential to a device, without binding the credential to the appropriate identity, any identity management system is easily compromised. This is exactly the vulnerability that led to the SolarWinds breach. The vast majority of today's data breaches and online frauds exploit weak user authentication, associated with strong device authentication. Without strong, liveness-proven biometric user authentication, the strong credential/device authentication enables Advanced Persistent Threats (APTs), like SolarWinds.

By matching a liveness-proven biometric with the government-managed citizen identity profile (e.g., DMV or Dept of State database), that same biometric would be the ideal identity verifier for citizen and consumer identity-related needs. Taking a selfie can provide all the necessary liveness and biometric matching data necessary to instantly verify one's identity in society and marketplaces. All biometric data would reside behind the government firewall, yet be rendered unusable for resubmission, avoiding honeypot risk. A government identity verification submission would be compared to the biometric, bound to the civilian identity, and associated with a driver's license number or social security number. An API system would generate a binary "Yes" or "No", response. The relying party would receive the API response and accordingly approve or disapprove the transaction. The establishment and maintenance of such a root identity require secure remote human verification and authentication technology that did not exist until recently.

The FaceTec technical diagram informs subsequent business models for identity issuers around the world, follows:



How a DMV Becomes A Digital Verifier:

- Strong 3D Liveness proves the user is present in person
- Unique ID# used to find the correct mDL photo to match to
- 3D FaceMap is matched to the on-file 2D DMV ID Photo
- DMV API returns a **Yes/No** match result or threshold
- Relying Party ID can now remotely verify user identity & authenticate users with the 3D FaceMap when they return
- DMV upgrades DB from Photos to 3D FaceMaps over time
- Optional: API for private companies allows them to add FaceTec to Apps & send in 3D FaceMaps for IDV
- **No stored biometric data or PII leaves the DMV Servers**

Conclusion

Thank you for the opportunity to provide our insight into the current state of the market and art in biometrics, and proper citizen/user identity proofing, enrollment, and verification. More information can be found at www.facetec.com.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Fight for the Future

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Ban Dangerous AI

Dear Dr. Eric Lander and Dr. Alondra Nelson,

Thank you for the opportunity to submit comments on the community impacts of artificial intelligence. I strongly support the creation of an AI Bill of Rights as a first step towards protecting people against the harms of many AI tools. Beyond the development of this Bill of Rights, I urge the White House to ensure federal agencies, local and state governments, and private companies abandon–or never use–AI tools like biometric surveillance that violate our rights and deepen structural racism.

Systemic racism is often reflected in the outcome that an AI system is meant to predict, such as in criminal legal system uses, or in housing, employment and credit. For example, in February 2020, a report issued by the Student Borrower Protection Center found that a fintech lender abused borrower's educational and current employment data in its model, ultimately charging higher interest rates and loan origination fees for borrowers who attended Howard University, a historically Black university, or New Mexico State University, which principally enrolls Latinx students, when compared with a similarly situated New York University graduate [1].

Meanwhile, biometric surveillance and data collection are spreading rapidly in both private and public realms, creating unprecedented threats to privacy and safety. If we don't put an end to the proliferation of this tech, individual anonymity in public spaces will soon be a relic of the past. Instances of irreversible identity theft (i.e. theft of biometric data) will multiply, and systems of mass incarceration and violent policing threatening the lives of Black and brown people nationwide will continue to be strengthened. Civil rights campaigns to ban the use of facial recognition by law enforcement, airlines, retail stores, and other actors call attention to these dangers and more [2, 3, 4, 5, 6, 7].

Like nuclear or biological weapons, biometric surveillance poses a threat to human society and basic liberties that far outweighs any potential benefits. The only appropriate response to such destructive tech – and any other inherently discriminatory and invasive AI tool – is an all out ban [8]. I urge the White House to adopt such a position, and throughout the process of developing an AI Bill of Rights, to center those most harmed by these technologies.

Thank you.

References:

1. https://protectborrowers.org/educational-redlining-2/
2. https://www.banfacialrecognition.com/
3. https://airlineprivacy.com/
4. https://www.banfacialrecognition.com/stores/
5. https://actionnetwork.org/petitions/stop-corporations-from-mapping-kids-bodies-for-profit/?source=web-endchildsurveillance_an_stop-corps-mapping-kids-bodies_0521&
6. https://www.amazondoesntrock.com
7. https://www.baneproctoring.com/
8. https://fightfortheftr.medium.com/why-we-absolutely-must-ban-private-use-of-facial-recognition-98094736933

First name	Last name	ZIP code	Comments
Caitlin	Seeley George	[redacted]	
Milos	Stancic		
Leila	N		
Ryan	McCarthy		
William	Fisk		
Chris	Washington		
Marjory	Keenan		
James	Small		
Jess	DePew		
Cody	Goin		
Carol	Baier		
Jaclyn	Harris		
Joanne	Kaplan		
Karyn	Lebrun		
Kevin	Silvey		
Andrea	Schauer		AI is invasion of privacy!
Ann	Bein		
J.T.	Smith		

Marguerite	Rouleau	[redacted]	
Martin	Bouffard		
Riley	Canada II		
Libby	Esther Berman		
Michael Dean	Michel		
bernardo	alayza mujica		
John	Miller		
Meera	P		
Adam	Henderson		
Sean	Shannon		
Jesse	Szczygiel		
Sarah	Ninaud		
Stephanie	McFadden		
Jesse	Calderon		
Robert	Craig		
marissa	gonzalez		
Justin	Nafziger		Automation is a powerful tool, and AI a particularly potent expression of it. We need to be very careful what processes we allow to be automated and avoid those that magnify inequalities or strip away civil liberties. Collection of biometric data is a particularly problematic area for automation. The dangers of even a perfectly designed and implemented system are manifold. Meanwhile the systems themselves suffer from deep ongoing bugs that harm some of the most vulnerable among us. While the implementations are hidden from independent review by NDAs and claims of protecting IP while essentially strip mining our citizens for raw data resources converting them into the means towards corporate ends. All at the speed of automation. Uses of this technology must be transparent, open for public review, and rigorously regulated by all levels of government be they state, federal, or local.
marissa	gonzalez		
Elle	Lovelace		
Meghan	Prior		
Arthur	Ulam		
Sophia	Abramovitz		We have ample evidence from the use of existing internet technologies that tech companies cannot be trusted. The very business models used by high tech firms enable sale of our personal data. The algorithms used by these same firms are invasive, biased and discriminatory. Please consider the damage to our freedoms caused by unregulated technology.
Leslie	Smith		
Evan	Finkelstein		
Daniel	Howe		
Donna	Wagahoff		
B.	R.		
Marla	Feldhacker		
Liz	Tymkiw		
judith	zwarun		
Juli	Wood		
Diane	Parnell		
Michael	G		
LINDA	davis		
alexandre	julien		
John	Robinson		

Geraldine	Card	[redacted]	
Adedokun	Ojo-Ade		
Clifford	David Saffer		
william	watkins		
Lois	White		
Armando	A. Garcia		
Jesse	Caldwell		
Stefanie	Johnson		
Sue	Walden		
Dolores	Sloan		
Susaan	Aram		
Justin	Sorensen		I do not wish to live in a world governed by computers. Let's take the steps that we need to keep our freedoms safe from the tyranny of algorithms.
Nancy	Stamm		
Dennis	Keller		
Khang	Ong		
David	Malcolm		
Carrie	Miller		
Rev John	Long		
Marjory	Basso		
Jen	Bees		
patricia	orourkesteiner		
David	Williams		
Angelo	bagood		
Davindranauth	Shiwratan		
Joseph	Pitt		
Gaye	Detzer		
SHAWN	MEEKER		
Andrea	Templon		
Doris	Austin		
Terry	Reser		
Jean W	Hanson		
joshua	hoffman		
Kathryn	Burns		Strange times we live in. We have to worry that computers are invading our privacy. That's not acceptable.
Barbara	Luciw		Once again, don’t let big corporations dictate how the government is run. I’ m sure there is already a few politicians with their hands in the corporate pockets, looking to make a BUCK on the taxpayers.
STEVEN	Lebeck		BAN BAN BAN
Thomas	Knecht, MD, PhD		
Brandon	Perras		
Kay	Glinsman		
Alexis	T Langelotti		
Eric	Forney		1984 was a Warning NOT a manual !!
Erik	Schnabel		
Susan	Dickerson		
paula	moats		
Karen	Kirschling		
James	Babbin		
Jessica	Claudio DVM		

Mark	Giordani	[redacted]	
James	Stover		
Jason	Harris		
S	K		
Scott	Jeffers		
Michael	Bennett		
Jennifer	Hintz-Romano		
linda	redenbaugh		
Rosemary	Colson		
Timothy	Dunleavy		Constant surveillance is Unamerican.
Holly	Lloyd		Please, our privacy is important!
geoffrey	saign		
STEPHEN	HUTCHINSON		
Felicia	Chase		
Maggie	Louden		
Jerry	Shell		
Mike	Winget		
Suzanne	Hellums		
Doug	Bender		
Eduardo	Samaniego Amaya		
Elizabeth	Garratt		
Thomas	Blotz		
Christina	Raptis		
Scarlet	Balucan		
Viviana	Della Vecchia		
Jenny	North		
Steven	Christian		
Ramsey	Jammal		
Sarah	Hoffman		
Eric	West		
William	Crosbie		We cannot trust those trained solely in the intricacies of technology to have the best interests of society in mind. We get the tools and society we choose to allow. We need to halt the use of unchecked AI
Matthew	Falconer		
Jovohn	Hornbuckle		
Ava	Evans		
Reed	Williams		
John	Swanson		
Raymond	Intemann		
Renee	Villanueva		
Jody	Gibson		
Steven	Sy		
John	Simmons		
Byron	Connell		
John	W Thompson		
Gennete	Saciri		
Wayne	Langley		
Jean-Pierre	Moundou		
Benjamin	Barajas Jr		

Deborah	Williams	[redacted]
Kevin	Morris	
Russell	Novkov	
Jayne	Cerny	
Aleksey	Gurtovoy	
B.	E.	
Lauren	Murdock	
J	Davis	
Dennis james Sagu	Parker+	
Janette	Reid	
Noel	Parenti	
Chris	Stockinger	
Ibn-Umar	Abbasparker	
G D	Abbott	
Britta	Fischer	
Matthew	A.	
Evan	McDermit	
A	beato	
Melissa	Lawrence	
Joann	Pfeifer	
Carl	Meyer	
Martha	Riggle	
Felicia	Wright	
Lynn	Pooley	
Renee	Clark	
ADRIANNA	SUTHERLAND	
Leslie	Irlanda	
Karen	Laakaniemi	
Nidia	Santana	
Dean	Swaydan	
Kelsey	Rust	
Bonnie	McGill	
Giannie	Couji	
Nancy	Johnston	
Carlos	Arnold	
Candace	LaPorte	
Ben	Wegley	
Eva	Suhr	
Chris	Kermiet	
Jeannie	Finlay-Kochanowski	
Gayle	Price	
Angela	McClendon	
Sonia	Goldstein	
Patricia	Auer	
Stacie	Dullmeyer	
Jane	Simpson	
Emily	Bryant	

Karin	Kellam	[redacted]	Part of our inherent right to life, liberty and pursuit of happiness is having the right to our privacy. Unless there is strong probable cause that someone has broken a law, these corporations need to keep their spyware out of our households and communities. I don't even use my real name on grocery store membership cards because it's nobody's damn business what kind of toothpaste I buy. We don't want the USA to be like the East Germany of old where they kept files on their citizens. Creepy.
Natalie	Santana		
Diane	Olson Schmidt		
L.	A.		
Joyce	Heyn		
Clarence	Harper		Everyday, there is a new story of "smart" systems doing real harm. Systems supposedly without bias carry the biases of their creators, and act as a convenient crutch, an excuse for continuing institutionilized inequity. Never in history have private entities, beholden only to themselves, had so much power. We need to put the brakes on it.
Kerry	Velazque		
Ellen M	Forrest		
Jeaneen	Andretta		
Mo	Kafka		
Valeria	Castaneda		
Sheryl	Iversen		
Tana	Cahill		
David	Ringle		
Sylvia	Vairo		
Tara	kerksick		
Andrew	O Fragale		
Beverly	Kubachka		
Tracey	Katsouros		
Elak	Swindell		
Kathe	Garbrick		
Jodi	Rodar		
Nuredeen	Bhanji		
Jeremy	Spencer		
Judith	Ford		
Erik	Moss		
renee	Carl		
Marilyn	West		
Morgan	MacConaugha-Snyd		
George	Dugan		
Sheila	T.		
robert	clark		
Timothy	Mullen		
Andrew	Geisler		
Samone	Jones		
Kristin	Kokal		
Jane	Wiley		
Jamie	Thomas		
Evelyn	Griffin		
Coree	Spencer		
Tim	Carrigan		
Joan	Farber		

V	Evan	[redacted]
William	McGunagle	
Matanga	Matanga	
Matthew	Gonzalez	
ruth	Cary	
stephanie	edwards	
Mike	Montes	
Skylar	Safholm	
Murray	Kaufman	
Mari	Mennel-Bell	
Mandy	Tshibangu	
Klaus	Schreiber	
Aileen	Taylor	
Shirlene	Harris	
William	Meneese	
Sara	Keesling	
Camille	LoSapio	
Marla	Berry	
Josias	Berganza	
Helen	Stuehler	
Todd	Clark	
Crystal	Smith	
Barbara	Shenton	
Marilyn	Matthews	
J.D.	Capece	
L.L.	Wilkinson	
Elizabeth	Enright	
Sharon	Baker	
Debbie	Schepis	
Tommy	Lewis	
Sheena	Hill	
Tony	Milano	
Gail	Fleischaker	
Rochelle	La Frinere	
Roberta	Moore	
Michael	Klausing	
Klaudia	Englund	
Michele	Paxson	
Mark	Meeks	
Lynne	J Berg	
Veronica	Schweyen	
Ginny	Nolan	
Louise	Krus	
Crystal	Smith-Connelly	
Beth	Norwood	
Charles	Schafer	
Benjamin	Alonso	
Jacqueline	Mills	
Kathe	Garbrick	

Barbara	Buck	[redacted]	
Scott	Baker		
Guy	Zahller		
Peter	Brunner		
Esther	Weaver		
Robert			
Lorne	cheeseman		
Aaron M	Vernon		
Michelle	Remite-Berthet		
Randy	Lauritzen		
Lisa	Ragsdale		
Darryl			
Patricia	Harris		
Tithi	Dutta Roy		
J	FRIED		
Steven	Hester		
Jesse	Bohl		This is not the only thing tech is digging out of us: personal info, clicks, on line history, etc. All of this is a violation of us for the sake of multi-billionaire fat pockets.
Eric	Crouch		
Jennifer	Gildred		
Ellen	Rice		
janna	piper		
Elaine	Linet		
Dan	Heffernan		
Ira	H		
Kathleen	Mireault		
Judith	Fonsh		
B.	Robinson		
Lorne	Beatty		
Larry	Lewis		
Richard	Pihlgren		
Noah	Ertz		
Lorna	Fortune		
Karla	Hinton		
Irving	Lee		
Pat	Reese		
MJ	Cittadino		
Dale	F Haas		
Timothy	Coughlin		
Geraldine	Booth		
Mark	Farrow		We deserve our privacy
Bre	Cleary		
Karen	Sewick		
Patricia	Sherman		
Emma	Miniscalco		
Edward	Laurson		
Rebekah	King		
David	Pyle		

Larry	Rolfe	[redacted]	
Leanne	wolf		
Winifred	Poster		
Louise	McClure		
Peter	Mueller		
Curtis Walter	Walter		
Max	Salt		
Alexis	Lamere		
Davis	montalvan		
Dash	Porter		
Lynn	Perry		
Barbara	Abraham		
Caryn	Graves		
Mark	Gotvald		
Cindy	Hwang		
Karen	Lein		
Rebekah	Williamson		
Joe	Joyner		
Stefanie	Weisgram		
Vaida	Mal		
Patricia	Harlow		
Marvel	Stalcup		
Anime	Rakurai		
Katie	Schultz		
james	richmond		
Gayle	Edelman-Tolchin		
Ryan	Wilke		
Ruth	Yurchuck		
Marvel	Stalcup		
Lori	Silverberg		
Joseph	Henderson		
Eric	Garcia		
Andrew			
Linda	Gonzales		STOP the systematic killing of our world.
Amber	Mott		
Marvel	Stalcup		
Sandra	Dean		
Lisa	D'Ambrosio		
Tony Cho	Dwyer		
Melissa	Beaudet		
toby	tarnow		
Lisa	Simms		
Prisca	Gloor		
Ruth	Pouliot		
George	Curti		
Dominique	Edmondson		
Elizabeth	Castro		
Joe	Nolan		

Tamara	Matz	[redacted]	
Annetta	Winkle		
Lynda	West		
Michael	Howard		
Trish	Webb		
Elaine	Donovan		
Raymond	Berrios		Tell the White House Ban Dangerous Ai
Janet	Yoshida-Gordon		
Tami	Hillman		
Risa	Schiff		
Terri	Rose		We must look out for unforeseen threats
Nancy	Limpar		
Kathy	Rice		
Colleen	Lynch		
Timothy	Studt		
Brian	Schwartz		
Allen	Daniel		
Laura	Neiman		
Mira	Bhayroo		
Tina	Krauz		Protect the people of this nation, please.
Lori	Silverberg		Please address this important issue!
Paula	Fenda		
Molly	Swabb		
Scott	Miller		
Jerry	Mawhorter		
Judy	White		
Amanda	Summers		
Eric	Scheihagen		
George	Cornwall		Get these damn algorithms out of social media
Phyllis	Bottoms		
Hazel	& Hyman Rochman		
Cathy	Carleton		
Barbara	Ardinger		
William	Welkowitz		
King	Schoenfeld		Invisible control is the worst!
Bertha	Guzior		
sam	hill		
Dorothy K	Miller		
Christine	Roane		
Ree	Whitford		
Paul	Kindel		Place much better controls on Social Media!
Jean	Pressoir		
Rebecca Wish	Esche		
Anthony	Miragliotta		
Gina	Sager		
melanie	dieringer		
Stefanie	Siegel		
Irene	Franck		
Nancy	Stafford		

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Ganesh Mani

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

AI Bill of Rights must be a bridge from the original Bill of Rights to modern times.

Ganesh Mani, PhD, MBA
@NetThoughts
(Disclaimer: The views expressed here reflect citizen Mani's current individual outlook and should not be construed as the official position of any institution he is affiliated with. Also, his views are bound to evolve based on further dialog with affected groups, policymakers, other technologists and citizens.)

First Amendment. A great conception conferring freedom of religion, speech and expression, assembly as well as the right to petition.

The Supreme court, roughly a century ago (in Schenk v. United States), highlighted that the most stringent protection of free speech would not protect a man for falsely shouting fire in a theatre and causing a panic. Today's social media allows thousands of people to "shout fire" in multiple geographies, simultaneously! With the potential to cause widespread panic. The new AI Bill of Rights must recognize, clarify and address this increasingly common use case.

Second Amendment. The right of citizens to protect themselves by "bearing arms." Own deadly weapons such as guns. Today, the proliferation of guns has also resulted in gun-toting policeman responding to minor traffic violations, domestic (family) disputes and petty financial crimes. George Floyd was apparently trying to foist a questionable twenty-dollar bill at a neighborhood convenience store, when a small squad of armed policeman were summoned. Facial recognition plus offline forensics by a detective would have been a graceful way to handle it. Sidestepping the tragic outcome!

The list goes on. Technology has evolved and societal behavior has changed. The recent pandemic has also brought some behavior changes into focus. Citizen rights, their protection as well as broader societal implications must evolve to reflect the new reality and contemporary, quotidian use cases.

I have previously alluded to the "AI is Fire" metaphor.[1] Fire extinguishers are commonplace and firecrackers are regulated; nuclear codes are safe-guarded and multi-national treaties often govern part of our arsenal. Human experience with fire – the good and the bad – can and should guide some of our thinking.

The world is global, digital and work, play as well as living patterns continue to evolve. The world is also becoming increasingly algorithmic; algorithms nudge us – including children – in many quotidian activities. Digital twins embedded in the metaverse will soon became a reality for many people; this raises additional thorny issues. The US AI Bill of Rights must further reflect the new landscape as citizens go about their daily life.

Design thinking can perhaps be brought to bear on this issue; it telegraphs a citizen-centered approach to innovation, melding a) the needs of the people, b) the opportunities and

possibilities afforded by the technologies; and c) the requirements of national security and success.

Biometrics

Biometrics involves establishing identity or recognizing "who" based on physical (but can be extended to behavioral) traits. Its history can be traced back to the Habitual Criminals Act enacted by the British Parliament in 1969, to trace and track repeat offenders. [2] In the modern era, biometrics are in everyday use (e.g., on one's smartphone), yet controversy arises due to its fallibility and unintended or borderline illegal uses.

Dimensions to keep in mind (when greenlighting the use of Biometrics) include the error rates, brittleness and bias, privacy issues and explainability. For example, facial recognition is more error prone than methods based on fingerprints and irises. Mistakes have received significant attention in the press.[3]

More questions than answers

Our country and its citizens now need to be protected from bio and cyber warfare, not just kinetic wars. Biometric and other AI technologies need to consider many interesting use cases around this. For instance, citizens are continuing to work from remote locations, including overseas, with workstyles altered considerably by the pandemic.

The AI Bill of Rights must reflect

- That biometrics can be immensely useful
    - In many scenarios (the high-profile George Floyd case, alluded to earlier, comes to mind), but needs guard rails (incl. to prevent, for instance, accidental exposure of data – encryption is necessary, but not sufficient)
    - for triage (along w/ other AI techniques) – to decide whether to summon a law enforcement officer, a social worker or a reconnaissance expert.
    - by introducing people or traffic flow efficiencies (e.g., while boarding a plane, at a toll booth). While opt-in frameworks are suggested, care must be taken to make sure the folks opting out do not make the overall value-added futile. A tricky exercise to get the balance right.

- That citizen trust and access are important (as we experienced recently with vaccines).
- Global cooperation, to the extent possible, especially among democracies. Keeping in mind that democracies come in many flavors, much like apples and mangoes. A patchwork of inconsistent global regulations will make digital platform usage inefficient and costly. Digital public goods, many with a global scope, are becoming increasingly important.
- Personalization and accommodating persons with special needs (e.g., alternative biometrics, a non-biometric mechanism to establish identity).

- Emerging metaverse issues (e.g., linking physical identity with avatars, the role of law enforcement in the metaverse).
- While it might perhaps be benign to shout fire in a crowded metaverse theater, coordinated cyberbullying and other toxic behavior may have to be addressed.

This opinion brief is meant to spark thought by asking questions and exposing additional use cases. Arriving at a good set of principles Is difficult, but paramount. Legislative or executive action should not be thought of as abridging the traditional Bill of Rights but providing a robust bridge to modern, free, fair and prosperous times, via the AI Bill of Rights. The mantra should be: Of the people, by the people *with machines*; for the people!

References:

1) Mani, G., Chen, F., Cross, S. ., Kalil, T. ., Gopalakrishnan, V. ., Rossi, F., & Stanley, K. (2021). Artificial Intelligence's Grand Challenges: Past, Present, and Future. *AI Magazine*, *42*(1), 61-75. https://ojs.aaai.org/index.php/aimagazine/article/view/7375
2) Jain et al. Biometrics: Trust, but Verify. https://arxiv.org/pdf/2105.06625.pdf
3) https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html
4) https://press.uchicago.edu/ucp/books/book/chicago/P/bo14007600.html (Werner Troesken's book "The Pox of Liberty").

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Georgia Tech Research Institute

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Georgia Tech Research Institute
250 14th Street, NW
Atlanta, GA 30318
https://gtri.gatech.edu/

Respondent Type: ***Academic Institution (University Affiliated Research Center)***

Technical POC: Dr. Craig Arndt / Principal Research Faculty
Electronic Systems Laboratory
[redacted]

Information Requested: Respondents may provide information for one or as many topics below as they choose. Through this RFI, OSTP seeks information on the use of biometric technologies in the public and private sectors, including on the following topics:

General Comments:

Biometrics are based on good science. However, like any other science, there are limitations to how the science is applied. In order to understand and characterize the limitations of biometrics as a science and in specific applications, it is critical that the system is decomposed into its constituent parts and each part is well-described analytically.

Biometrics as a class of technologies is not inherently an AI-embedded class of technologies. Biometrics existed long before Artificial Intelligence (AI) or even computers existed; e.g., fingerprinting as a forensic science has been used extensively since the 1880s. In many ways, more importantly, humans have used biometrics (e.g., face, voice, and gate) since the beginning of recorded history. The way the human brain recognizes other humans has influenced our understanding of biometrics for many years. It is important to note that biometric applications do not operate the same way that the human brain operates. Furthermore, the portrayal of biometrics through media and entertainment is often inconsistent with the realities of the technologies.

A number of biometric systems do use AI algorithms, and this is an artifact of the fact that AI algorithms are well suited for many classes of image processing, and that image processing is a key part of some kinds of biometrics, including voice recognition systems.

Because of the complexities of AI systems, they often produce matching or other decision results that are not easily understood by humans interpreting the outputs. Consequently, the development of explainable AI is a high priority for a number of government agencies including the Department of Defense. Biometric applications of AI are explainable, and every effort should be made to maximize operational explanations of how exactly biometric systems work. Further, intellectual property rights and considerations are sometimes limiting factors in biometric algorithm expandability. IP rights and expandability should be major considerations in the development of governance. Biometrics are used extensively across government and industry. In order to correctly make policy in regards to the use of biometrics, it is important to understand the key elements of biometric systems and how the different parts of the system contribute to the

performance of the system. The key components of biometrics as a science and as a technology are the following:

Biological differences: Each human has specific biological characteristics that are created through random developmental processes (e.g., irises and fingerprints), heredity (e.g., DNA), and other factors. What is important is the amount of information the biology provides to the system. Some biological indicators have a lot more information than others and some are more consistent than others. For example, DNA is both data rich and very consistent. Face recognition has less data and is less consistent.

Feature definition: Feature definition is a technical process that takes the biological indicators and converts them into computable data that can be input into matching algorithms.

Matching algorithms: The matching algorithms are used to determine an identification match. Neither feature definition nor matching algorithms are perfect and have some degree of accuracy issues.

Manual verification: Many implementations of biometric systems are computer-aided applications. That is, the computer makes recommendations to a human operator who then makes final decisions about matches. This is common in law enforcement and national security applications. Performance of man-in-the-loop systems can suffer from accuracy issues for both the computer systems and the human operators.

Specific application: Lastly, the specific application has a lot to do with the reliability and accuracy of any biometric system. Small changes in how a biometric system operates can radically change its reliability, performance, and intrusiveness.

National Defense and law enforcement applications It is important to note that in the 21st century, the use of biometric systems is critical to achieving and maintaining national defense and rule of law at its current rate of effectiveness. The loss of this technology as a tool for national defense and law enforcement would have significant impacts to the safety of the United States. It is clear that the adversaries of the United States and our international competitors will not limit the use of biometrics for their own national security in any meaningful way.

Given the complexity of biometrics and their criticality to national security and rule of law, it is required to ensure that policy decisions are informed by technical experts and by a clear understanding of the specifics of the applications. As a result, decisions about the use of biometric technology should be made in direct consultation with engineers and other technical experts with a deep understanding of the technology.

1. **Descriptions of use of biometric information for recognition and inference**: Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

Comments:

a) The use of traditional biometrics for identification and verification of identity to control access and enforce security will continue to grow in both the national security and commercial application spaces.
b) The traditional application of biometrics for surveillance will grow in the commercial sector as companies recognize the value of data on people movement.
c) In the past few years the technology has advanced to a point where the use of biometrics for inference is reliable and cost effective to a point where it is viable for commercial applications. This data can and will be used for both customization of services and for customization of influence. We can expect that industry will grow its use of biometric technology for inference significantly in the next 10 years. The data collected for inferencing can and will be used by a variety of Artificial Intelligence algorithms to influence people in using marketing and other influencing methods (targeted presentation of data) in a highly individualized and targeted manner.

2. **Procedures for and results of data-driven and scientific validation of biometric technologies**: Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

Comments:

a) Validation of the performance of biometric systems and their use in an ethical manner are both important and required to protect the rights of people and the availability of biometric systems to law enforcement and national security applications.
b) The use of AI and other non-liner algorithmic methods as well as the very large data sets that are often used in the development and operations of biometric systems makes these systems very difficult to test completely. As noted in many studies and earlier in this response, the complexities of biometrics require us to look at and validate more than just the aspects of biometric systems. Complete verification and validation require: i) validating the performance of the science and algorithms, ii) validating the design and application of biometrics to a specific system or purpose, and iii) validating the risks and benefits of that systems in their intended use.
c) Currently, the most complete testing of biometric testing being conducted is being done by NIST, the National Institute of Science and Technology. This testing should continue and be expanded to increase its usefulness across technologies, modalities, and applications.
d) Currently the Department of Defense has a very robust model for the development and execution of developmental and operational testing. There are processes used to ensure the performance and safety on weapons used by the military that could also be used as a model for an independent test agency to define and conduct testing of both government and commercial biometric applications.

e) Finally, a risk-based, comprehensive method for biometrics benefits analysis needs to be created and administrated by an engineering and science-based government or non-profit organization to ensure that promised benefits are achieved and risks and harms investigated and mitigated across the multitude of biometric techniques and their use in combination with one another.

3. **Security considerations associated with a particular biometric technology**: Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.

Comments:

a) Biometric security systems and the securing of biometric input signals and images from cyber-attacks have the same issues as any computer system. Like any other computer-based system, appropriate levels of cyber security protection need to be put in place for any biometric system.
b) Much has been made of potential issues with the loss or compromise of biometric images and or biometric templates. It has been said that, unlike passwords, a person only has one set of fingerprints, and only one face, and once the template is compromised it is a significant security issue. Although this is very much true, current methods for generating biometric templates has completely mitigated this issue. In the same way solutions have been found and implemented to overcome many other widely publicized biometric security threats from masks, and other methods to defeat biometrics (e.g., gummy fingers).
c) Biometrics, contrary to what has been propagated in the media, are fundamentally security- and privacy-enhancing technologies. Biometric based security systems also enjoy two critical advantages over traditional computer-based security. First, biometric tokens can never be forgotten, can be as complex as the security application requires, and do not need to be written down. Second, a properly implemented biometric system offers positive attribution of who is accessing the application, where, and when.

4. **Exhibited and potential harms of a particular biometric technology**: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

Comments:

a) When looking at the possible harm from biometric systems, it is critical to understand that the technology itself is incapable of doing harm. What biometric technologies can do is tell their operators things about images and signals. As has been noted here, biometric applications can be designed to recommend several classes of results. First, they can provide positive identification. Positive identification reports the identity of an individual based on an assertion of identity or a question of identity ("Who is this?"). Negative identification, on the other hand, is the question of whether a person is not in a group of interest. An example of this is the "watch list" application. In both positive and negative identification tasks, the accuracy and the performance of biometric systems can be measured and any harm can then be documented based on the performance of the system.
b) Inference applications on the other hand are not as clear or easy to measure. Inference applications attribute feeling or intentions to individuals based on biological indicators. The performance and accuracy of these inference biometrics are not anywhere near as accurate as traditional applications that verify identity.
c) Potential harm coming from the use of biometrics can take two possible forms. The first is in the performance / accuracy of the biometric system, and second for the improper use of the technology. Harm can be intentional or unintentional. There are few cases in the United States of biometrics that are designed to be intentionally harmful to the subjects of the system. Intentional harm created by a biometric system is generally easily seen and mitigated in many ways. On the other hand, unintentional harm exists in many systems all around us. Preventing unintentional harm requires an understanding of the engineering design of the application and its intended use. Unintentional harm can come from issues with the accuracy or performance of the system, the reliability of the system, or in bias in the design of a biometric system. There are generally three major categories of unintentional harm that result from poor design or incorrect use of biometric systems. The first is incorrect or inappropriate action taken by the operator of the systems as a result of an incorrect biometric match. This can take many forms based on what the specific function of the system, either government or commercial, may be. The second category of harm involves the loss of privacy. In this case, the security design of a biometric system needs to guard against the loss of privacy. The last major category involves the loss of anonymity. People expect the ability to come and go and live their daily lives without a) having to prove their identity unnecessarily and b) not have their every move, action, and interaction with others monitored, recorded, and correlated. Biometric technology offers both commercial entities and government to collect and manage this data about people.
d) When they build a system, any good engineer or designer evaluates the performance of the system and, to the extent they know the application of the system, they mitigate any potential harm that the system they design may cause.
e) In order to ensure that biometric systems are both reliable and unbiased requires extensive testing of these systems and transparency in their design and operation. Currently, there is little testing or transparency in the commercial use of biometric systems. Both commercial and government use of biometric systems need greater visibility and more testing in order to improve performance and to increase the public confidence with respect to their usefulness.

f) In order to proactively deal with potential unintentional harm from poor performance or bias in biometric systems, standards for performance, testing, and transparency must be established and good designs produced and reviewed by licensed (professional engineers, for example) professionals.

5. **Exhibited and potential benefits of a particular biometric technology**: Consider benefits including, but not limited to: Benefits arising from use in a specific domain (absolute benefit); benefits arising from using a specific modality of biometric technology (or Start Printed Page 56302 combination thereof) compared to other modalities in a specific domain (relative benefit); and/or benefits arising from cost, consistency, and reliability improvements. Information on evidence of benefit (in the case of an exhibited benefit) or projections, research or relevant historical evidence (in the case of potential benefit) is also welcome.

Comments:

a) The availability of biometric data sensors continues to increase in the US and across the world. The primary biometric sensor is the digital camera. The use of internet connected digital cameras and audio devices are common, both in public places and more so in homes. Also, the reliability and accuracy of biometric systems continue to improve. With these improvements in performance, security applications of biometrics significantly benefit a wide range of users.
b) Commercial application of biometrics allows for data aggregation and personalization of services. The large amounts of data about citizens collected can provide a wide range of services, customized to the individual needs and wants of the customer.
c) With the growing availability of these new technologies, there will be a wide range of future applications. Some of the most interesting new applications will include a new class of application looking at "user state." These applications help monitor a wide range of emotions and medical conditions.

6. **Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case**:

Comments:

a) Governance is critically important at this point in the life cycle of the technology. The process of governance will involve the development of policy, process, regulation, and law. However, the biggest issue in governance is trust. Unfortunately, trust is a function of many things, a good deal of which are not based on truth about the technology. Biometrics have suffered from misrepresentation in the press, movies, and other media. All governance must be based on the best possible science and engineering.

Information regarding:

- Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;

Comments:

b) Stakeholder engagement is critical for any governance; however, it is critical that the governance that the US government is currently considering for the biometrics industry prioritize the interests of the people of the United States. There are a lot of vocal stakeholders whose interests are different than the interests of the public. Commercial industries' (e.g., the major electronics and social media companies) interests are based on profitability and many undisclosed interests including the collection and control of personal data on as many people as possible. Additionally, there are a number of activists whose interests are based on specific political agendas.

c) The interests of the US public are many faceted. Their interests fall into five major categories, including: safety, security, privacy, access to services, and non-discrimination.
   - Safety: Law enforcement is critical to establishing safety and rule of law. The correct use of biometrics (e.g., fingerprint, face, and DNA) is critical to physical evidence and accountability.
   - Security: The security of the nation is in the interest of all citizens, and biometrics is an important tool of national security and the intelligence community.
   - Privacy: Individuals have an interest in their privacy. Although biometrics are not inherently an anti-privacy technology, many applications of the technology, if not used correctly, can encroach on privacy.
   - Access to services: One of the most prevalent applications of biometrics is to use identity to customize a wide range of services.
   - Non-discrimination: Non-discrimination is an absolute requirement and can be achieved through careful technical planning and testing.

   By doing careful design and testing the biometrics community can meet all of these objectives. These interests should be the only factors traded against each other and not political agendas or profit.

- Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

Comments:

d) The development of best practices in the field of biometrics is already under way. In December of 2020, the Federal ID community published a community-developed document, Biometric Face Recognition: References for Policymakers (https://www.mitre.org/publications/technical-papers/biometric-face-recognition-references-for-policymakers) This document should serve as a guide to the development of biometrics policy.

- Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;

Comments:

e) The industry has yet to create a way to perform meaningful informed consent. This is one of the most important issues that needs to be resolved as part of any governance. Because individuals do not know or understand how their data is used in the present or the future, new ways of creating consent will need to be developed. If the public doesn't understand how their data is used then informed consent is meaningless. In addition to informed consent, data sharing and data retention must be addressed. In order to resolve these critical issues policy needs to be created to ensure that people are properly informed of the use of their data, not once but every time it is used, shared, or aggregated (e.g., grouped or linked). There are technical means to implement safeguards to data use without informing the data subjects.

- Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;

Comments:

f) Informed consent is only one of the critical aspects of biometrics safeguards. In addition, testing is critical to ensure that bias is not introduced into biometrics applications. However, if informed consent is implemented correctly, with both legal and technical safeguards, then the users will be enabled to regulate the industry themselves to a large degree. Auditing of the use of biometric data and application needs to be conducted on a regular basis by an independent agency.

g) In addition, we need to deal with the issue of data ownership. Currently, the default in the industry is that the data is owned by the organization that collects the data. In order to guarantee individual rights data needs to be owned and controlled by the individual. HIPPA has been a major consideration on protecting the rights of people with respect to their own data. However, much more needs to be done in order to preserve privacy and civil rights.

- Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);

Comments:

h) Performance auditing is critically important and must be done to validate performance of biometric systems and whether the systems are being used correctly and in an unbiased manner. In some cases, testing of biometric systems cannot be fully and effectively performed prior to the use of the systems. As the user population of the system changes the performance of systems can change and bias can be introduced. This is particularly true with AI-based systems. Post-deployment testing and validation of biometric systems need to be based on how they are used and how their user population changes. This needs to be part of the design and testing plans for the system, and any certification of the system. Testing and maintenance of the system needs to be part of any professional and responsible development plan.

- Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);

Comments:

i) Biometrics are not a surveillance technology, though some but not all biometrics can be used for surveillance. Surveillance is by definition observing and documenting individuals' location, movement, and actions without their consent or knowledge. Surveillance is needed in some applications and for some specific reasons. The determination of whether an application is appropriate is an evaluation of the benefits versus potential harm. The bigger and more difficult issue is not the use of biometrics data for a specific, singular application but rather the aggregation of data about individuals across time and multiple, different applications. Biometrics can make this more complex because of the increasing reliability of biometrics and their ability to ensure that data is associated with an individual identity. Data aggregation is the single greatest danger to privacy. Combatting data aggregation will require a regulatory approach specifically developed to address the issue.

- Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems;

Comments:

j) Fingerprints and DNA have been used extensively in the courts. As more biometrics are used it is important that there are standards for the technology and for the experts.

k) The use of AI-based technology in biometrics does create a number of issues for court testimony. To begin with, the experts must be very familiar with the inner working of any technology that is used and for which they testify. This can be problematic in multiple ways. First, not all AI based technology used in the industry is well understood by all biometrics experts. This is due to the fact that the companies that make these systems use trade secrets. Second, many AI systems are not transparent in their inner working because of the nature of the training algorithms they use. Finally, many biometrics experts are not also AI experts. In order to mitigate these issues, a number of steps need to be taken: 1) Biometrics experts need to be well trained and certified on all aspects of the technology that they are working with. 2) AI based biometric systems need a higher degree of transparency. 3) Some group of very experienced senior level experts need to supervise the certification of experts in this area. In addition, as with any evidence that is used in court, the testimony needs to be backed up by a body of scientific studies, formalized testing and published research. The IEEE (Institute of Electrical and Electronics Engineers) started this process several years ago with biometric professional certification program.

- Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.

Comments:

l) Transparency is incredibly important. Transparency overlaps with a number of other issues and needs of the community, and needs to address several key factors:
- Transparency of the design of the system, reviewed by technically competent experts.
- Transparency of the algorithms, the ways the system makes its decisions about matching.
- Transparency of applications, in what applications the algorithms and data are used.
- Transparency of data use, how and when individual's data are used.

In addition to data ownership and better-informed consent, transparency will address most of the issues with biometric and AI technologies.

Additional concerns

In order to effectively address the use of biometrics in government and industry it is critical that several major issues be addressed in the development and implementation of governance.

1. Equity and Bias: Any science can be misused or used incorrectly. Equity and bias can be designed out of any system by expert engineers.
2. The rights to anonymity / ownership of data: The right to anonymity is important to most individuals and is quickly eroding in 21st century America and throughout the world. As a part of biometrics governance, we should also more specifically specify the rights to anonymity in the United States. Likewise, the people need to be given full rights to control the use of their data and to decide how and when it will be used to target them.
3. Economic incentives: Economic incentives inherently drive behavior of commercial businesses. The data that many electronics, on-line shopping, and social media companies are collecting on people is valued in the trillions of dollars. Any regulations and governance of the biometrics industry inherently requires addressing the economic incentive to industries that collect, share, group, integrate and use this data.
4. In evaluating biometrics governance, it is necessary to create and use tools that can evaluate biometric systems in a meaningful way based on benefits and risks, and can create an ability to do trade space analysis when it comes to biometric technology selection, and test as part of an overall system and/or ensemble of other biometrics for defined applications (i.e., the trade space is not the same for different applications, but the framework/ process would be foundational). Additionally, the development of the governance will be complex and its impact should be evaluated incrementally by creating a roadmap that captures needed advances in technology, governance, regulations, and incentives for different problem domains (i.e., the governance for industry should not be the same as for national security of law enforcement). Finally, A part of this needs to include a meaningful risk analysis framework across many of the dimensions of use and reliability of the technology and benefits to the individuals.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Google

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Response to Request for Information:
Public and Private Sector Uses of Biometric Technologies
86 Fed. Reg. 56300 (Oct. 8, 2021)

January 14, 2022

Google strives to make the technology we develop human-centered, accurate, fair, secure, based on sound science, accountable to people and, ultimately, a benefit to society. Google welcomes this opportunity to provide comments in response to the White House Office of Science and Technology Policy (OSTP) Request for Information (RFI) on biometric technologies.[1]

The development and use of biometric technologies in a variety of applications in the public and private sectors – and our collective understanding of the benefits and risks for individuals, communities, and society more broadly – has rapidly expanded in recent years. We agree with OSTP that it is timely and important to examine which classifications and applications of biometric technologies can be used responsibly to enable useful, secure, personalized, and accessible products and services that guard against harmful outcomes. In parallel, it is important to examine how best to protect against misuse and abuse, such as mass surveillance of individuals, particularly without their awareness or consent, in a manner that infringes on human rights and civil liberties.

Our comments focus on how OSTP can help foster the responsible development and use of biometric technologies. Terminology around biometric technologies is varied; to provide clarity, we define and assess the biometric techniques identified in the RFI and provide examples of how Google employs these techniques in our products and services. Our comments also speak to the risks and benefits of the development and use of the techniques and the mitigations we put in place.

Google believes any governance framework for biometric technologies should be proportional and enable a holistic examination of the technologies employed. It should also recognize that not all techniques or use cases are equally able to anticipate the specific use cases to which they are applied. To that end, our comments describe the principles and practices Google considers core to the responsible development and use of biometric technologies, including those reflected in our AI Principles[2], Privacy

[1] 86 Fed. Reg. 56300 (Oct. 8, 2021).
[2] https://ai.google/principles/

and Security Principles[3], and Human Rights Program[4] which guide our careful approach. We also suggest factors for consideration in developing a governance framework, including any regulatory treatment.

We welcome the opportunity to engage further on these issues with OSTP and other stakeholders, and expand on the issues covered in these comments.

Biometric technologies that identify individuals: Authentication and Identification

Biometric technologies identify specific individuals based on their biological characteristics (*e.g.*, face, iris) and/or behavioral traits (*e.g.*, gait).[5] They can be divided into two general categories of applications: authentication and identification.

Biometric "authentication": Biometric authentication involves comparing an individual's biometric data, such as a fingerprint, to a template or trusted identity document. The goal is to determine whether they match to verify the identity of an individual (*e.g.*, to provide access to a secure location or device). Many people embrace biometric authentication (*e.g.*, voice, fingerprint) because it is simple; biometric identifiers cannot easily be lost, forgotten, or stolen; and they can be combined with traditional password and PIN methods for even greater security and accountability.[6]

Biometric "identification"**:** Biometric identification involves searching a database of biometric identifiers for a match with the identifier of a specific individual.[7] Biometric identification enables a variety of beneficial features and personalized experiences for users, and there are a number of safeguards that can be put in place to manage risk. But certain biometric identification technologies like facial recognition can also be used in high-risk applications, for example for mass surveillance. Google has taken a cautious approach[8] to these technologies, and they are deployed in a small number of Google products with specific provisions guiding their application in areas where we have identified beneficial uses.

Biometric authentication and identification systems are used in a variety of Google products. For example:

- *Pixel Unlock:* Users can opt to set up fingerprint recognition to unlock Pixel phones, by providing a series of differently angled fingerprints which are used to create a model of the fingerprint belonging to the phone's owner. When

[3] https://safety.google/principles/
[4] https://about.google/human-rights/
[5] *See, e.g.*, ISO/IEC TR 24741:2018(en), Information technology — Biometrics — Overview and application.
[6] https://www.gartner.com/smarterwithgartner/the-iam-leaders-guide-to-biometric-authentication
[7] *See, e.g.*, ISO/IEC TR 24741:2018(en), Information technology — Biometrics — Overview and application.
[8] https://ai.google/responsibilities/facial-recognition/

someone tries to use the phone, the system can compare that person's fingerprint against the enrolled model, keeping malicious actors out while allowing users to unlock their device with a single touch.

- *Unlocking Incognito Tabs:* With the Chrome 92[9] update for the iOS version of Chrome, users can optionally secure incognito browser tabs to only be unlocked with Touch ID, Face ID, or a passcode. To enable this, just as for Pixel Unlock, users provide samples (either fingerprints or face images), which are used to create a model of the authorized user on the device.

- *Confirming credit cards with biometrics:* Users that choose to save credit card information to their Google account can enroll to retrieve that information via biometric authentication stored on the device, such as fingerprint or face verification.

- *Face Match on Nest Hub Max:* Face Match uses facial recognition to allow multiple people in a home to get personalized help on a shared home device – from seeing their personalized calendars and morning commute details, to checking missed messages meant just for them, or even playing their own favorite song. For each person who opts in to Face Match, the Assistant guides them through the process of creating a face model, which is encrypted and stored on the device. Following setup, all face matching occurs locally on the device. The user remains in control all the time and can opt-out of the feature and delete their face data at any time.

- *Nest Familiar Face Detection:* Users can opt in to use the Familiar Faces feature on Nest Cameras with a Nest Aware subscription (in compliance with the law). When a Nest Cam detects a face, the Familiar Faces feature allows a user to teach their camera whether that face is a known or unknown person. The user can assign known individuals names, and opt to receive notifications when these known individuals are detected by the camera on their property. The user remains in control at all times and can opt-out of the feature and delete their face library at any time.

- *Cloud Celebrity Recognition API:* Google Cloud offers a celebrity recognition API to authorized media and entertainment companies, helping them to identify a limited number of commonly recognizable celebrities in professionally produced media content. We have defined service specific terms[10] that apply to all users of the API and the API is only available by application only to media & entertainment customers with use cases that align with our terms of service.

[9] https://chromium.googlesource.com/chromium/src/+/e567a85af0255a6d759fb11bf07576d95345df0b
[10] https://cloud.google.com/vision/docs/celebrity-recognition

Applications that do not identify individuals: Detection, Clustering, Inference and Tracking

There are also applications that may involve processing biological characteristics, but not with the purpose of identifying specific individuals. These applications often involve fewer risks to individual rights and privacy than those associated with systems that identify individuals. While there are still risks associated with these applications (as outlined in the next section), the addition of identification heightens those risks. Applications which do not identify individuals, but process biological characteristics to deliver beneficial functions that would not otherwise be possible, are an area where innovation should be encouraged.

Detection: Allows a system to discern the presence and location of humans or particular body parts (*e.g.*, faces) in images or videos.[11] This technology can help computers answer questions like "where are the hands in this image?" or "how many faces are there in this image?" Detection is used in products like the Google Pixel camera to unblur faces.[12]

Clustering: A method that groups faces or other objects in images and video by likeness. Clustering is used in products like Google Photos to help users search and label their pictures by grouping pictures that include the same person.[13]

Inference: The process of drawing conclusions regarding a person's characteristics using physiological or behavioral information. This process would include, for example, providing suggestions for improved wellness based on data from sensors or trying to improve communication through interpretation of facial or vocal expressions. For example, an accessibility feature in beta in Android 12 allows users to control their phones with facial expressions, helping users who have difficulty with touch or voice controls more easily use their phones.[14]

Tracking: Identifies distinct attributes of an individual, but not who that individual is, allowing them to be tracked as they move through a space and are picked up on different sensors, such as through different video frames. Tracking can help computers answer questions like "what path do customers follow through this store," but not who those specific customers are, to help with product placement and identify areas of frequent congestion.

[11] Object Detection in 2021: The Definitive Guide, available at https://viso.ai/deep-learning/object-detection/
[12] https://www.androidcentral.com/how-does-face-unblur-feature-work-google-pixel
[13] https://support.google.com/photos/answer/6128838?hl=en&co=GENIE.Platform=Android
[14] https://www.theverge.com/2021/8/16/22626754/android-accessibility-face-gesture-controls

Responsible development of technologies that use biological characteristics

Technologies that use biological characteristics to identify individuals or to infer emotion, disposition, character, or intent (as outlined in the RFI) carry a wide array of potential benefits and risks – some linked to features of the technology itself; others arising from how the technology is used. For example, face detection can be used to help cameras take better photos by improving focus on faces, but it may not work equally well for all skin tones and thus create or exacerbate inequities.[15] Similarly, inference technology can help people who are blind or low-vision to read facial expressions, or help those with neurodiverse conditions (*e.g.*, autism) learn to better recognize different human emotional expressions. However, using such technologies to attempt to infer criminal intent (*e.g.*, based on an individual's facial expressions or voice characteristics) may lead to unfair interventions or create escalation dynamics that lead to harm. It is thus important to consider both the technology and the specific use case or application when assessing risk.

Google is very careful about deploying biometric identification in products and services because they come with heightened risk. Potential risks include performance and fairness issues (*e.g.*, lower accuracy across different genders, skin tones, ages); privacy and security risks to users' information being exposed (*e.g.*, voice, fingerprints); and sensitive use cases (*e.g.*, when identification is combined with tracking, it can be used to surveil individuals' movements over time, while identification and inference could be used to profile individuals' preferences and private thoughts in ways that violate their privacy). These risks can lead to serious harms. For example, false matches can lead to individuals being incorrectly accused of crimes, and non-matches can lead to denial of services.

While each biometric technology application is distinct and context specific, there are some generalizable responsible practices in line with our AI Principles and Privacy and Security Principles.[16] In summary:

- The application must be likely to deliver significant, concrete overall benefit to users and customers. Likely benefits should be verified through extensive user testing, including testing to determine whether any groups have been negatively affected in consultation with experts in machine learning fairness and internal stakeholders;

- Data used for model development, training, and evaluation should be appropriately licensed or otherwise approved for the intended use. Similarly, appropriate notice and consent mechanisms must be in place for collection and use of user data by the application;

[15] https://modelcards.withgoogle.com/face-detection
[16] https://ai.google/principles/ and https://safety.google/principles/

- Unless there is a critical product need, or reasonable expectation on behalf of users that biometric data will be stored, it should be immediately processed and not stored at all. If biometric data is to be stored, it should be in line with best practices and legal requirements (*e.g.*, deleted or obscured within a defined number of days where appropriate; safeguards in place to prevent misuse).

For more established forms of biometric applications, such as face-related technologies, we provide more specific guidance to product teams in the form of internally tailored questions and recommendations. Such frameworks are intended to be living documents, which can be updated as needed to account for evolving technology and changes to government policies.

Another responsible practice is to consult with relevant experts in communities that may be impacted by these technologies. For example, in 2018 Google commissioned BSR (Business for Social Responsibility) to conduct a human rights impact assessment of facial recognition technologies based on the UN Guiding Principles on Business and Human Rights. The assessment included a review of existing literature in the space and consultations with potentially affected stakeholders and independent experts. While we identified potential benefits – including business benefits – of certain specific applications of facial recognition, we ultimately determined that we would not offer general-purpose facial recognition APIs before working through key technology and policy questions.[17] Instead, we advised our product teams to concentrate on narrowly focused solutions, and enacted several safeguards to ensure the responsible development and use of tailored applications. For example, we developed a Celebrity Recognition API (noted above) which allow-lists companies for access and includes an opt-out policy for celebrities to request removal from the system.[18]

There also are heightened security risks posed by biometric identification technologies. Because an individual's biometric data (*e.g.*, fingerprints, DNA, vein patterns) cannot typically be changed if compromised, they are high value targets for bad actors. As such, companies that collect and process biometric data need to implement appropriate safeguards to protect against data breaches. For Android, we maintain an open source Measuring Biometric Unlock Security[19] resource to help our partners ensure the security of biometric data across services and devices. This includes guidance on architectural security, biometric security performance, and related metrics like imposter acceptance rate (the chance someone mimicking a legitimate input can deliberately fool the model), and false acceptance rate (the chance the model will accept a randomly chosen input).

Because biometric recognition technologies are based on biological characteristics, variations in characteristics across different groups of users can lead to differences in

[17] https://cloud.google.com/blog/products/ai-machine-learning/celebrity-recognition-now-available-to-approved-media-entertainment-customers
[18] https://cloud.google.com/vision/docs/celebrity-recognition
[19] https://source.android.com/security/biometric/measure

performance. To address this risk on Android devices, for example, Google calibrates presentation attacks[20] across a variety of faces to maximize the chances of uncovering performance gaps. Testing biometric authentication mechanisms in this way helps to reveal substantially poorer performance for segments of the global population, thereby helping Google ensure that these models function fairly and equitably across different demographics. Google employs a similar approach for its fingerprint recognition technology, using a variety of fingerprints to determine the optimal parameters for recognition and spoof testing.

Recommendations to OSTP

Technologies that use biological characteristics create beneficial new capabilities and offer personalized experiences for users. Any framework for biometrics should take a risk-based approach, enabling beneficial innovation in lower-risk applications while promoting effective protections for certain high-risk technologies and applications. Because biometric recognition technologies can pose a higher risk of harm to individuals, communities, and society, it is appropriate that they incorporate more rigorous safeguards. Furthermore, frameworks governing biometric technologies should provide clear guidance and resources to deployers of biometric identification systems. This could include, for example, recommended practices for receiving and responding to user feedback, and a library of techniques for measuring the accuracy[21] of biometric identification systems, including benchmarks of minimum sample sizes for determining error rates and standards for performance testing across different user attributes - such as gender, skin tone, voice or region - as relevant to a given technology.

To assess potential risks, the framework should take into account both technical features and the application or use case of a biometric system, including how people interact with and interpret the outputs of the system. This includes factors like accuracy, latency, the benefits and drawbacks of cloud versus on-device biometrics processing,[22] the likelihood of malicious attack or attempted deception, and the impact of any successful attacks. It also includes whether the system is used to, for example, authenticate users for secure device access or to identify individuals passing through a building. The framework could also provide guidance on factors to consider when determining appropriate safeguards against both anticipated and unanticipated

[20] A presentation attack is the presentation of an artifact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended function of the biometric system. *See* Evaluation of Presentation Attack Detection: An Example, NIST available at https://www.nist.gov/system/files/documents/2020/11/04/15_tuesday_johnson_evaluation_of_presentation_attack_detection_an_example_ibpc2014_sacs2.pdf

[21] Accuracy refers to the frequency with which biometric signals are matched with the correct individuals. Certain biometric technologies offer higher accuracy than others, for example, DNA and fingerprint biometrics generally offer a higher level of accuracy than face or palm print biometrics.

[22] For example, on-device processing may provide greater privacy if the device itself employs strong security measures, but the biometric system may be less accurate given limitations associated with on-device computing resources.

misuse or harms. It could include, for example, guardrails that can be put in place for downstream use, such as contractual terms prohibiting certain uses of data or models by third parties and by requiring certain data security measures to be in place.

However, OSTP should also recognize that biometric technology is still an emerging field and relevant benchmarks and best practices will continue to evolve. OSTP should allow for continuing innovation in this space. A US framework should encourage global interoperability and align with national and international standards through organizations like the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

******

Google appreciates this opportunity to provide a response to OSTP's request for information and looks forward to continued discussion on these important issues.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Health Information Technology Research and Development Interagency Working Group

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 11, 2022

Dr. Eric Lander
Director, Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Response to RFI on "Public and Private Sector Uses of Biometric Technologies," FR Doc. 2021-21975

Dear Dr. Lander,

The Networking and Information Technology Research and Development (NITRD)'s, Health Information Technology Research and Development (HITRD) Interagency Working Group (IWG) appreciates the opportunity to comment on the Request for Information (RFI) from the OSTP on public and private sector uses of biometric technologies.

The HITRD IWG is a federal interagency working group that reports to the NSTC's NITRD Subcommittee. The HITRD IWG was formed in 2010 to advance information technology (IT) research and development (R&D) for medical, functional, and public health outcomes across 15 participating federal agencies[1]. The HITRD IWG advances R&D by coordinating agency plans and activities, promoting collaborations, and providing a forum for exchanging information and articulating R&D needs to policymakers and decision-makers.

*Reference the Federal Health Information Technology Research & Development Strategic Framework[2] for areas/agencies where this work is being done.

With a focus on the connection of biometrics and health, we offer the following observations.

*Opportunities for new biometrics technology
- 5G
- Artificial Intelligence
- Pervasive computing

*Challenges for using biometrics to understand health
- Privacy/security is an ongoing concern
- Ethical and trustworthy technology and data is still not a standard
- Ability to share data for research and monitoring is limited
    - Exculpatory language in commercial Terms of Service
    - Data ownership
    - Data sharing plans
- Lack of infrastructure to leverage technology and data across agencies
- Lack of transparency in existing technologies and need for best practices

[1] https://www.nitrd.gov/coordination-areas/hitrd/
[2] https://www.nitrd.gov/pubs/Federal-Health-IT-Strategic-Framework-2020.pdf

- Need for interoperability of technologies and data, including a need for ontologies and standards

*Suggested actions that the HITRD IWG could coordinate, if called upon
- Data call / portfolio analysis of health-focused biometric work across agencies
- Support infrastructure development to facilitate data sharing of health biometric data and coordination across agencies
- Listening sessions and engagement with industry and the research community to facilitate R&D, as well as data sharing related to health biometric technologies

Once again, we appreciate your efforts to understand the biometric technology landscape. The HITRD IWG would be pleased to serve as a partner and resource for the OSTP as it continues work to understand the use biometric technologies.

This submission represents the individual views of the members of the Health IT IWG, not necessarily those of their home agency or the NITRD Program.

If you have any questions, please feel free to reach out to Wendy Nilsen at [redacted] or Dana Wolff-Hughes at [redacted], co-chairs of the HITRD IWG.

Sincerely,

Wendy Nilsen, NSF

Dana Wolff-Hughes, NIH

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

HireVue

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

Office of Science and Technology Policy
1650 Pennslyvania Avenue NW
Washington, DC 20502
Via email to *BiometricRFI@ostp.eop.gov*

Re: RFI Response: Biometric Technologies

To Whom It May Concern:

HireVue submits the following comments to the Office of Science and Technology Policy's Request for Information on Public and Private Users of Biometric Technology (the "RFI").

HireVue is the global leader offering an end-to-end hiring software platform featuring video interviewing, assessments, and text-enabled recruiting tools using AI. HireVue has hosted more than 27 million video interviews and 150M chat-based candidate engagements for over 700 pioneering customers around the globe.

With respect to employment, HireVue believes the only factors that should be evaluated during the recruitment process are a candidate's competencies concerning job-related knowledge, skills, and abilities associated with that particular job. From our beginning more than 15 years ago, HireVue's core mission has always been to democratize the hiring process and improve accessibility for job candidates.

In the early stages (~2016-2019) of HireVue's development of our assessment solution, work was undertaken to score video interview responses by analyzing the same data humans use to evaluate interview answers. These verbal (words spoken), para-verbal (e.g., audio tones), and video (e.g., facial action units) data sets were used to custom build algorithms statistically linked to on-the-job performance metrics (e.g., customer service ratings). Over these few years, we had enough data and expert human ratings (of job performance and competency evaluations) to study the incremental relations of the verbal, para-verbal, and video data to job success and rater evaluations. This research, along with significant improvements in Natural Language Processing (NLP) technology, proved the para-verbal and video data features did not add incremental measurement accuracy in our algorithms. Thus, in 2020, we discontinued those uses and began only putting into production (and updating existing client assessments) our NLP-based assessments to evaluate candidates' interview responses. As of January 31, 2022, all of our USA-based customers will only be using NLP analytics in the assessments (with the exception of one customer who will switch to the upgraded assessment a month later; due to business constraint issues.

To avoid doubt, HireVue does not use technology to identify or analyze physical aspects of a person (e.g., DNA, fingerprints, face, or retina scans) or behavioral aspects derived from voice patterns, tonality, body gestures, or gate. HireVue also has no plans to use biometric information to identify or infer emotion, disposition, character, or intent into any of our recruiting tools.

HireVue's hiring assessments simply score candidates' spoken responses to recorded interviews using NLP technology. The candidates' spoken responses are scored using an expertly guided rating scale for each individual competency related to the job requirements (e.g., service orientation) to help companies quickly, accurately and fairly assess job candidates.

Even though HireVue only uses NLP analytics in our assessments, we are submitting comments to this RFI because we recognize the impact our software can have on individuals and on society, and we feel our experience can help guide development of regulations with respect to employment decisions whether biometrics or other analytical tools are deployed. Based on the state and continuing pace of innovation with technology, we believe any current regulatory guidance should be updated and HireVue supports public and private sector efforts to update these policies and provide guidance and clarity of all automated and algorithmic aided hiring decisions. Thus, HireVue is supportive of the OSTP's RFI and its review of policies and regulation regarding the use of biometric technology.

We also believe that technology providers need to be actively engaged and open to discussing the applicable legal standards, demonstrating a commitment to transparency and accountability, and establishing ethical standards in the use of their technology. Based on these topics, HireVue addresses Point Seven generally and sets forth the practices or procedures it's taken with its use of NLP-assisted assessments which could be informative when considering guidance for the use of biometric technology.

First, HireVue's methods are firmly grounded on over 100 year of selection science.[1] We believe that technology providers have a responsibility to implement standards and best practices from the fields of industrial-organizational psychology and data science. We employ a team of advanced degree industrial-organizational psychologists and data scientists who develop scientifically validated algorithmic assessments that target the core competencies needed for a job role being filled. NLP technology relies only on what is said by the candidate and does not need to use any video analysis or other audio characteristics because our scientifically validated research found that facial analysis and audio patterns do not significantly contribute to the competency measurement or job performance success.[2]

Second, HireVue follows and in many ways exceeds the Equal Employment Opportunity Commission (EEOC) Uniform Guidelines when developing, testing, and monitoring all HireVue NLP-driven assessments and takes efforts to describe the process and regularly update that information for employers and candidates alike. HireVue works to go beyond what is legally required to mitigate any bias that may exist as a result of its use of technology by testing for adverse impact in its prediction models, then removing or minimizing the weight given to data points in the assessments that may create biased results. [3]

Third, HireVue set an industry standard by publishing its own ethical AI principles to inform the public of the standards to which it voluntarily holds itself and creates accountability. Furthermore, in an effort to bolster its accountability, HireVue tested its methodologies and bias mitigation techniques by subjecting them to multiple independent third-party audits, then publishing the details of the resulting reports.[4] With respect to each auditor's recommendations,

HireVue took into consideration and modified our solutions, to further enhance and fine tune our assessments and methodologies.

HireVue supports thoughtful and reasoned legislation and guidance to employers and technology providers to achieve accurate and fair technology assisted employment decisions. HireVue can provide any requested additional information and is willing to engage in constructive dialog with policy makers as a leading Human Resources technology provider. HireVue is happy to discuss what other transparency, ethics and accountability measures are reasonable and necessary in the recruiting technology industry.

Sincerely,

[redacted]

Kevin Parker

HireVue, Inc. CEO

---

[1] See Zedeck, S. (Ed.). (2011). APA handbook of industrial and organizational psychology, Vol. 1. Building and developing the organization. American Psychological Association. https://doi.org/10.1037/12169-000; and Schmidt, F. L., & Hunter, J. E. (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. Psychological Bulletin, 124(2), 262-274.

[2] The interview-based NLP models demonstrate high levels of convergent validity (average r value of 0.66; n=60,183), good test-retest reliability (average r of 0.72; n=181,610), and minimal levels of between-group differences (Cohen's d < 0.20; n=81,910). Additionally, the predictive validity on organizational data in four criterion validation samples has acceptable evidence (Interview-based NLP models average uncorrected criterion validity of .24; n=1,687). In similar criterion validation studies customized AI-based algorithms yield even higher validities (range 0.25 to 0.49) which are comparable to the predictive validity of structured interviews (McDaniel et al., 1994; Schmidt & Hunter, 1998).

[3] See Mondragon, Nathan (June 6th, 2021). Creating AI-driven pre-hire assessments. hirevue.com. Retrieved January 10, 2022, from https://www.hirevue.com/blog/hiring/creating-ai-driven-pre-employment-assessments: "*The Guidelines require fair treatment of applicants in the hiring process regardless of race, gender, and age (40 and over). These protections include the 4/5ths Rule, also known as the Red-Flag Rule, and other statistical tests for group differences; all of which HireVue uses to monitor and mitigate our assessments. We go beyond that to test for a wider array of group differences beyond those solely required by law. Only after we are confident that the adverse impact of any bias has been minimized do we release any algorithmic-based assessment for customer use. Furthermore, we continue to monitor the algorithm for any bias creep that may occur…. In addition to EEOC guidelines, at HireVue, we test for a wider array of group differences, beyond those required by law. That's because there are biases beyond age, gender, and ethnicity, for example, attractiveness, country of residence, non-native accent, etc.*"

[4] Zuloaga. Lindsey. (January 11, 2021), *Industry Leadership: New audit results and decision on visual analysis*, HireVue.com. Retrieved January 10, 2022, from https://www.hirevue.com/blog/hiring/industry-leadership-new-audit-results-and-decision-on-visual-analysis; See also Hire Vue, Inc. April 7, 2021, Independent audit affirms the scientific foundations of HIreVue Assessments. HireVue.com, retrieved January 12, 2022 from https://www.hirevue.com/press-release/independent-audit-affirms-the-scientific-foundation-of-hirevue-assessmentsL "Central to the audit findings is the conclusion that the HireVue job analysis process was "of very high quality and rigor in relation to established standards... resulting in the creation of trustworthy content-related validation evidence and subsequent hiring decisions." Also of note was Dr. Landers' conclusion about the company's use of AI and IO Psychology produces results supported by IO Psychology science."

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

HR Policy Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

COMMENTS BY HR POLICY ASSOCIATION

TO THE

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

REQUEST FOR INFORMATION ON

PUBLIC AND PRIVATE SECTOR USES OF BIOMETRIC TECHNOLOGIES

Docket No. 2021-21975

JANUARY 14, 2022

Introduction: Thank you for the opportunity to lend our perspective in this critical area. HR Policy Association is the lead public policy organization of chief human resource officers (CHROs) representing more than 400 of the largest employers doing business in the United States and globally. The Association convenes these executives not simply to discuss how human resource practices and policies should be improved, but also to help create and promote HR strategies and initiatives for diverse and inclusive workforces. Collectively our members employ more than 20 million employees worldwide and have a market capitalization of more than $7.5 trillion. In the United States, Association members employ over 9 percent of the U.S. private sector workforce.

In these comments we will seek to provide insights on employer activities related to topic 6 of the RFI: "Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case." We will focus our comments on subitem A: "stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies," though our comments will have implications for several other areas noted in topic 6, including in subitems C, D, E, and F. We will also provide background on employer motivations for ensuring the ethical and responsible use of AI, including biometric technologies.

There is a premium on talent during the economic recovery from COVID. At the time of writing, the labor force participation rate is 61.8%, with the difference from the February 2020 rate of 63.3% representing the absence of millions of workers. Much of this loss reflects the impact of COVID on women and workers over 55 who have largely been pulled out of work by childcare responsibilities and early retirement, respectively. Black and Latino or Hispanic individuals have experienced unemployment rates much higher than other demographic groups throughout the pandemic, with Black women especially dropping out of the labor force at a much higher rate than any other group since schools reopened in August of 2021.[1] Also hard hit were workers without a college degree, whose labor force participation rate is far below even the current average while those with a bachelor's degree is much higher. In the U.S. alone there are 11 million job openings, with only 6.9 million unemployed Americans to fill them.

Consumers feel these shortages in terms of empty store shelves and rising prices. For example, longshoremen and truck drivers needed to move consumer goods are in short supply in many places in the world as record numbers of container ships have become stuck along Los Angeles, Long Beach, and other key U.S. ports in 2021. Over the last 12 months, the Producer Price Index has soared above an also rising Consumer Price Index as consumer demand has remained

[1] Barr, Anthony, Makada Henry-Nickie, and Kristen E. Broady. "The November Jobs Report Shows Black Women Are Leaving the Labor Force." Brookings, December 9, 2021. https://www.brookings.edu/blog/the-avenue/2021/12/08/the-november-jobs-report-shows-black-women-are-leaving-the-labor-force/.

strong among worker shortages. According to a recent survey of local chamber of commerce leaders, more than 90% reported that lack of available workers is holding back the economy in their area and less than 1% reported it is easy to fill jobs.[2]

For large companies, attracting and retaining diverse talent and achieving the right culture is a core component of their business strategies and the economic recovery. Even as the labor shortage persists, large companies are seeking to attract, train, advance and retain diverse talent and cultivate inclusive workplace cultures. In the most recent HR Policy survey of CHRO priorities, diversity and inclusion ranked as the top concern. The three priorities that followed are related: cultural transformation in anticipation of the post-COVID work environment; executive development, including critical role succession; and talent management, including recruitment and retention. Digitization of the workplace followed as the fifth highest concern out of 20 total possible responses.

Large employers' commitment to Diversity, Equity and Inclusion (DE&I) goes beyond numerical requirements imposed by federal policy—companies are implementing workforce strategies to create respectful work environments that foster a vibrant diversity of perspectives represented at every level of the organization. Such a balance leads to a more productive workforce and better business outcomes.

DE&I has also increasingly come to be seen as material to business performance by outside stakeholders, including institutional investors. Investors are considering environmental, social, and governance (ESG) disclosures as a potential information source for extracting a competitive advantage, especially over the long term. Companies are integrating ESG as a remunerative facet of their business models—and as a risk management strategy.

Finally, it is worth noting that for large companies with operations throughout the U.S. and globally, DE&I efforts are also designed to ensure that the workforce reflects the company's diverse geographical footprint and customer base. Not surprisingly, companies operating on a global level face a more complex challenge in promoting diversity and inclusion. The challenge manifests on two levels—one within the country where operations exist and the other involving the company's global employee population. With regard to the first, there are varying legal requirements in the jurisdictions within which companies may operate. In fact, diversity-related legal requirements in most countries outside the U.S. often focus exclusively on disability and gender, with little or no attention paid, for example, to ethnicity or nationality. Yet, for all the reasons stated previously, the absence of legal requirements typically does not stop companies from working to apply their own cultural diversity and inclusion imperatives wherever they have employees.

[2] "The America Works Report: Quantifying the Nation's Workforce Crisis." U.S. Chamber of Commerce, October 25, 2021. https://www.uschamber.com/workforce/education/the-america-works-report-quantifying-the-nations-workforce-crisis.

Artificial intelligence has the potential to further enhance the employee experience and expand employment opportunities to underrepresented populations. For example, AI solutions to analyze demographic composition of a given workforce, comparing against industry or regional demographic statistics, are beginning to emerge. Such insights can help companies detect disparities across race, ethnicity, age, gender, disability, veteran status, and other identities, while also diving deeper into intersectional indices. Other platforms may track employee attrition rates and enhance employee feedback mechanisms to detect areas where a company may have an opportunity to implement diversity and inclusion initiatives.

Many employers utilize AI-powered tools to augment recruiters and hiring managers' efforts in sourcing job candidates, increasing efficiency significantly while helping ensure diverse slates of qualified candidates for consideration. (According to an Accenture study, a poor hire can cost up to five times the annual salary of that person.[3] A good hire, on the other hand, increases productivity, improves morale, and enhances a company's image as a good employer.) In other cases, employers are using AI-powered tools to identify and remove language on job descriptions that appears to reflect unconscious bias or requirements that are not necessary for the job. The use of such capabilities allow employers to access wider talent pools and begin building talent pipelines of underrepresented populations in ways not previously accessible.

Nevertheless, AI is an evolving technology and therefore careful attention must be paid to weigh benefits against potential risks. Use cases for AI in the workplace vary widely, with risk profiles that vary considerably both in scope and in kind. In addition, the types of data used are different—indeed there are many uses of AI in the workplace that do not rely on biometric data, and many HR tech vendors do not work on biometric information at all.

HR Policy members are aware that, if not implemented and used responsibly, artificial intelligence has the potential to produce adverse outcomes. In the HR context, this particularly means a focus on fairness, privacy, and safety. Even companies with a record of successes in terms of diversity and inclusion within their workplaces must wage a continuing battle against unconscious bias, which can be a barrier among hiring managers during sourcing and talent acquisition processes and can negatively impact diversity efforts.

There is legitimate concern that inaccurate, incomplete, or unrepresentative data potentially can amplify, rather than minimize, bias. Other seemingly objective data may prove misleading—for example, metrics on who leaves the workforce may not take into account that the cause could be a hostile work environment. Moreover, the manner in which certain technologies are deployed, and the practices surrounding use of such technologies, may propagate or create patterns of bias, even in circumstances where the technology is deployed in order to help eliminate bias and while giving the illusion of objectivity.

[3] Chambliss, Corey; Vaughan, Kristen. "Next generation talent assessment." Accenture.

AI-enabled tools powered by biometric data could carry their own set of serious risks. Programs to track facial movements and speaking patterns in interview settings may score a candidate inaccurately due to demographic differences. Facial recognition tools have often scored poorly in accuracy tests for those with darker skin, and particularly darker-skinned females.[4] Recently, a Facebook algorithm prompted viewers of a video featuring Black men in confrontation with white individuals, including law enforcement, to "Keep seeing videos about Primates."[5]

In order to build trust and support worker attraction and retention, large employers are committed to the prevention of bias in the workplace. Reputational damage alone may detrimentally impact a company's efforts to assemble a competitive workforce, and may cost employers as much as 10% in additional cost per hire.[6] Other potential negative outcomes may be produced by the misapplication of AI in the work context, which could undermine efforts to establish an inclusive corporate culture. Notwithstanding regulatory concerns, in practice the impact of poorly used AI affects both employers as well as current and potential employees. With a loss of trust, companies would face significant challenges deploying even responsible uses of AI to increase efficiency, enhance the worker experience, and support their DE&I efforts.

Regulatory activity and the consideration of such in this area is beginning to emerge. In addition to the White House's initiative to create an AI Bill of Rights, last November the Equal Employment Opportunity Commission launched an initiative to ensure that artificial intelligence and algorithmic decision-making tools "do not become a high-tech pathway to discrimination," according to Chair Charlotte Burrows. Meanwhile, the Federal Trade Commission is considering rulemaking to "ensure that algorithmic decision-making does not result in unlawful discrimination." At the state and federal level, legislation is being considered to provide worker protections against discrimination through the use of AI, with several noteworthy measures already having passed at the state level.

Examples of employer-driven efforts to promote ethical and responsible use of AI: Business leaders and NGOs recognize the importance of building trust regarding the use of AI, and more importantly of avoiding deploying artificial intelligence in ways that discriminate or otherwise undermine corporate business objectives. There are many current examples of employer-driven efforts to ensure AI is used ethically and responsibly, several of which HR Policy Association has led or participated in. Below are examples of just some of these initiatives.

- **HR Policy Association AI principles for company adoption:** In 2020, HR Policy Association recommended to our members a set of principles on the use of employee

[4] Najibi, Alex. "Racial Discrimination in Face Recognition Technology." Science in the News, October 26, 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.
[5] Mac, Ryan. "Facebook Apologizes after A.I. Puts 'Primates' Label on Video of Black Men." The New York Times, September 3, 2021. https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html.
[6] Burgess, Wade. "A Bad Reputation Costs a Company at Least 10% More per Hire." Harvard Business Review, March 29, 2016. https://hbr.org/2016/03/a-bad-reputation-costs-company-at-least-10-more-per-hire.

data and AI as a framework and starting point for companies to leverage in their own work environments. These principles include:

- **Privacy and Security:** Although most companies currently have an existing data privacy policy, such policies are often broad in scope or geared toward customers and consumers. Principles for the use of data and AI should include a statement specific to employee privacy and security, and may explicitly state that data may not be used for the purpose incompatible with the specific purpose for which it was collected without employee consent.
- **Transparency:** The intended uses of data should be able to be clearly understood, explained and shared, including the impact on decision-making and the processes for raising and resolving any issues. In some cases, this may include an explanation of the algorithms involved in machine learning assisted analysis and how those algorithms are developed and "trained" to analyze employee data.
- **Integrity:** The principle of integrity is interpreted in a variety of different ways by companies according to their culture but is rooted in the concept of "positive intent." In addition to committing to the use of data in a highly responsible way, companies may also specify that the purpose of all AI is to augment and elevate humans rather than replace or diminish them, and that data usage should be sensitive to cultural norms and customs and aligned with company values.
- **Bias:** Although AI has been touted as the solution to unintended bias in many people-related processes, such as hiring, performance management and promotion, the risk of unintentional bias occurring within AI algorithms or the datasets used to train them is concerning. Principles around data and ethics should commit to continuous monitoring and correction for unintended bias in machine learning.
- **Accountability:** Individuals should be accountable for the proper functioning of AI systems and for unintended consequences arising out of its use. Companies should ensure that everyone involved in the lifecycle of an AI system is trained in AI ethics and that ethics is part of the product development and operation of an AI system. This may include the coders and developers responsible for creating the software, the data scientists responsible for training it, or the management of the company.

- **World Economic Forum "Human-Centred Artificial Intelligence for Human Resources Toolkit"[7]:** In cooperation with a task force of AI and HR experts including HR Policy Association, the World Economic Forum developed a framework that aims to equip HR professionals with a basic understanding of how AI works in the context of HR, guide

[7] "Human-Centred Artificial Intelligence for Human Resources." World Economic Forum. December 2021. https://www.weforum.org/reports/human-centred-ai-for-hr-state-of-play-and-the-path-ahead.

companies on the responsible and ethical use of AI, and help companies use AI-based HR tools effectively. The toolkit includes two useful checklists: one for assessing new AI tools before making the critical decision to implement them in a company and one for strategic planning regarding how to responsibly use AI in general.

- **The Data & Trust Alliance** is a not-for-profit consortium bringing together leading businesses and institutions to learn, develop and adopt responsible data and AI practices. Participating HR Policy Association members include American Express, CVS Health, General Motors, Humana, IBM, Johnson & Johnson, MasterCard, the Nielson Company, Pfizer, Under Armour, and UPS. The Alliance has released its Algorithmic Bias Safeguards for Workforce—criteria and education for HR teams to evaluate vendors on their ability to detect, mitigate and monitor algorithmic bias in workforce decisions.[8]

In addition to collaborative efforts, many employers have developed principles and best practices to build safeguards against potential harms in using AI and build trust both within and external to their company. It is important to note that many HR Policy companies do not use or produce biometric technologies, but nevertheless are leaders in developing robust AI oversight policies and practices. The following are just a small sample of such efforts.

- **Accenture's AI ethics and governance framework** takes an interdisciplinary approach that supports agile innovation and ensures governance of AI systems. Accenture emphasizes the need for organizations to put into practice well-defined AI principles, minimizing unintended bias, ensuring transparency, creating opportunities for employees, and protecting the privacy and security of data.

- **Microsoft's AI principles** – Fairness, Inclusiveness, Reliability & Safety, Transparency, Privacy & Security, and Accountability – are put into practice throughout the organization largely through the work of its Office of Responsible AI (ORA); the AI, Ethics, and Effects in Engineering and Research (Aether) Committee; and Responsible AI Strategy in Engineering (RAISE). The Aether Committee advises Microsoft's leadership on the challenges and opportunities presented by AI innovations. ORA sets AI rules and governance processes, working closely with teams across the company to enable the effort. RAISE, meanwhile, enables the implementation of Microsoft responsible AI rules across engineering groups.[9]

- **IBM's AI Ethics** features a robust, multidisciplinary, multidimensional approach to trustworthy AI, with three principles and five foundational pillars for ethical AI. IBM's AI

[8] "Algorithmic Bias Safeguards for Workforce Overview." The Data & Trust Alliance. December 2021. https://dataandtrustalliance.org/Algorithmic_Bias_Safeguards_for_Workforce_Overview.pdf

[9] "Responsible AI Principles from Microsoft." Microsoft. Accessed January 6, 2022. https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3Aprimaryr6.

> Ethics Board, a central, cross-disciplinary body to support a culture of ethical, responsible, and trustworthy AI throughout IBM, supports a centralized governance, review, and decision-making process for IBM ethics policies, practices, communications, research, products and services.[10]

AI, including that which uses biometric information, is not a monolithic concept, and therefore a "one-size-fits-all" approach to oversight may inadvertently expose workers to risk. AI use cases among HR Policy members vary considerably, depending on a wide variety of factors. The risk profiles of different uses of artificial intelligence vary considerably both in scope and in kind (i.e., safety, privacy, autonomy, or fairness). For example, using facial recognition technology during interviews presents a different degree of risk than an AI-powered predictive text tool, and raises different types of risks than GPS tracking features on a company-owned vehicle.

A "one-size-fits-all" model of oversight may inadvertently expose workers to risk, even while providing protections in the cases for which the oversight was aimed. Companies build these considerations into their technology oversight process, seeking to apply their principles on AI in a nimble manner as innovation accelerates. Any AI policy promoting ethics and trust without these characteristics will prove both insufficient and unviable.

New guidelines or standards should align with existing government policies and commonly adopted employer best practices. Any government guidelines on the use of AI in the employment context should be aligned with regulatory expectations across the federal government. For example, the U.S. Equal Employment Opportunity Commission (EEOC) recently announced an "Artificial Intelligence and Algorithmic Fairness" initiative, part of which will involve the "issuance of technical assistance to provide guidance on algorithmic fairness and the use of AI in employment decisions."[11] Any guidelines should be fully aligned with forthcoming guidance from the EEOC and any other agencies that promulgate AI workplace-related proposals.

Further, any government guidelines should be compatible with existing processes, procedures, and policies that employers have established to comply with the patchwork of state, federal, and international laws affecting the use of innovative technologies in the employment context. Employers have invested significant resources to develop compliance processes, procedures, and policies, and employers should be able to leverage these governance structures when aligning with the OSTP guidelines.

The use of technology in the employment context is regulated by many frameworks. In the United States alone, federal and state laws relating to anti-discrimination, labor laws, data

[10] "Ai Ethics." IBM. Accessed January 6, 2022. https://www.ibm.com/artificial-intelligence/ethics.
[11] "EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness." U.S. Equal Employment Opportunity Commission. October 28, 2021. https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness.

privacy, and AI-specific laws affect the use of technology in the employment context. A brief overview of these laws is below.

- **Anti-Discrimination:** Title VII of the Civil Rights Act (Title VII) prohibits discrimination in the employment context on the basis of race, color, religion, national origin, or sex. An employer can violate Title VII for disparate treatment or disparate impact. Disparate treatment occurs when similarly situated people are treated differently based on a protected class. Disparate impact occurs when facially neutral policies or practices have a disproportionately adverse impact on protected classes. Discriminatory intent is relevant to establish a claim of disparate treatment, but intent is not necessary for claims of disparate impact.

  Employers are also prohibited from unlawfully discriminating in the employment context based on age or disability due to the Age Discrimination in Employment Act and the Americans with Disabilities Act.

  Liability for discrimination may arise under anti-discrimination laws when employers use artificial intelligence systems that are trained on biased datasets or that infer or otherwise uncover protected class information and adversely impact members of the protected class. With respect to anti-discrimination, any new government guidelines should be co-extensive with existing anti-discrimination laws instead of imposing novel obligations that exceed existing law.

- **Labor Laws:** The National Labor Relations Act, enforced by the National Labor Relations Board (NLRB), is the cornerstone of American federal labor law and guarantees the right of private sector employees to organize and engage in collective bargaining. The National Labor Relations Act prohibits employers from interfering with employees' exercise of rights to engage in protected "concerted activity." The NLRB has determined that the NLRA prohibits employers from unlawfully surveilling employees' protected activity, which can occur when an employer acts in a way that is out of the ordinary to observe protected activity. Systems that automatically monitor employee activity, whether physical or digital, could be considered unlawful surveillance depending on the facts.

  Employers using artificial intelligence in the employment context, such as for workforce management, are already subject to the NLRA's obligations regardless of whether they are unionized. Any new government guidelines should therefore be compatible with the NLRA.

- **Data Privacy Laws:** Data privacy laws at the federal and state level directly affect the use of technology in the employment context.

  Federally, the Fair Credit Reporting Act (FCRA) regulates, among other things, how consumer reporting agencies use and share consumer information. A "consumer report"

is defined as information bearing on a consumer's credit worthiness, including information related to a consumer's credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. The FCRA requires consumer reports to be used for only permissible purposes, such as for employment. Employers must provide disclosures and obtain consents if using consumer reports.

In addition to the FCRA, employers must also navigate biometric information privacy laws in numerous states. For example, the Illinois Biometric Information Privacy Act (BIPA) prohibits organizations, including employers, from collecting and using biometric information unless they have provided notice and obtained written consent.

Meanwhile, congressional lawmakers are actively deliberating on comprehensive consumer privacy reform that may impact the use of technology in the employment context.

- **AI-specific requirements:** An increasing number of state and local laws are directly regulating the use of artificial intelligence in the employment context. The Artificial Intelligence Video Interview Act (AIVIA) in Illinois, for example, requires transparency, consent, and certain government reporting from employers who require candidates to record an interview and use artificial intelligence to analyze the submitted videos. In December of 2021, the New York City Council enacted a law requiring companies to obtain independent audits of certain algorithms used in the employment context. The law also prohibits the use of "biased" algorithms, although the law does not define the term. The new law poses several significant unaddressed concerns, including that immature technical standards may not be robust enough to address concerns around bias and therefore may deepen rather than address mistrust, and mandating third-party assessments will infringe on the privacy and security of personal information and potentially on confidential business information and IP rights.

  We believe that the federal government should coordinate its efforts to promulgate guidelines and requirements on artificial intelligence in the employment context. Where possible, we encourage OSTP to look for ways to promote consistency between federal and state efforts.

- **International efforts:** OSTP should also take note of international developments. In Europe, the EU General Data Protection Regulation (GDPR) prohibits solely automated decision-making that has legal or similarly significant effects unless the decision is made pursuant to an individual's consent or another exception applies. Decisions relating to employment may be similarly significant effects, and employers have taken steps to ensure humans remain in the decision-making process for employment accordingly.

  In addition, the European Union is considering an EU-wide regulation of artificial intelligence systems under the proposed Artificial Intelligence Act (AI Act). Though the

text remains under deliberation, the AI Act as introduced involves a risk-based classification system for artificial intelligence systems. AI systems in the employment context may be considered "high-risk," requiring employers using these systems to implement risk management processes, adopt governance structures, provide transparency, register the AI systems, and maintain documentation about the AI systems.

AI specific requirements are being discussed in many other jurisdictions, including in China. OSTP should track those discussions so that any promulgated guidance does not produce unnecessary compliance challenges, if possible, with forthcoming frameworks.

Concerns over third party assessment/audits before standards mature: Guidelines on the use of artificial intelligence in the employment context should not require employers to undertake third party assessments or audits. Mature, auditable, and accepted standards to evaluate bias and fairness of AI systems do not yet exist despite ongoing efforts at the National Institute of Standards and Technology, the International Organization for Standardization, and industry associations.

Until such standards are matured and accepted, assessment and audit outputs may be inconsistent, and thus ineffective at promoting fairness, may cause companies to forgo innovative technologies in the employment context despite their clear benefits, or may inadvertently deepen rather than alleviate distrust in such systems. Moreover, there are concerns that mandating third-party assessments will infringe on the privacy and security of personal information and potentially on confidential business information and IP rights.

Final product should be subject to notice and comment and stakeholder meetings: Finally, we believe that any guidelines prepared by OSTP in response to this proceeding should be presented for public comments through a notice and comment process prior to being finalized. Furthermore, we encourage OSTP to hold stakeholder meetings prior to the development and issuance of proposed guidance to solicit input from HR and the regulated community.

We appreciate the opportunity to provide our view and look forward to further lending any assistance we can to this important initiative by the U.S. Office of Science & Technology Policy.

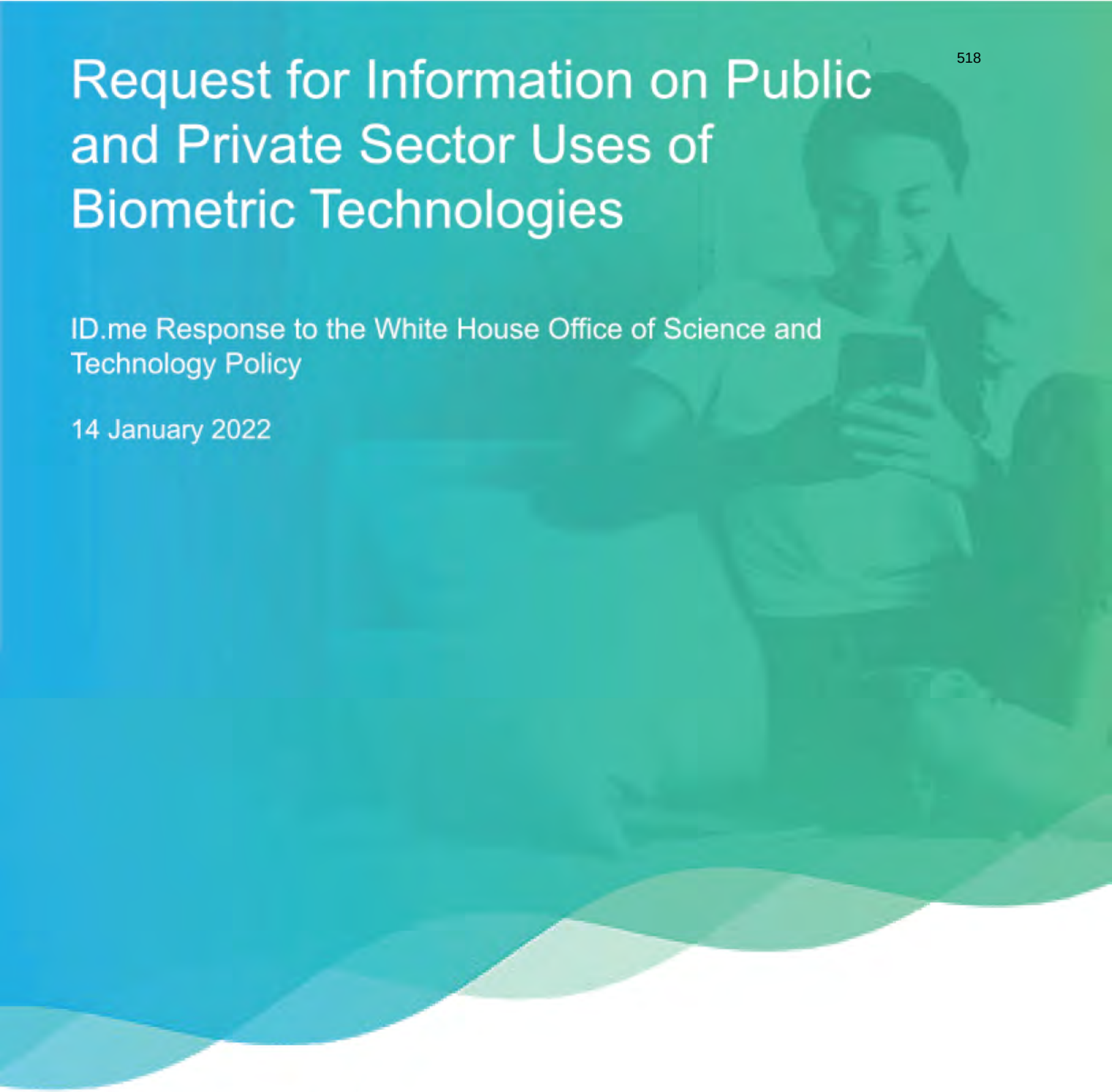
Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

ID.me

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Request for Information on Public and Private Sector Uses of Biometric Technologies



ID.me Response to the White House Office of Science and Technology Policy

14 January 2022

COMPANY DETAILS

Company Name: ID.me, Inc.

Address: 8280 Greensboro Drive, Suite 800
McLean, VA 22102

Respondent: Pete Eskew
Respondent's role: GM, Public Sector
Email: [redacted]

Public and Private Sector Uses of Biometric Technology

Comment provided by ID.me (industry) representative Pete Eskew, General Manager of Public Sector

Executive Summary

As the COVID pandemic accelerated the transition to digital services and the rapid at-scale adoption of evolving technologies, questions emerged about equitable access to government benefits and services. Two such technologies under scrutiny are facial recognition and face match for remote identity verification.

Facial recognition is a precise technical term used by organizations such as the National Institute of Standards and Technology (NIST). There are two distinct types of facial recognition: 1:many and 1:1, and they are frequently conflated. Media reports and even university studies often fail to distinguish between them correctly. For ease of understanding in this paper, we will refer to them as 1:many facial recognition and 1:1 face match. Simply put, 1:1 face match is equivalent to an airport agent comparing your face to the photo on your government ID card. 1:many facial recognition is equivalent to giving your picture to the same agent, on stage at a rock concert, and asking the agent to pick your face out of the crowd. When there are millions of possible matches, the challenge of finding the right face increases measurably. ID.me does **not** use 1:many facial recognition.

As the Credential Service Provider (CSP) to 68 million Americans, 10 federal agencies, 29 states, and over 540 companies, ID.me is fully committed to ensuring equitable access through our "No Identity Left Behind" initiative. Millions of Americans rely on us to gain access to critical services that are also vulnerable to exploitation by fraudsters, including, but not limited to taxpayer services, unemployment benefits and electronic prescriptions. We have an enduring obligation to ensure everyone has the opportunity to participate. Research shows that the most equity-enhancing solution for remote identity verification involves best-in-breed algorithms with human-in-the-loop relief valves.

Through meticulous research, planning, and product development, our hybrid solution promotes access, equity, and inclusion. We believe in transparency and appreciate this opportunity to share insights and lessons learned from research into these algorithms, which includes close collaboration with National Institute of Standards and Technology (NIST), independent assessments of face match vendors, and tests of our own identity verification orchestration platform.

Using artificial intelligence (AI) and biometrics can unlock convenience and time savings in an ethical and equitable manner that includes all groups. **To further strengthen identity assurance services for government programs, policy-makers could require human-in-the-loop relief valves and develop equity and inclusion metrics as part of a certification program.** This approach offers the best path to equity and access for all.

This comment is responsive to Topics 1, 2, 4, and 5 detailed in the Request for Information. In regards to Topics 3 and 6, ID.me's security policies are available at id.me/security, ID.me's privacy policy is available at id.me/privacy, and ID.me's full biometric data and consent privacy policy can be accessed at id.me/biometric. We can provide additional information upon request.

Key Takeaways

Four key takeaways are covered in detail in this paper:

- **Facial recognition and face match are frequently misunderstood**- Media reports and even university studies often fail to use precise terminology, leading to confusion among readers
- **Leading algorithms perform more equitably**- The best facial-recognition algorithms perform more equitably across demographic groups for 1:1 face match, such as an application in which a user is attempting to verify identity

- **Human reviewers and in-person verification control for any potential bias**- Peer-reviewed scientific studies show the best face-match results are achieved by fusing computer-based and human-driven facial recognition
- **There are significant benefits to AI and 1:1 face match that can be captured when implemented correctly**- AI and 1:1 face match can stop identity theft at scale, help state workforce agencies process legitimate claims faster, deter fraud, recover accounts easier, and bring justice for those who have been exploited

Introduction

As services and transactions increasingly move online and the economy becomes ever more digital, we have an enduring obligation to ensure everyone has the opportunity to participate. ID.me makes that real with our "No Identity Left Behind" initiative, a fundamental commitment to equity and access. Equity is why we do what we do. This paper shares insights on the application of AI technology and facial recognition in identity proofing at NIST SP 800-63-3 Identity Assurance Level 2 (IAL2). IAL2 is the federal standard that defines required and suggested controls for authenticating consumers to high-risk services. It is used to authenticate individuals for access to taxpayer services, to enable individuals to apply for unemployment benefits, and to empower consumers to access healthcare records in the public and private sectors.

Equity with respect to AI and facial recognition can be difficult to parse because there are many different applications of the technology and scrutiny on how law enforcement, in particular, uses it. Still, it is crucial to unpack how AI affects individuals from various communities and demographics as they attempt to access vital government programs. Given that AI and facial recognition can automate many workflows – enabling faster service delivery – the empirical data and truth must win over false perception.

Findings from a 2019 NIST report on facial recognition are important for policymakers because those findings relate to NIST SP 800-63-3 IAL2. Understanding how the leading face recognition algorithms affect equity and access in the context of NIST 800-63-3 can help policymakers understand if IAL2 requirements are equitable. That is vital to ensure optimal policies for equity and access and so the public understands the controls that are used. The best available research and data on these topics paint a clear and hopeful picture:

- The leading algorithms show extremely high accuracy across all demographics in IAL2 flows
- ID.me's internal tests across 15,468 images show no detectable bias tied to skin type
- Mitigating controls – such as human reviewers and in-person verification – control for any potential bias

The ID.me NIST IAL2 solution uses leading algorithms as validated by NIST and NIST-accredited laboratory testing. ID.me also employs two sets of human reviewers to check the technology's decision when AI denies access in the self-serve flow. That hybrid approach enables the leading algorithms, which are more accurate and less biased than trained humans,[1] to streamline access while mitigating any risk of bias.

The remainder of this paper goes beyond the headlines, unpacks the science, and explains:

- An overview of the 2019 NIST Face Recognition Vendor Test (FRVT)
- The difference between 1:1 face match vs 1:many facial recognition and why it matters
- The critical difference between a false positive and a false negative
- Confusion about facial recognition and pass rates by gender
- NIST's findings on the highest-quality algorithms
- How ID.me uses those findings and Trusted Referees to enhance equity in identity verification

[1] Crumpler, William, How accurate are Facial Recognition Systems - and Why Does It Matter?, Center for Strategic & International Studies https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter

An Overview of the 2019 NIST Face Recognition Vendor Test

In 2019, NIST conducted a study of more than 189 commercial algorithms from 99 developers to quantify the accuracy of facial-recognition algorithms for different demographic groups. Notably, many of those algorithms were immature and submitted by universities for research purposes. Test results from those algorithms should not be conflated with the performance of leading algorithms or algorithms actually used by IAL2 vendors.[2]

The results were based on a dataset of more than 18 million images of 8.5 million individuals. Key findings include[3]:

- **Algorithms perform differently:** The results show a wide range in accuracy across developers. The best performers produce "many fewer errors" than less-mature algorithms. Mature algorithms can therefore be expected to have smaller demographic differentials.
- **Demographic effect is vanishingly small:** False negatives – when a legitimate person's selfie fails to match a reference photo of his or her face – occur at extremely low rates across demographic groups. This is particularly important because a false negative error would deny a legitimate person access.
- **Leading algorithms perform more equitably:** The best facial-recognition algorithms perform more equitably across demographic groups for 1:1 face match in scenarios when a valid user is attempting to pass. False negative errors, which block valid people, are usually remedied on a second attempt.
- **Confusion about bias abounds:** Media reports and even university studies often fail to use precise terminology and, as a result, negatively skew the public discourse. For example, studies on gender, which related to face-classification algorithms, were falsely conflated with facial recognition, which looks for similarity.

What does this mean to organizations seeking to leverage those technologies to provide secure, equitable services? In short, they should understand how performance varies across types of algorithms (for example, 1:1 vs. 1:many), they should adopt only the highest-performing algorithms, and they should take action to mitigate known and potential performance limitations and errors. The sections that follow provide insights into how to take those actions to increase access, equity, and inclusion in digital identity.

The Difference Between 1:1 Face Match and 1:Many Facial Recognition and Why It Matters

Let's clarify why there are more errors tied to more complex use cases. As previously noted, 1:1 face match is equivalent to an airport agent comparing your face to the photo on your government ID card. 1:many facial recognition is equivalent to giving your picture to the same agent, on stage at a rock concert, and asking the agent to pick your face out of the crowd. With millions of possible matches, the challenge of finding the right face increases measurably.[4] Face match tied to NIST IAL2 deals specifically with 1:1 matching. The goal is to avoid a false negative so legitimate people are able to gain access. An additional goal is to avoid a false positive so an identity thief is unable to claim a different person's identity. This is a simplistic use case in the context of advanced technology.

With more than 129 million Android smartphones and 113 million iPhones in use in the U.S., 1:1 face match is already widely adopted by tens of millions of Americans. It has been proven at scale. *False negatives* occur when the technology fails to match the same person from the FaceID enrollment photo to the image captured during a specific attempt to unlock the phone. Apple and Android manufacturers allow for additional attempts and then prompt the user for a PIN if repeated attempts fail. While this content isn't covered by the 2019 NIST report directly, it provides a helpful frame to interpret the results of the study and how leading companies introduce additional controls to provide access pathways in the event the AI doesn't perform as intended.

[2] IAL2 vendors should disclose the specific algorithms they are using to certifying bodies so they can be evaluated for equity and inclusion.
[3] Grother, Patrick; Ngan, Mei; and Hanaoka, Kayee. Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects, 2019, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
[4] NIST benchmarks FPIR for 1M+ databases at 0.001, which is much higher than 1e-6 for 1:1,. but still excellent for many use cases.

The Difference Between False Positives and False Negatives

False-positive errors occur when two faces look similar but do not belong to the same person. Those errors are often embarrassing when humans make them in social interactions, such as mistaking a stranger for a friend. A false-negative scenario might involve failing to recognize an old friend you went to school with years ago.

False positives are much more common in 1:many facial-recognition scenarios. They are far less common in 1:1 face matching. After all, what are the odds that a person who steals your wallet looks just like you?

When verifying identity for government benefits, false-negatives would be associated with denying access to a person who is the same as in the government ID photo. The NIST report shows that false-negative errors are vanishingly small across demographic groups. To the extent false-negative errors occur across all algorithms, false-negative errors are actually lower in darker skin tones for 1:1 matching under certain conditions. Keep in mind, false negatives can often be remedied by trying a second time, as NIST notes.

The errors related to false positives are most relevant for fraud and unauthorized access. Those errors would not relate to legitimate people getting blocked from their rightful benefits, but rather to a criminal gaining unauthorized access. The NIST report notes “false positive differentials are much larger than those related to false negatives and exist broadly, across many, but not all, algorithms tested.” While this is relevant for 1:many anti-fraud scenarios, **the false-negative rate is the key metric in 1:1 identity verification as it deals with blocking a valid person.**

The NIST report highlights three additional findings related to error rates:

- False-negatives are often remedied by the user attempting a second time
- False-negative rates are extremely low across demographic groups
- False-negative errors tend to be algorithm specific

The Difference Between Face Classification and Facial Recognition and How They Perform Across Genders

The 2019 NIST report addressed confusion in the market about facial-recognition versus facial-classification algorithms as they relate to pass rates across genders. The excerpt from the NIST report that highlights the confusion, and how it affects perceptions of bias, follows with bolding added for emphasis by ID.me:

> Over the last two years there has been expanded coverage of face recognition in the popular press. In some part this is due to the expanded capability of the algorithms, a larger number of applications, lowered barriers to algorithm development, and, not least, reports that the technology is somehow biased. This latter aspect is based on Georgetown and two reports by MIT. The Georgetown work noted prior studies articulated sources of bias, and described the potential impacts particularly in a policing context, and discussed policy and regulatory implications. **The MIT work did not study face recognition, instead it looked at how well publicly accessible cloud-based *estimation* algorithms can determine gender from a single image. The studies have been widely cited as evidence that face *recognition* is biased.**
>
> This stems from a confusion in terminology: Face classification algorithms, of the kind MIT reported on, accept one face image sample and produce an estimate of age, or sex, or some other property of the subject. **Face recognition algorithms, on the other hand, operate as differential operators**: They compare identity information in features vectors extracted from two face image samples and produce a measure of similarity between the two, which can be used to answer the question ‘same person or not?’. Face algorithms,

> both one-to-one identity verification and one-to-many search algorithms, are built on this differential comparison.[5]

The NIST report goes on to compare false negative rates of the 52 most accurate recognition and matching algorithms to the classification algorithms in the MIT study: The best algorithms

> almost always gives (sic) false-non-match rate (FNMR) below 1%. These error rates are far better than the gender-classification error rates that spawned widespread coverage of bias in face recognition. In that study, two algorithms assigned the wrong gender to black females almost 35% of the time. The recognition error rates here, even from middling algorithms, are an order of magnitude lower. Thus, to the extent there are demographic differentials, they are much smaller than those that (correctly) motivated criticisms of the 2017-era gender classification algorithms.[6]

NIST Findings on the Highest-Quality Algorithms

NIST found leading algorithms to be exceptionally accurate, with far fewer errors and smaller differentials across demographic groups. Breaking this down a bit further, leading algorithms have false-negative rates that are "usually low with average demographic differentials being, necessarily, smaller still."[7] For false positives, results were a bit more nuanced. NIST found that "false positive differentials (across demographics) are much larger than those related to false negatives across many, but not all, algorithms tested."[8] That means only a few algorithms were found to have low error rates and low demographic differentials across both false negatives and false positives. For this reason, it is critical that conversations around accuracy account for the type and quality of the algorithm, as determined by NIST FRVT rankings.

After a rigorous screening and selection process, ID.me partnered with Paravision, which has been repeatedly benchmarked by NIST as a global accuracy leader and in internal testing has demonstrated 99.8% transactional pass rates (i.e., 2 in 1,000 false negative rates) at 1 in 100,000 false positive rates across a wide range of demographic groups. Generally, NIST found that false-negative errors are typically remedied by repeating an image-pair comparison, for example, uploading a new selfie. This means that if an individual fails to match on the selfie step on the first attempt, a second attempt typically passes. Those findings are consistent with how ID.me uses Paravision and actual pass rates in an applied setting.

How ID.me Uses the Findings and Trusted Referees to Enhance Equity in Identity Verification

ID.me is committed to our "No Identity Left Behind" initiative. We built our identity verification products by combining best-in-class technology with human-in-the-loop relief valves. From a technology standpoint, ID.me uses the best face-matching and presentation-attack detection (PAD), or face liveness, capabilities available in the market. We monitor associated error rates to detect any potential bias and to improve pass rates.

The ID.me face-match step has a 98.9% pass rate per user and a 98.5% pass rate per transaction in our self-serve flow, which includes variables such as image quality, lighting, and skew. Improvements to user-experience copy and to FAQ pages have increased the rate from 95% in March 2021. That gain shows the power of usability research, language accessibility, and data feedback loops to improve overall accessibility over time. Keep in mind, this pass rate is likely artificially low because it does not account for fraudulent attempts.

---

[5] Grother, Patrick; Ngan, Mei; and Hanaoka, Kayee. Introduction, page 14. Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects, 2019, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[6] Ibid. Page 54.

[7] Ibid. Page 10.

[8] Ibid. Page 5.

ID.me always implements secondary and tertiary controls to ensure no user is blocked by a false negative. To do so, we direct any user who fails the 1:1 face-match step to join a video chat with a human agent, a Trusted Referee. Trusted Referees primarily support users who encounter challenges, such as thin credit files and recent name changes, to attain verification. They are also available for face-match backup. In addition, we layer in a team to review automated decisions in real time to ensure two levels of human review in the online flow.

ID.me has verified more than 2.8 million people through Trusted Referees. Recently, ID.me also partnered with Sterling Identity to make in-person identity verification available at 650 retail locations across the country. New Jersey was the first state to adopt that identity verification method.[9] In so doing, ID.me offers multiple relief valves or escape hatches to ensure there is always a path forward for everyone. We are committed to the policy of "No identity left behind."

Technology Performance

ID.me uses Paravision, the top-ranked 1:1 face-matching algorithm developed in the U.S. and a leading algorithm globally across all leading benchmarks.

When it comes to false negatives, the algorithms in use by ID.me do not exhibit operationally significant differentials across demographics. It is also important to note that technology performance improves with each year. The leading algorithms, which were already equitable for 1:1 access in 2019, have advanced further over time and have been tested for performance gains against multiple demographic groups.

In March 2021, ID.me performed tests to look for bias related to face match and skin tone. We picked the Social Security Administration (SSA) for analysis as a broadly representative government agency that is not a target for fraud like state unemployment agencies. We then pulled a randomized sample of 627 individuals who had failed the face match step. We used the Fitzpatrick skin type framework to classify individuals: 1 being the lightest and 6 being the darkest.

A regression analysis did not yield any P values lower than .05 to correlate a given skin tone to face-match failure. We also ran a Chi-Square test for categorical variables and proportion tests for significant differences in proportions for group and reason while controlling for sample size. Neither test presented evidence of a relationship between skin type and failure reason. **See Appendix A for the March 2021 test results** .

In December 2021, ID.me performed additional tests to look for bias related to face match and skin tone per the Fitzpatrick Skin Type Scale. We picked the IRS as a separate agency that is also broadly representative and not an extreme target for fraud outside of tax season. We used 15,468 labeled images, collected in two sample sets for separate tests. The first tests were run to evaluate the selfie 1:1 match for any correlation between the Fitzpatrick Scale number and the rates of selfie match 1:1 failures. The second set was used to run the same tests on liveness data. Both samples passed the Chi Square Independence Test, indicating selfie-match and liveness-failure rates were independent of skin type value on the Fitzpatrick Scale. **See Appendix B for the December 2021 test results**.

Paravision performed a 1:1 face match demographic assessment using a highly diverse set of 70,000 face images against known match images and nonmatch images. The two metrics Paravision measured the dataset against are false non-match rate (rate at which it should have matched two images and didn't) and false-match rate (rate at which it matched two images when it shouldn't have). Within every ethnicity represented in the dataset, Paravision achieved a false non-match rate of less than 2 in 1,000 and a false match rate of less than 1 in 100,000. That means that out of the dataset and across all skin types and genders, 2 out of 1,000 should have been matched and weren't and 1 out of 100,000 were matched and shouldn't have been.

[9] GCN Staff. NJ offers in-person ID verification for online services: https://gcn.com/cybersecurity/2021/11/nj-offers-in-person-id-verification-for-online-services/316338/

For PAD, to ensure the selfie submitted is actually that user's face, ID.me partners with iProov, a leading vendor that has been independently tested by an evaluating body accredited by the NIST National Voluntary Laboratory Accreditation Program. The laboratory's accreditation also includes ISO 30107-3, the international standard that governs PAD. The UK National Physical Laboratory audited iProov's performance data, found the solution conformant with ISO 30107-3, and concluded that performance is "state of the art." In a trial conducted in 2021 under controlled conditions for a UK government agency with a diverse set of 500 individuals, balanced for ethnicity, age and gender, 99.91% of users were able to successfully complete the face-liveness process and pass.

iProov's service is already deployed in different regions across the world. As a result, performance variation can be compared across countries and regions with varying demographics. Signals of bias, including age, gender and ethnicity, are periodically calculated in order to seek out any potential inequities and enable remediation. In South Africa, like-for-like performance rates are not different from other regions, with no detectable differential pass rate that might negatively impact different demographic or ethnic groups. In Singapore, iProov passed bias testing administered by Govtech. **See Appendix C for more detailed information about iProov's PAD performance during testing through a NIST-accredited lab.**

The Role of Humans in the Loop

ID.me uses AI and facial recognition in an ethical manner. We believe every system must be built in a resilient manner to detect potential biases that might have otherwise gone unobserved and to ensure there is a real-time to near real-time path forward for any affected user, regardless of the reason. As a result, we employ teams of trained human agents to serve as relief valves – just like a smartphone will prompt the user for a PIN to unlock the device if too many selfie attempts fail. There is always a way forward and feedback loops too.

Peer-reviewed scientific studies[10] show that leading algorithms are more accurate than even forensic examiners, who specialize in facial comparison, at comparing two human faces. Additionally, human reviewers are subject to bias. That bias is inherently harder to standardize and control because it varies by each individual.

Studies emphasize that the best face-match results are achieved by fusing computer-based and human-driven facial recognition. That is exactly what ID.me does. If a computer algorithm cannot conclude that a given person matches a given photo in a government-issued ID, ID.me will then invoke human-based recognition by inviting the ID.me member into a video chat with one of more than 1,000 U.S.-based, specially trained Trusted Referees.

According to NIST 800-63-3, Trusted Referees "assist in the identity proofing and enrollment for populations that are unable to meet IAL2 and IAL3 identity proofing requirements or otherwise would be challenged to perform identity proofing and enrollment process requirements." Examples of populations include the disabled, elderly, and homeless; individuals with little or no access to online services or computing devices; unbanked individuals and those with little or no credit history; victims of identity theft; children under 18; and immigrants.

Our team of Trusted Referees represent all ethnicity groups in the U.S. census. We meet or exceed the level of minority representation in the U.S. population for the four largest non-white ethnicity groups: Black or African American; Hispanic or Latino; Asian; and two or more races. To further enhance equity, our Trusted Referees can verify individuals in 16 languages: English, Spanish, Haitian Creole, Korean, Arabic, Mandarin, Cantonese, Hindi, Farsi, Wolof, Nepali, Mandingo, Punjabi, Urdu, Russian, and American Sign Language.

[10] "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," https://www.pnas.org/content/pnas/115/24/6171.full.pdf

We believe that combining a talented pool of service-minded Americans with best-in-breed technology is the best way to ensure everyone has the same opportunity to participate in the digital economy. To date, we are the only credential service provider serving the public and private sectors that blends leading automated technologies with purpose-designed teams of human agents to ensure equitable access for all.

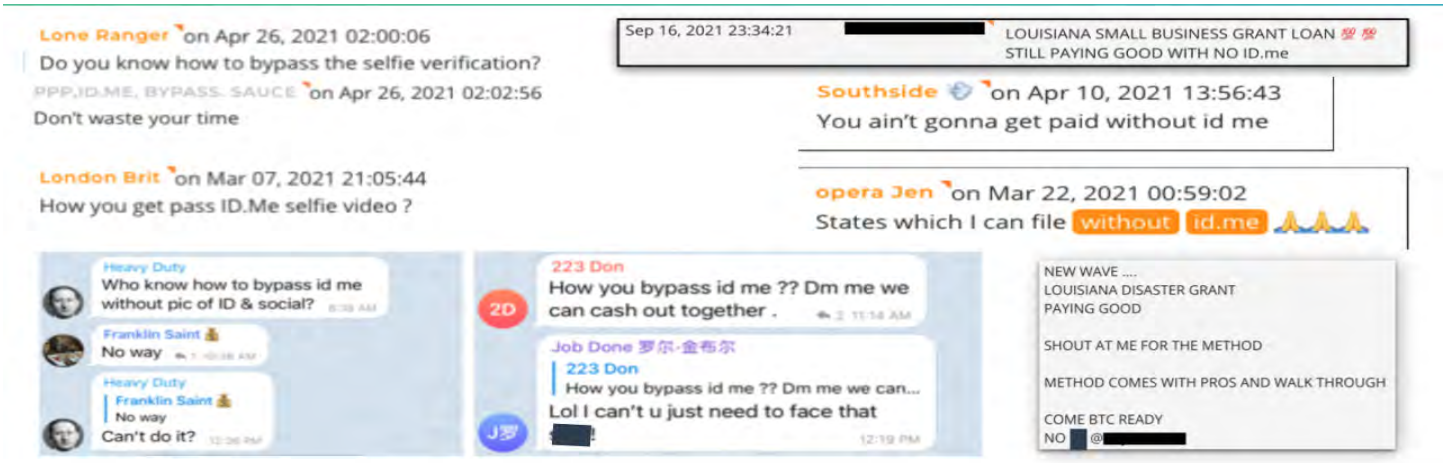
The Benefits of AI and 1:1 Face Match

People and the government agencies that serve them see clear benefits when best-in-breed AI and 1:1 face-match technology are paired with humans-in-the-loop. Those benefits include:

A State Workforce Agency (SWA) can process genuine claims faster. During the pandemic, the unemployment rate skyrocketed from 3.5% in February 2020 to 14.8% by April that year.[11] SWAs did not have the staff, technology infrastructure, or automated processes to keep up with the spike in demand. At the same time, international crime rings overwhelmed SWAs with fraudulent claims using stolen identity data, making it nearly impossible to distinguish legitimate applicants from fraudulent claims and causing large claim backlogs. By implementing NIST IAL2/AAL2 and PAD, SWAs stopped fraudulent claims while continuing to process legitimate claims the same day claimants completed identity verification. When Arizona implemented IAL2, new Pandemic Unemployment Assistance claims fell by 98.8% and existing claims fell by 68.3%, nearly all of which was fraud.[12] That enabled the SWA to focus on the smaller pool of legitimate claims and serve those applicants faster while dramatically reducing claim backlog.

Face Liveness actively stops identity theft at scale. Face liveness prevents an attacker from committing identity theft by ensuring the selfie submitted is an actual face and not an image, video or mask. This control actively blocked tens of thousands of identity theft attempts that would likely have succeeded and resulted in traumatized victims and lost funds.

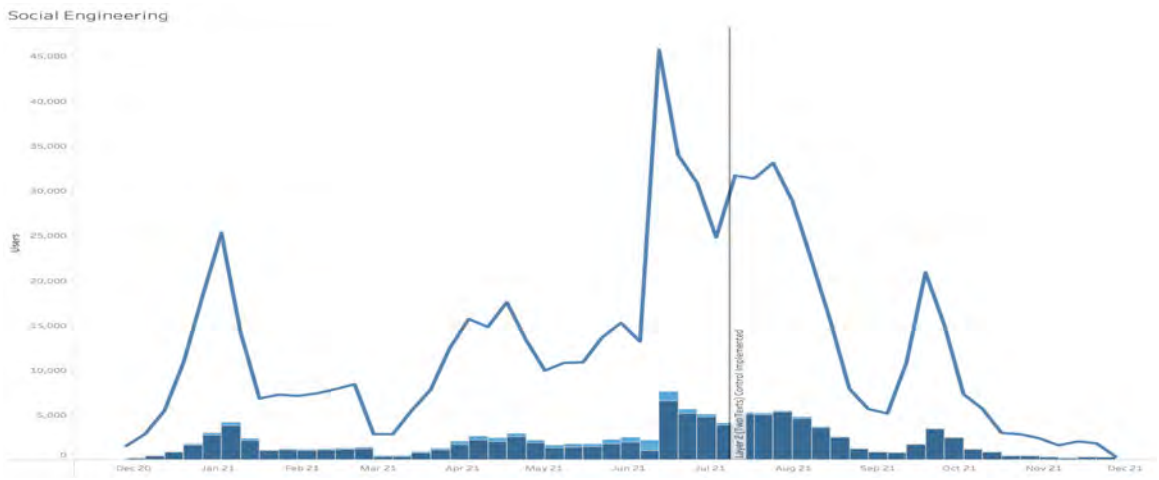
Face liveness deters bad actors from attempting fraud. By the time fraud is detected, the criminal is typically long gone, leaving the government and the identity theft victim with no way to know who filed the fraudulent application. With PAD, the fraudster's selfie is preserved as part of the application audit trail. Thieves are understandably reluctant to provide an image of their true face when committing a crime, so face liveness helps deter fraud and the associated increase in case backlog. If a thief is brazen enough to submit a selfie while committing fraud, that information can be helpful to government agencies as they seek to recover stolen funds. Dark web chatter among fraudsters underscores the strength of face liveness as a deterrent:



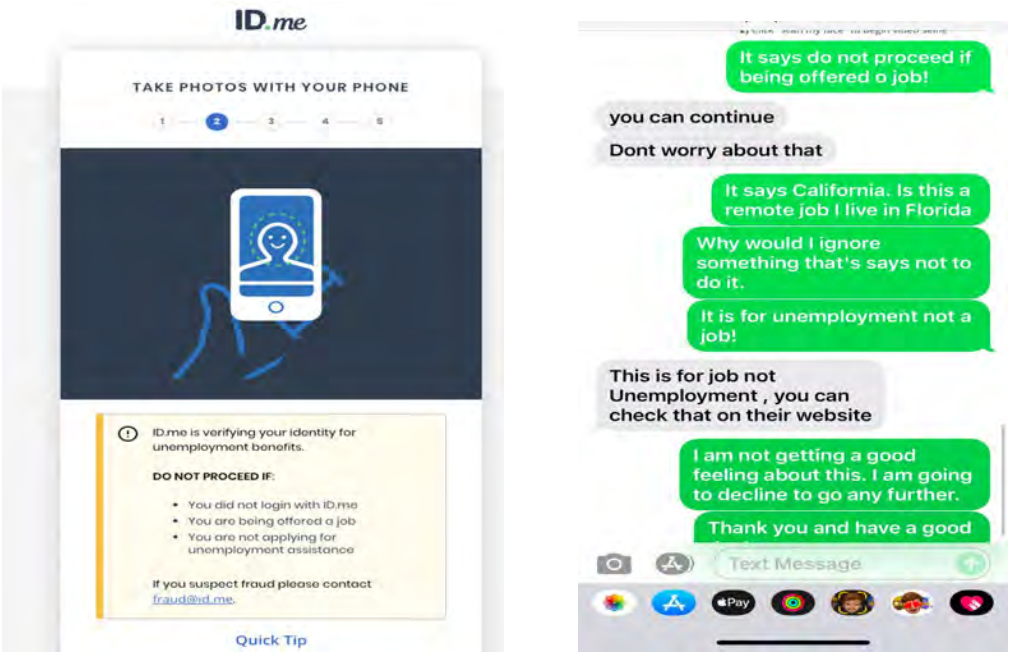
Dark-web chatter illustrates face liveness effectiveness.

[11] Bureau of Labor Statistics, accessed January 2022. https://www.bls.gov/cps/
[12] "How a Public-Private Partnership Provided Benefits to Eligible Individuals and Saved Billions for One State," September 2021. https://cdn.fedscoop.com/IDme-Arizona-PUA-Case-Study.pdf

Interstitial screens before the selfie stop imposter scams. Social engineering involves identity thieves manipulating a victim into divulging confidential information or taking actions that compromise portions of the victim's identity. For example, people might be fooled into giving their Social Security number over the phone to a fraudster posing as a law enforcement agent or persuaded to upload a picture of a driver's license to a fake online job site. Currently, the most popular imposter scams involve lottery winnings, dating sites, job applications, and fake retail sites. The figures below show the scale and speed at which organized crime syndicates can ramp up social-engineering attacks, the interstitial screens ID.me used to pierce the scams, and examples of actual text exchanges between potential victims and attackers after the contextual warnings alerted the victim to the scam.



Anti-social engineering controls enabled ID.me to stop tens of thousands of imposter scams a week



Interstitial screens prior to the selfie provide context to stop social engineering attacks and validated user feedback from an exchange with an attacker shows the screens are effective.

The rapid drop-off in attempted attacks reflects the effectiveness of controls enabled by the screens tied to the 1:1 face-matching process. The "Do Not Proceed" bullets actively target the most common false pretenses attackers use and let the victims know they are being tricked. Those measures have helped more than 100,000 people stop, or mitigate, the effects of identity theft over the past year.

It helps bring justice for those who have been exploited. In October 2021, the Pennsylvania attorney general brought charges against a caregiver at a facility for people with disabilities for "stealing personal information of several intellectually disabled people in his care to fraudulently apply for and receive Pandemic Unemployment Assistance funding."[13] The caregiver was unable to navigate the ID.me unsupervised flow with the victim's information because of adherence to NIST IAL2 fraud controls. When the victim's application was escalated to a video chat with an ID.me Trusted Referee, it became clear the victim was being manipulated by the caregiver. The ID.me Trusted Referee alerted the state, and the Pennsylvania attorney general's office took swift legal action.

Makes account recovery easier if someone loses a device. NIST SP 800-63B provides guidance on how to establish a new authenticator should someone lose access to a primary authenticator (typically a cell phone). Individuals can repeat the identity-proofing process or use an "abbreviated proofing process confirming the binding of the claimant to previously-supplied evidence."[14] The abbreviated pathway can be completed by submitting a selfie that is checked against the photo on the piece of identity evidence that was captured during original proofing. With a 1:1 face match between the new selfie and the image submitted during enrollment, account recovery can happen in seconds. In that scenario, people who lose their phones can recover their accounts and link to a new phone with less time tax than with other options, such as calling a help desk or going somewhere in-person.

Prevents account takeovers. Face liveness has prevented a significant number of account takeovers, particularly attacks against elderly users, because the criminal who stole the login credentials from the user is unable to pass the selfie check that ensures the same user who enrolled still controls the login.

Crafting a Path to a More Equitable Society

ID.me performed this analysis to improve understanding of AI and facial recognition as applied to authentication for government services. We hope it raises awareness of the benefits of AI in enabling faster service delivery – particularly during a time of crisis and heightened need. Using AI and biometrics in an ethical manner unlocks the convenience and time savings that are driving the growth of the digital economy in an equitable manner that includes all groups. Those gains should be realized with appropriate oversight.

Currently, OMB M-19-17 directs agencies to use "Federally or commercially provided shared services…to deliver identity assurance and authentication services to the public." OMB also calls for a certification program to ensure those shared services meet the NIST 800-63-3 standards at a given assurance level. To further strengthen identity assurance services, policy-makers could require human-driven relief valves and develop equity and inclusion metrics as part of that certification program.

On August 27, 2020, Pew reported, "States that were generous and quick to help workers were also quick to be targeted by scammers. In response, states have had to slow down the processing of claims, delaying payouts to people supposed to be getting them." During the pandemic, agencies were unable to simultaneously scale services to meet demand while also effectively stopping fraud using manual processes. A hybrid approach that fused best in class AI algorithms with human reviewers as a relief valve proved vital. Getting this approach right is critical to scale services during a time of great need.

The best performing systems are resilient. Combining algorithms with multiple layers of human review mitigates any potential bias that might arise. **This approach offers the best path to equity and access for all.**

[13] State of Pennsylvania, Attorney General Josh Shapiro website, Accessed on November 16, 2021. https://www.attorneygeneral.gov/taking-action/press-releases/ag-shapiro-arrests-caregiver-for-stealing-intellectually-disabled-clients-personal-information-to-get-nearly-90k-in-unemployment-benefits/

[14] National Institute of Standards and Technology Special Publication 800-63B, Section 6.1.2.3. https://pages.nist.gov/800-63-3/sp800-63b.html

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Identity and Data Sciences Laboratory at Science Applications International Corporation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

1.0 About the Identity and Data Sciences Laboratory (IDSL)

The Identity and Data Sciences Laboratory (IDSL) is an independent research organization within SAIC, a technology integrator for the US government. The IDSL is comprised of scientists, engineers, IT specialists, and program managers with demonstrated expertise in the test and evaluation of AI systems.

Since inception, the IDSL has carried out authoritative analyses and reporting on the performance of biometric identity systems, including face recognition systems. Much of our work has been in support of the Department of Homeland Security Science and Technology Directorate (DHS S&T). The IDSL operates the Maryland Test Facility (MdTF) in support of research conducted on behalf of the DHS S&T Biometric and Identity Technology Center (BI-TC). Starting with our work on the Air Entry-Exit Re-engineering (AEER) project we have tested well over 200 commercial biometric technologies in varied use-cases. Our technology evaluations have been provided to inform government agencies (DHS S&T, CBP, TSA, USCIS, OBIM, DOD, DOJ, and others) as well as published in peer-reviewed scientific journals[1]. Our expert staff are regularly invited to present our findings at conferences within the US and internationally. IDSL applied research addresses topics including biometric system performance, demographic group fairness, and human-algorithm teaming. We are using this insight to inform the development of international standards, including technical editorship of ISO/IEC 19795-10 on quantifying biometric system performance variation across demographic groups.

Given this relevant background, we are pleased to respond to the White House Office of Science and Technology Policy (OSTP) request for information (RFI) titled "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies". In the sections below, we provide responses to topic areas outlined within the RFI.

2.0 Responses to RFI Topic Areas

2.1 Descriptions of use of biometric information for recognition and inference

As defined by OSTP, the definition of biometric technology to include both individual recognition and cognitive/emotional state inference encompasses a wide range of disparate technology. Because of foundational differences in these two kinds of computer applications, care is often taken to separate the two in the scientific community. For example, there are internationally adopted standards that define the term "biometrics" as "automated recognition of individuals" based on their behavioral and biological characteristics" (emphasis ours)[2]. This definition has also previously been adopted by agencies in the U.S. Government[3]. By this definition, biometric recognition involves a comparison between two biometric samples to determine whether they are of the same individual.

[1] MdTF Publications. https://mdtf.org/Research/Publications.
[2] ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37:"Biometrics Recognition" term 37.01.03. https://www.iso.org/standard/66693.html
[3] DHS OBIM defines a biometric as "a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition". https://www.dhs.gov/biometrics

Biometric recognition has well defined scientific underpinnings, metrics, and international standards that have been in existence for nearly 20 years[4]. Indeed, biometric systems may be one of the most well tested current applications of artificial intelligence (AI)[5]. For nearly a decade, biometric systems have been deployed in a variety of scenarios including to facilitate identity determination at international borders and airport checkpoints, for individual identification in both public and commercial settings including the identification of missing persons and those involved in human trafficking, and for access to personal electronic devices.

In contrast, technology for inference of cognitive and/or emotional states based on a single sample are varied in their domain of application and poorly understood. The scientific basis for these technologies also varies dramatically (some basis for emotion recognition[6] vs no basis for criminality[7]). Additionally, we are not aware of any international standards for the test and evaluation of these systems. Despite growing commercial deployment in areas such as hiring and exam monitoring, these technologies are rarely, if ever, vetted for validity by independent third parties.

As an entity specifically focused on AI system test and evaluation, the bulk of our responses to this RFI are centered on biometric technology as used for recognition since this is where our primary experience lies. Our position is that it may be timely to consider similar scrutiny to other AI systems in the public domain.

2.2 Procedures for and results of data-driven and scientific validation of biometric technologies

With support from the Department of Homeland Security Science and Technology Directorate, the IDSL conducts data-driven scientific evaluations of biometric technology in government use-cases. At a high level, there are three kinds of biometric evaluations as defined by ISO standards[8] enumerated below. In Sections 2.2.1 – 2.2.3, we outline each evaluation type, including measurement setup, evaluation procedure, specific measures, outcomes and error rates.

Technology evaluations are typically centered on a specific component of a biometric system (e.g. a matching algorithm) and use previously acquired biometric datasets with large sample sizes. This type of testing is appropriate for measuring the limits of a technology's performance and for comparison of different technologies. This testing is not appropriate for answering questions about how a technology performs in a specific application.

[4] ISO/IEC JTC 1/SC 37 Biometrics. https://www.iso.org/committee/313770.html
[5] NIST: Biometrics. https://www.nist.gov/programs-projects/biometrics.
DHS S&T Biometric and Identity Technology Center (BI-TC). https://www.dhs.gov/science-and-technology/BI-TC.
The Maryland Test Facility. https://mdtf.org.
[6] Barrett, Lisa Feldman, et al. "Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements." Psychological science in the public interest 20.1 (2019): 1-68.
[7] Bowyer, Kevin W., et al. "The "Criminality From Face" Illusion." IEEE TTS 1.4 (2020): 175-183.
[8] ISO IEC 19795-1: Information technology–biometric performance testing and reporting-part 1: Principles and framework. https://www.iso.org/standard/73515.html.

Figure 1. Maryland Test Facility test bay set up for a "Rally" scenario test.

Scenario evaluations center around a specific technology use-case (e.g. airplane boarding) and test a full multi-component biometric system (i.e. including any acquisition devices, databases, and algorithms) with test volunteers in a controlled environment. This type of testing gathers new biometric samples to answer questions about how a technology performs for a specific intended use (**FIGURE 1**).

Operational evaluations assess the performance of a technology in the fielded environment. This testing measures the performance of the system within a specific location and environment (e.g. a face recognition system installed in at a specific airport terminal). While most operationally relevant, reduced experimental control in operational evaluations makes it harder to identify the key factors influencing performance.

2.2.1 Technology evaluations

By far the most common category of biometric evaluation are what's known as technology evaluations. Technology evaluations typically rely on large static test datasets and can be used to test performance limits and track the performance of algorithms over time, motivating innovation. Tests are typically executed on biometric algorithms in isolation, disentangling them from the larger workflows of full operational biometric systems (i.e. cameras, databases, administrative systems, etc.).

The IDSL regularly executes technology evaluations to report on both the state of the biometric industry and industry progress. To execute technology evaluations, the IDSL maintains a sophisticated data storage, processing and reporting infrastructure in house at the Maryland Test Facility. This computational testbed consists of over 25 distinct server systems, 100 virtualized software platforms for redundancy, and 20 TB of on-premise storage.

The protocols, measures, and outcomes for technology testing are defined in the international standard ISO/IEC 19795-2, which has been in place since 2007[9]. Typically, experimental setup in a technology test involves a large static dataset of biometric samples with ground truth. Biometric algorithms are used to create biometric templates, or mathematical models of the physiological sample. These templates can then be compared to calculate a similarity score. Once this process has been executed on many biometric sample

[9] ISO/IEC 19795-2:2007 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation. https://www.iso.org/standard/41448.html

pairs (face pairs, iris pairs, etc.) the generated scores are separated into two categories; those that came from biometric samples that should match (individual A's face image on day 1 and individual A's face on day 2) and those that should not (individual A's face and individual B's face). These pairs are called mated and non-mated pairs respectively. Using these pairs, two foundational error rates for a biometric algorithm can be calculated, namely the false non-match rate and the false match rate. Both these error rates measures are specific to a match or discrimination threshold. Its common in technology testing for these error rates to be calculated over a range of thresholds to produce summary statistics, such as detection error tradeoff curves.

The main benefits of technology evaluations of biometric systems lie in their reproducibility. This is advantageous because 1) the findings can be replicated by others and used to improve their systems (assuming data availability) and 2) the findings can be replicated longitudinally as algorithms or other system components improve. In this way technology evaluators can monitor and report on industry progress. We have previously used technology evaluations to identify a phenomenon named "demographic clustering", by which face recognition algorithms tend to score different people of the same race, age, and gender as more similar than those who do not share demographic characteristics[10]. We first pointed out this "homogeneity effect" in 2019 and subsequently replicated it with numerous algorithms and on other datasets[11].

Technology testing has important limitations. Much like comparing two formula 1 race cars on a test track, you are able to see what is achievable, but you are unlikely to see comparable performance driving your sedan around town. Technology testing will miss important aspects of operational system performance. For example, a technology evaluation may not discover a scenario in which a facial recognition camera systematically cannot find faces (and therefore take pictures) of individuals with darker skin, since these evaluations starting point is captured images. Furthermore, the static nature of the datasets used in technology evaluations means that they often do not represent changing circumstances in the real world. For example, when the COVID-19 pandemic led to large scale public masking requirements, the datasets used in typical face recognition technology evaluations no longer reflected the facial characteristics of individuals a face recognition system was likely to encounter in situations like an airport or border crossing.

In summary, technology evaluations of biometric technologies are well defined processes that provide important information, particularly to biometric system developers. However, they are not sufficient to anticipate the full range of issues a biometric system might experience once deployed in a robust, operational environment. They are one part of a larger, necessary testing regime to ensure the effectiveness and equitability of biometric systems.

[10] Howard, Sirotin, Tipton, Vemury. Quantifying the Extent to Which Race and Gender Features Determine Identity in Commercial Face Recognition Algorithms. DHS S&T Technical Paper Series. (2021). https://www.dhs.gov/sites/default/files/publications/21_0922_st_quantifying-commercial-face-recognition-gender-and-race_updated.pdf

[11] Grother, Ngan, Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

2.2.2 Scenario evaluations

Scenario evaluations of biometric technologies simulate a full biometric application and its real-world deployment environment. Unlike technology evaluations, scenario evaluations measure error and success rates on full biometric systems (i.e., algorithms, acquisition devices like cameras, and any needed databases). Further scenario evaluations measure performance using new data collected from test volunteers. In every new evaluation, volunteers utilize biometric systems just as they would in a real-world deployment, allowing unique insights into the efficiency of the system (e.g. how long it takes to use) and on human perceptions of the system (e.g. how satisfied are the users).

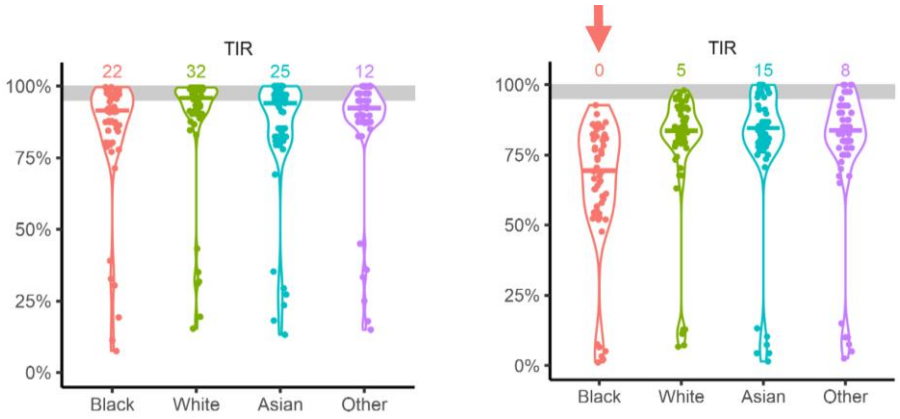


Figure 2. *True Identification Rate (TIR) of face recognition systems without face masks (left) and with face masks (right) disaggregated by self-identified Race. Note greater reduction (arrow) due to masks for those self-identifiyng as Black.*

To date, the IDSL has primarily focused on scenario evaluations of both staffed and automated biometric systems within the travel environment[12]. We curate and maintain an ethically collected structured dataset of over 137,000 face, fingerprint, and iris images of over 2,000 unique persons together with metadata on demographics and phenotypes (e.g. skin tone). For our scenario tests, we recruit volunteers from the local area stratified by race, gender, and age or other factors as needed for each evaluation. We have tested well over 200 face, fingerprint, and iris recognition systems with over 5,000 unique volunteer visits to the Maryland Test Facility. The IDSL uses dedicated data processing systems for computing standard measures of biometric performance and generating reports.

Using this scenario test model, scientists at the IDSL have identified important new insights into biometric performance. For example, in a widely cited 2018 study that explored the effect of camera on bias, we found evidence that differential performance in face recognition could largely be traced to differences in camera's abilities to capture high quality photographs of individuals with difference skin tones[13]. This impact of camera had largely been ignored in discussions of "bias" in face recognition but plays a key role in creating a more equitable system. Additionally, using the scenario test model the IDSL was able in 2020 to collect the first

[12] Howard, Blanchard, Sirotin, Hasselgren, Vemury An Investigation of High-Throughput Biometric Systems: Results of the 2018 Department of Homeland Security Biometric Technology Rally. https://mdtf.org/publications/rally-results.pdf.
[13] Cook, Howard, Sirotin, Tipton, Vemury. Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems. https://mdtf.org/publications/demographic-effects-image-acquisition.pdf

dataset of masked individuals since the onset of the COVID-19 pandemic. We were able to quantify the expected reduction in face recognition performance due to masked face occlusion and critically demonstrated that this performance reduction was not equivalent across demographic groups (individual with darker skin saw larger reductions in performance than those with lighter skin, **FIGURE 2**)[14]. This insight motivated improvements in masked face recognition performance across industry and helped created more equitable face recognition systems.

Lastly, we have found that scenario testing at the IDSL forecasts error cases in the operational environment. In particular, scenario testing predicts the use errors and differences in performance associated with demographic factors. On the other hand, results observed in technology tests depend critically on the type of data used for the evaluation. For instance, the performance of face recognition technologies in NIST's FRVT tests depends critically on the type of dataset used[15]. In our own assessments, we find that the performance of system components is inter-dependent with algorithm results depending strongly on the acquisition camera used (**FIGURE 3**)[16]. We strongly believe that, like other forms of AI, biometric technologies must be proven in scenario tests in order to understand their likely performance within the operational environment.

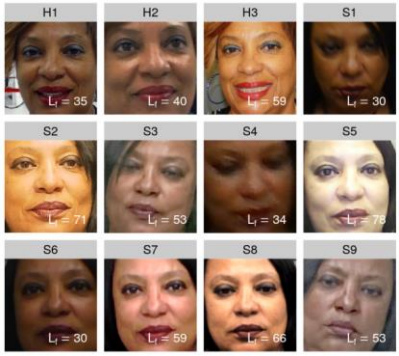


Figure 3. *Images of a person gathered using different biometric cameras. Note the change in appearance and skin tone. Images S1-S9 were collected on the same day under consistent lighting conditions.*

2.2.3 Operational evaluations

The final variety of biometric system evaluation is known as an operational evaluation. The protocols and procedures for this form of testing is defined in international standard ISO/IEC 19795-6, which was published in 2012[17]. Operational evaluations provide the most direct insight into how a biometric system is performing as deployed in a given implementation. However, despite their value, operational evaluations of biometric

[14] Y. B. Sirotin and A. R. Vemury. "Demographic variation in the performance of biometric systems: Insights gained from large-scale scenario testing." In Virtual Events Series – Demographic fairness in biometric systems. EAB, March 2021. https://mdtf.org/publications/ EAB2021-Demographics.pdf.
[15]Grother, Patrick, et al., "Onoging Face Recognition Vendor Test (FRVT) Part 1: Verification."
[16]Hasselgren, Jacob A., et al., "A scenario evaluation of high-throughput face biometric systems: select results from the 2019 Department of Homeland Security Biometric Technology Rally." DHS S&T Technical Paper Series. (2020). https://www.dhs.gov/sites/default/files/publications/2021_st-01_2019selectrallyresultstip20201104_revised_3046.pdf
[17] ISO/IEC 19795-6:2012 Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation. https://www.iso.org/standard/50873.html

systems can be challenging to resource and execute properly. Consequently, they are relatively rare compared to scenario and laboratory evaluations of biometric systems. The two main challenges when conducting operational evaluations of biometric systems are lack of experimental control and lack of ground truth information. For example, it can be arduous to collect accurate race, gender and age information from people in crowded operational environments, like airports or train stations. It can also be challenging attributing observed effects directly to specific causes because of many nuicanse factors.

To perform operational evaluations, the IDSL team goes on location to observe and record the operational environment, the technology configuration, and first-hand observations of user interactions with the system. The IDSL can receive and process operational sample-based and transactional data to generate performance measures. We believe operational evaluations of biometric systems provide the most direct evidence of system performance in the field to inform system developers and system owners.

2.3 Security considerations associated with a particular biometric technology

Discussion topic 3 in OSTP's RFI deals with the security of biometric systems, particularly around spoofing and more traditional software system security (i.e. encryption, data access/audit, etc.). We anticipate many respondents will provide material on these two topics. However, we wanted to raise a security issue that OSTP might not yet be aware of that relates specifically to face recognition applications. Often when face recognition is used for security applications, the digital images that require identification can come from poor quality cameras and challenging environments. There is a strong incentive to improve the utility of such low-quality images for biometrics, especially when this may help solve a crime.

However, the performance of biometric systems with altered digital images, even if altered with the intent to enhance, is generally not well understood and has been suggested to lead to potential law enforcement errors[18]. Further, recent advances in AI have made it easier to perform such alterations without needing technical skill[19]. This creates additional concerns regarding privacy whereby security equipment previously suitable only for detecting suspicious activity may now become useful for biometric surveillance.

To avoid errors and privacy implications that may be caused by image manipulation in security applications, it is important that biometric systems include specific descriptions of their intended context of use and that any performance information be clearly associated with this context of use.

2.4 Exhibited and potential harms of face recognition technology

The deployment of face recognition technologies undoubtedly carries with it potential harms, some of which have been realized as these technologies are increasingly used in the real world. First, in regards to the validity of the science, there is little doubt the human face contains characteristics that allow for individual recognition. Human beings innately perform such functions on a daily basis when we recognize friends,

[18] Garvie, Clare, et al., "The perpetual line-up. Unregulated police face recognition in America". Georgetown Law Center on Privacy & Technology. (2016). https://www.perpetuallineup.org/

[19] Some examples: research from Google (https://ai.googleblog.com/2021/07/high-fidelity-image-generation-using.html) and of a tool easily available online (https://github.com/TencentARC/GFPGAN).

family, co-workers, etc. It stands to reason that computer processes could similarly carry out such tasks, a notion which has been repeatedly validated by over 20 years of government and industry testing.

However, just because a given technology works in the general case, does not mean it works equally well for all groups of people. Additionally, a technology that works well in the general case can also have idiosyncrasies that cause it to fail in predictable ways. Both of these conditions are true for face recognition. Many scientists, IDSL staff included, have documented error rates that can differ for individuals based on their demographics in face recognition. We coined the, now widely adopted, term "demographic differentials" to describe these effects in 2018[20]. While studying these phenomena is important, IDSL scientists have also pointed out that solving for this situation may not fully solve issues of "bias" in face recognition. In 2021, IDSL scientists highlighted an often overlooked but nearly universal characteristic of face recognition. Face recognition algorithms judge different individuals who share demographic characteristics (same race, gender age, etc.) as more alike than those that don't. We used the term "broad homogeneity" to describe this effect and pointed out that no other major biometric modality does this, yet it has somehow become accepted in face recognition[21].

We believe this clustering by demographics may be one source of potential harm in face recognition deployments when used for law enforcement. The fact that broad homogeneity exists means that identifications against galleries that are demographically skewed (majority male, for example) could have unequal false positive identification rates. Implementers of face recognition workflows should be aware of this effect and its consequences. Training may help avoid adverse impacts that stem from this phenomenon.

2.5 Exhibited and potential benefits of face recognition technology

The deployment of face recognition systems has undoubtedly benefitted the general public in many ways. One of the clearest examples is in the travel environment, where face recognition applications have sped airplane boarding and border crossing. Prior to the introduction of automated face recognition in these environments, identity verification tasks were performed by exclusively by humans. However, humans have well documented shortcomings when it comes to identifying unfamiliar faces. Humans also have limitations in terms of attention. This makes automated face recognition an attractive choice to both improve the effectiveness and efficiency in these environments.

2.6 Governance programs, practices, and procedures

All IDSL scenario test activities conducted at the Maryland Test Facility receive approval from an external Institutional Review Board (IRB) to ensure that ethical and data safeguards are met. Additionally, all data collected as part of our work with DHS S&T is maintained in accordance with a Privacy Threshold Analysis approved by the DHS Privacy Office. As part of standard practices required by the IRB, all human-subjects that participate are properly informed about the test and provide explicit consent to participate.

[20] Howard, Sirotin, Vemury. The Effect of Broad and Specific Demographic Homogeneity on the Imposter Distributions and False Match Rates in Face Recognition Algorithm Performance. https://mdtf.org/publications/broad-and-specific-homogeneity.pdf
[21] Ibid., 10

The IDSL conducts two forms of informed consent for all test events: group consent and individual consent. In the group consent, all human-subjects are informed of what data will be collected and how their data will be protected. In the individual consent, human-subjects are called into private interview rooms with doors and white noise to guarantee privacy to each human-subject while going over consent forms. Each human-subject is asked for explicit permission to reproduce any images collected during the test in publication materials; subjects that opt-out are not excluded from the test.

All data collected by the IDSL is associated with a unique subject-ID, separated from any personal information. This protection is to avoid personally identifiable information (PII) from being leaked or compromised. The IDSL's datasets are also sequestered to prohibit datasets from being taken advantage of by developers of AI/ML systems. Developers of AI/ML systems will leverage all available information in developing their system, but this can result in 'overfitting' (a phenomenon where you can do better on the data you know and paradoxically worse on new data) or even cheating[22]. For this reason we limit access to our datasets and routinely gather new data to prevent such practices, even when unintentional.

We believe technology and scenario evaluations play a critical role in biometric system governance prior to system deployment by reducing the odds that non-performant or unfair systems are put into real-world applications. However, following system deployment, additional performance auditing steps are also necessary to ensure that real-world conditions have not adversely impacted the expected performance of a biometric system. Because post-deployment performance evaluations are likely to contain PII collected outside the lab context, the IDSL utilizes separate systems for processing data gathered as part of an operational evaluation. Operational data used for performance evaluations resides on Government systems granted Authority to Operate (ATO) and is used in accordance with any required Privacy Threshold Assessments. Steps and considerations when conducting post deployment, operational evaluations of biometric systems are discussed in Section 2.2.3.

3.0 The case for requiring independent testing of biometric systemsl

As real-world deployments of AI systems multiply, the public is becoming increasingly aware of the need to evaluate the performance of AI systems. Our research shows that, when these systems are used to establish the identity of individuals and make inferences about individuals, they can make errors, sometimes conflicting with notions of 'fairness' or 'equitability'. Our experience suggests that vendor-reported efficacy claims may not always align with real-world performance. Depending on the application, biometric system errors may carry significant costs or harms at both the individual and group level[23].

[22] Markoff, John. "Baidu team is barred from A.I. competition." The New York Times. (2015). https://www.nytimes.com/2015/06/04/technology/computer-scientists-are-astir-after-baidu-team-is-barred-from-ai-competition.html and Quach, K. (2020, June 18). How a kaggle grandmaster cheated in $25,000 ai contest with hidden code – and was fired from Dream SV job. The Register - Biting the hand that feeds IT. Retrieved January 14, 2022, from https://www.theregister.com/2020/01/21/ai_kaggle_contest_cheat/

[23] Hill, Kashmir. "Wrongfully accused by an algorithm." The New York Times (2020). https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Despite technology developers racing to create and implement AI systems, few entities have the capability and focus, like the IDSL, to test the performance of these systems. The situation is comparable to the field of drug development prior to The Federal Food, Drug, and Cosmetic Act of 1938, which required new drugs to be shown safe and prohibited false therapeutic claims[24]. AI systems may not have direct effects on human life, but their increasing ubiquity and scale also carry the potential for significant harms.

Some recent discussions have focused on AI audits as means to ensure that harms of AI systems are managed[25]. While important, we believe that audits in the absence of independent third-party *performance testing* are insufficient to ensure that systems meet required benchmarks for performance and equitability.

The IDSL has a unique mission to evaluate biometric systems to better understand their likely performance in the field and to provide quantitative empirical evidence to inform analyses of these systems' potential harms, including harms to protected demographic groups. Currently, there is little incentive for companies to perform independent third-party tests of their biometric technology products. Conversely, companies have strong incentives to present optimistic performance claims in marketing that conflate results of technology testing performed during AI training and real-world performance.

Without robust regulations and requirements for rigorous scientific testing, like the kind carried out by the IDSL, few biometric system developers have the incentive to test their systems. Indeed, the US government currently shoulders much of the cost associated with testing these technologies. The costs of deploying untested systems will be realized in unexpected technology failures, including potentially unfair systems. These issues may be realized only after deployment, when changes or adjustments become more costly. Worse still is the possibility that such issues may simply go undetected, leading to increasing opportunity periods for harms to manifest. This will undermine public trust in biometric systems.

We believe that independent third-party scenario and operational testing with demographically diverse people should be a prerequisite to marketing biometric systems for any high-risk applications that carry potential for harms at the individual or the group level. We hope the information we have provided herein can inform the development of an AI bill of rights[26].

Durkin, Erin. "New York tenants fight as landlords embrace facial recognition cameras." The Guardian (2019). https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex

[24] FDA. "Milestones in U.S. Food and Drug Law." https://www.fda.gov/about-fda/fda-history/milestones-us-food-and-drug-law

[25] The New York City Council - File #: Int 1894-2020 (nyc.gov) https://legistar.council.nyc.gov/LegislationDetail.aspx

[26] Lander, Eric and Nelson, Alondra. "ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World." The Office of Science and Technology Policy. (2021). https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Information Technology and Innovation Foundation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

Re: RFI Response: Biometric Technologies

Dear Dr. Lander,

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Office of Science and Technology Policy's (OSTP) request for input on the use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.[1]

ITIF is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

SUMMARY

Overall, biometric technologies offer many benefits to society, improving convenience, security and commerce. However, biometric technologies are not a monolith. Within biometric technologies for recognition and inference there are component technologies that not only differ in their application areas, but in the computational processes they employ and the data they are trained on. As such, they present unique considerations, benefits, and potential harms, and require distinct policy approaches. Some nascent technologies that require biometric data to function, such as age estimation and augmented and virtual reality, offer unique benefits to protecting children in online spaces, reducing barriers to opportunity, and enhancing equity and inclusion. Because of the scope and scale of biometric data they need to collect for their core functions, some biometric technologies can also present unique risks, such as autonomy and discrimination risks from inferred data about preferences from involuntary or subconscious movements or reactions. The government can help address and mitigate many of these risks by increasing and expanding independent public testing of these systems (as NIST has done for some technologies); developing performance

[1] "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Federal Register, October 8, 2021, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.

standards for any systems that use biometric information procured by the federal government; and developing more diverse training and evaluation datasets for recognition and inference.

Sincerely,

Hodan Omaar
Policy Analyst, The Information Technology and Innovation Foundation
[redacted]

Daniel Castro
Vice President, The Information Technology and Innovation Foundation
[redacted]

(1) PROCEDURES FOR AND RESULTS OF DATA-DRIVEN AND SCIENTIFIC VALIDATION OF BIOMETRIC TECHNOLOGIES.

The RFI broadly refers to any system that uses biometric information for the purpose of recognizing or inferring information about an individual as "biometric technology." Biometric information includes data derived from an individual's physical characteristics (e.g., DNA, face, or fingerprints) or behavioral characteristics (e.g., gestures, gait, voice).

It is important to clarify at the outset that technologies that use biometric information to estimate the similarities between two individuals (what the RFI calls 'recognition') and those that use biometric information to predict attributes about an individual such as age, gender, and emotion (what the RFI calls 'inference') are completely different. They differ in the underlying computational processes they use, the data they are trained on, and the type of information they produce. As a result, characteristics about one technology do not necessarily apply to another.

For example, the accuracy rates of facial recognition are different than those for facial analysis, and the privacy implications of each differ too. Conflating these technologies under one broad umbrella term and seeking to understand the validity, accuracy, and error rates of the whole can create misperceptions about the risks associated with each. Therefore, policymakers should evaluate separately systems that use biometric information for recognition from those that use biometric information for inference.

Looking at systems that use biometric information for recognition first, our 2020 report *The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist* found that the best facial recognition algorithms in the world are highly accurate and have vanishingly small differences in their rates of false-positive or false-negative readings across demographic groups.[2] Taking a close look at data from the National Institute of Standards and Technology (NIST) on the accuracy of facial recognition algorithms across different demographic groups, the report reveals that most accurate identification algorithms have "undetectable" differences between demographic groups; the most accurate verification algorithms have low false positives and false negatives across

[2] Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist,"(Information Technology and Innovation Foundation, January 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

most demographic groups; and algorithms can have different error rates for different demographics but still be highly accurate.[3]

Looking at the validity and accuracy of tools that use biometric information for inference is more complicated because validity and accuracy vary significantly by application and implementation. Some tools may estimate an individual's age, gender, emotional state, or genetic conditions. The accuracy of age estimation algorithms has improved significantly over recent years with leading digital ID company Yoti's technology having a margin of error of 2.79 years across its total 45-year age range.[4] In 2020, an independent nonprofit called Age Check Certification Scheme found Yoti's system to be 98.89 percent reliable when identifying if people are under 25-years-old.[5] On the other hand, the validity of emotion recognition technology has little scientific support.[6] Even within an application area (such as age recognition), the accuracy and validity of different biometric information tools, as well as the methods used, may vary. For example, some systems estimate an individual's age using pictures of their face, while other use pictures of a person's hands or gait or the sound of a person's voice.

Therefore, policymakers should not draw broad conclusions about biometric technologies based on a single application or even a sample of the technology, but rather judge the potential of the technology based on the best-in-class implementations. This is important, because assessing a technology based on the average-in-class will lead to a very different result than assessing only best-in-class. Moreover, the level of accuracy necessary for various commercial and government uses cases will depend on the context in which it is deployed and the controls in place to mitigate potential errors.

(2) EXHIBITED AND POTENTIAL BENEFITS OF A PARTICULAR BIOMETRIC TECHNOLOGY.

Public understanding and appreciation of the benefits of systems that use biometric information for recognition continue to grow because this technology has multiple applications and is increasingly commonplace. For instance, authorities use facial recognition to help find and rescue human

[3] Ibid.
[4] Matt Burgess, "This AI Predicts How Old Children Are. Can It Keep Them Safe?" *Wired*, October 26, 2021, https://www.wired.co.uk/article/age-estimation-ai-yoti.
[5] Ibid.
[6] Lisa Feldman Barrett, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," *Association for Psychological Science,* Vol 20, Issue 1, 2019 https://doi.org/10.1177/1529100619832930.

trafficking victims, and identify individuals committing crimes ranging from shoplifting and check forgery to armed robbery and murder.[7] Businesses also use facial recognition to improve security and facilitate convenience for consumers. Several credit card companies such as Visa and Mastercard have launched services that allow customers to use selfies to verify the authenticity of online purchases and many airports use the technology to reduce the time it takes passengers to board their flights. Businesses can also use the technology to improve the accessibility of online services and help visually impaired individuals better understand their surroundings. Apps like Uber and Lyft use face recognition to verify identity documents for drivers and prevent unauthorized drivers from using an approved account, while these apps also use facial analysis to confirm they are wearing a face covering.

The benefits of systems that use biometric information for inference are less known because the technology itself is still nascent and its applications are less interwoven into society. However, two application areas are gaining increasing traction and offer significant value to consumers and businesses: age estimation and augmented and virtual reality. Given the many potential benefits of biometric technology, the primary purpose of policy should be to guide its development and deployment to ensure appropriate use, rather than impose strict limits or bans on the technology.

Age Estimation

Traditional age verification mechanisms are often trivial to circumvent. For example, a website or mobile app may use a form that asks users to submit their age or year of birth that younger children can easily bypass by giving false information. There have been multiple reports that document the routine nature by which children circumvent current age verification technologies to use websites and online services like Facebook and Instagram which are officially only available for individuals age 13 and over.[8] Systems that use biometric information to estimate age can be a valuable solution to better protect children from accessing potentially harmful content and services without strictly limiting them from having access to many types of online services.

This technology offers unique benefits in this context because most children in the United States do not have government-issued forms of ID, which means systems that use recognition cannot verify

[7] "ITIF Technology Explainer: What Is Facial Recognition?" ITIF website, April 8, 2020, https://itif.org/publications/2020/04/08/itif-technology-explainer-what-facial-recognition.
[8] Daniel Castro and Alan McQuinn, "Comments to the Federal Trade Commission on Implementation of the Children's Online Privacy Protection Act," (Information Technology and Innovation Foundation, October 2019), https://www2.itif.org/2019-ftc-coppa-comments.pdf.

their age against a reference ID. Given recent legislation such as the United Kingdom's Age Appropriate Design Code that requires social media companies, video streaming sites, and gaming platforms to verify the age of users that visit their websites, many companies are increasingly turning toward age estimation solutions. Members of the U.S. Senate and Congress have called on large U.S. technology and gaming companies to voluntarily adopt the UK's rules for American children as well.[9]

Augmented and Virtual Reality

Augmented and virtual reality (AR/VR)—immersive technologies that enable users to experience digitally rendered content in both physical and virtual space—can collect extensive biometric data. By collecting detailed biometric information from individuals, AR/VR systems can get a more complete picture of an individual and create immersive experiences for them. For example, hand-tracking technologies estimates important information such as the size, shape, and positioning of users' hands and fingers.[10] AR/VR devices may also use eye tracking sensors to determine where users are looking (to improve how they interact with the technology, to enhance graphics rendering, and to track user behavior) and to uniquely identify users.[11]

One of the benefits of AR/VR devices is that they can make several important contributions to equity and inclusion by reducing opportunity gaps, especially among members of underserved and disadvantaged communities.[12] First, AR/VR devices use a diverse set of sensors and inputs as well as digital outputs, which means they present potential workarounds for audiovisual barriers that users with vision or auditory impairments might encounter—without minimizing the user experience. For instance, immersive 3D audio that mimics 360-degree sound in physical space can provide a sense of spatial awareness for users with visual impairments: a musician performing in front of them, a friend

[9] Letter from Congressman Edward J. Markey, Congresswoman Kathy Castor, and Congresswoman Lori Trahan of the United States, June 30, 3031, https://www.markey.senate.gov/imo/media/doc/letter_-_age_appropriate_design_code.pdf.
[10] Shangchen Han et al., "Using Deep Neural Networks for Accurate Hand-Tracking on Oculus Quest," Facebook AI, September 25, 2019, https://ai.facebook.com/blog/hand-tracking-deep-neural-networks.
[11] Ellysse Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality," (Information Technology and Innovation Foundation, March 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality.
[12] Ellysse Dick, "Current and Potential Uses of AR/VR for Equity and Inclusion," (Information Technology and Innovation Foundation, June 2021), https://itif.org/publications/2021/06/01/current-and-potential-uses-arvr-equity-and-inclusion.

calling out from behind, an object appearing on their left, etc.[13] Second, because immersive experiences place the user in partially or fully virtual environments, they can manipulate and tailor these to their individual needs, making these technologies more inclusive for a wider set of users. For example, Microsoft's social VR platform AltspaceVR includes public channels such as "LGBTQ+ and Friends Meetup," "Autism VR," "ADHD and Neurodiversity," and "Indigenous Peoples in XR."[14] Finally, immersive experiences offer more engaging and realistic interpersonal and sensory experiences than their two-dimensional counterparts, creating new opportunities for digital communication and allowing virtual experiences to mirror the physical world. For example, AARP Innovation Labs developed a "virtual living room" program called Alcove aimed at families or other intergenerational groups, and offers virtual spaces for users to communicate, play games, and engage in a number of immersive experiences and activities together.[15] It is easy to imagine similar applications and activities being used to engage other communities who face distance or mobility barriers. Unnecessarily restricting the collection and use of biometric data could negatively affect the deployment of AR/VR technologies.

(3) EXHIBITED AND POTENTIAL HARMS OF A PARTICULAR BIOMETRIC TECHNOLOGY.

Systems that collect and use biometric information can reveal or enable one to infer biographical and demographic information, even if a user has not elected to provide these details. For instance, motion and eye tracking can capture a user's subconscious reactions, such as pupil dilation, which can in turn reveal inferred information about their interests and preferences—from favorite foods to sexual orientation.[16]

Bias and discrimination can occur when inferred personal information from biometrics such as details on race, gender, sexual orientation are used to deny a person access to something, such as employment, housing, loans, or basic goods and services. Consider an employer that uses an AI system with eye-tracking technologies to monitor how safely its employees drive when out on

[13] Mona Lalwani, "Surrounded by Sound: How 3D Audio Hacks Your Brain," The Verge, February 12, 2015, https://www.theverge.com/2015/2/12/8021733/3d-audio-3dio-binaural-immersive-vr-sound-times-square-new-york.
[14] From a review of the top 50 listings of "popular" channels on AltSpace VR as of April 16, 2021. See "Channels," AltspaceVR, https://account.altvr.com/channels/popular.
[15] "About Alcove," accessed January 11, 2022, https://alcovevr.com.
[16] Avi Bar-Zeev, "The Eyes Are the Prize: Eye-Tracking Technology is Advertising's Holy Grail," *VICE*, May 28, 2019, https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-trackingtechnology-is-advertisings-holy-grail.

delivery, as Amazon does.[17] The tool collects information about where a user is looking, changes in their pupil size, and whether their eyes are open or closed. If it identifies dangerous behavior such as distracted driving, it suggests actions to the driver, such as taking a break. However, many studies have found that people with autism react differently to stimuli when driving.[18] The employer may be able to infer from the eye-tracking AI software which drivers have autism, even though employees may want to keep this information private, exacerbating the risk of bias and discrimination. Similar risks could arise in other critical areas such as education, healthcare, and government services. But at the same time, the overall benefit to such a technology should not be underestimated —in this case, safer driving of delivery vehicles.

Although any system that collects biometric data raises autonomy and discrimination risks, AR/VR poses new potential risks because of the scope of information AR/VR devices gather and the potential for additional information to be inferred. Researchers at the Stanford Virtual Human Interaction Lab have estimated users generate "just under 2 million unique recordings of body language" in one 20-minute session in VR.[19] Immersive experiences require users to share—and allow devices to gather, track, and process—much more information than they would with other digital media platforms that simply transmit audiovisual information. The subtle, subconscious movements sensors can detect, which is called "nonverbal data," is virtually impossible for users to consciously control.[20]

(3) GOVERNANCE PROGRAMS, PRACTICES OR PROCEDURES APPLICABLE TO THE CONTEXT, SCOPE, AND DATA USE OF A SPECIFIC USE CASE.

To accelerate improvements in existing systems that use biometric information for recognition and inference, the government should increase and expand independent public testing of these systems. Despite the growing use and policy importance of age estimation, NIST has not performed a large-scale empirical evaluation of facial age estimation algorithms since 2014. And its evaluations of

[17] James Vincent, "Amazon delivery drivers have to consent to AI surveillance in their vans or lose their jobs," *Verge*, March 24, 2021, https://www.theverge.com/2021/3/24/22347945/amazon-deliverydrivers-ai-surveillance-cameras-vans-consent-form.
[18] Joshua Wade et al., "A Pilot Study Assessing Performance and Visual Attention of Teenagers with ASD in a Novel Adaptive Driving Simulator" (NCBI, November 1, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5693648/pdf/nihms896479.pdf.
[19] Jeremy Bailenson, "Protecting Nonverbal Data Tracked in Virtual Reality," JAMA Pediatrics, August 6, 2018, https://vhil.stanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf.
[20] Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

commercial facial recognition systems do not require cloud providers to participate.[21] Expanding and increasing testing would be useful as many commercial systems are using these services. These tests should include race, gender, and age diversity metrics as part of the testing protocol.

There should also be performance standards for any systems that use biometric information procured by the federal government, including for accuracy and error rates by age, race, and gender. These standards will ensure federal agencies do not waste tax dollars on ineffective systems or ones with significant performance disparities. NIST and the General Services Administration (GSA) would be best placed to develop such standards. Since the federal government and the private sector use the same technology, setting a performance standard for the federal government can promote better accuracy rates across all sectors of the economy, and greatly reduce the risk of systems with unacceptable accuracy rates.

To address the unique risks presented by the extent of biometric data collected and used in AR/VR, government agencies and industry should develop voluntary guidelines for AR/VR developers to secure users' privacy through transparency and disclosure practices. This could parallel the digital signage industry, which in 2011 adopted a set of voluntary privacy and transparency guidelines for the use of facial recognition and facial analysis.[22] This standard offers detailed guidance for how to provide clear and meaningful notice to consumers and under which conditions consumers should be able to opt in or opt out of data collection. A voluntary framework for AR/VR should include transparency and disclosure standards and mechanisms for immersive experiences, including clear disclosure of how sensitive biometric data is collected and used as ITIF explains in its 2021 report, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*.[23]

Finally, the government should fund the creation of additional and more diverse training and evaluation datasets for recognition and inference. For instance, the MORPH dataset is a widely used database for gender and race classification, as well as age estimation. By funding the creation of

[21]Hearings on "Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy," Before the House Committee on Oversight and Reform, January 15, 2020, Statement of Daniel Castro, Vice President of ITIF, https://www2.itif.org/2020-commercial-use-facial-recognition.pdf.
[22] "Digital Signage Privacy Standards," Digital Signage Federation, February 2011, https://www.digitalsignagefederation.org/wp-content/uploads/2017/02/DSF-Digital-Signage-Privacy-Standards-02-2011-3.pdf.
[23] Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality."

additional and more diverse datasets, the government can spur developers to further reduce any differences in accuracy across different demographics and reduce concerns about bias.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Information Technology Industry Council

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

ITI Promoting Innovation Worldwide

January 14, 2022

Via email to: biometricRFI@ostp.gov

RE: ITI Response to Office of Science and Technology Policy (NIST) Request for Information on AI-Enabled Biometric Technologies [Docket Number 2021-21975]

The Information Technology Industry Council (ITI) appreciates the opportunity to provide feedback in response to the Office of Science and Technology Policy's (OSTP) *request for information on AI-enabled biometric technologies.* One of the specific uses of Artificial Intelligence (AI) that has garnered attention not only in the U.S. but around the world is AI-enabled biometric technologies, with a particular emphasis on facial recognition technology. However, ITI recognizes the need to broaden the discussion around AI-enabled technologies beyond facial recognition, including, but not limited to, voice analysis, key stroke analysis, and various health indicators. As such, OSTP's RFI is timely and important.

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, and other internet and technology-enabled companies that rely on ICT to evolve their businesses. AI is a priority technology area for many of our members, who develop and use AI systems to improve technology, facilitate business, and solve problems big and small.

ITI is actively engaged on AI policy around the world and issued a set of *Global AI Policy Recommendations* in 2021, aimed at helping governments facilitate an environment that supports the development of AI while simultaneously recognizing there are challenges that need to be addressed as the uptake of AI grows around the world.[1] We have actively engaged with the USG on its AI-related workstreams, most recently providing feedback on NIST's efforts to develop an *AI Risk Management Framework* and the *National AI Research Resource.*[2]

ITI and our members share the firm belief that building trust in the era of digital transformation is essential and agree that there are important questions that need to be addressed regarding the responsible development and use of AI technology. As this

[1] Our complete *Global AI Policy Recommendations* are available here: https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

[2] See ITI comments responding to RFI on Developing an AI Risk Management Framework here: https://www.itic.org/documents/artificial-intelligence/NISTRFIonAIRMFITICommentsFINAL.pdf; see ITI comments on National AI Research Resource here: https://www.itic.org/documents/artificial-intelligence/2021-9-30_ITICommentsNAIRRRFIFINAL(1).pdf

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
[redacted]

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
[redacted]

info@itic.org
www.itic.org
@iti_techtweets

technology evolves, we take seriously our responsibility as enablers of a world with AI, including seeking solutions to address potential negative externalities. To be sure, the tech industry is aware of and is already taking steps to understand, identify and mitigate the potential for negative outcomes that may be associated with the use of AI and AI-enabled systems. Companies are developing technical toolkits to help increase understanding of how AI models perform across different demographic groups and are leveraging ethics frameworks to ensure they are developing AI in a responsible manner. We therefore welcome the opportunity to provide comments on AI-enabled biometrics technologies, with a specific focus on existing governance frameworks and best practices that may be useful to consider moving forward.

General Thoughts

In considering any future policy action, OSTP should focus on specific, high-risk uses of AI-enabled biometrics technologies, rather than on the technologies themselves. It is important to highlight at the outset that AI-enabled biometric technologies only represent one use-case of AI technology. We emphasize this because although there are a discrete set of risks that may be associated with particular types of AI-enabled biometric technologies, such risks are not uniform across all AI technologies, nor are they uniform across biometric technologies as a whole. As with AI more broadly, context and use are critical. In considering any future policy action related to biometric technologies, the USG needs to be careful to draw clear distinctions between different uses of biometric technologies and to focus its policies on specific uses rather than on the technology writ large. For the purposes of any future policymaking activity, we also encourage the USG to clearly define what it considers to be biometric technologies. At present, there seems to be conflation between private sector and public sector uses, and between uses for mass identification or surveillance in public settings and uses in private settings. The RFI – and more broadly, other USG messaging on this subject -- does not distinguish between these uses, though their risk profiles and implications -- especially in the context of privacy, human rights, and access to services and benefits -- can be vastly different. We encourage OSTP, and the USG more broadly, to keep this need for a use-based focus in mind if and when devising policy, which should be carefully tailored to address specific, problematic use cases and mitigate the associated risks, as opposed to horizontally applying one risk profile and one set of policy measures across all biometric technologies.

In seeking to use the information gathered via this RFI to develop a Bill of Rights for an Automated Society (hereafter "Bill of Rights"), we encourage OSTP to take a risk-based approach that considers use-cases or applications of the technology. We recognize that the use of AI-enabled biometric technologies can pose a serious risk to human rights when used for specific purposes in both the public and private sectors. In our view, the "Bill of Rights" terminology seems to imply a set of protections for consumers from government use of AI, but OSTP's focus does not seem limited to government uses. In line with the points we made above, risk should be assessed based on use case and context, instead of evaluating an entire set of technologies collectively, which can be used for many different

purposes. OSTP's event series on developing a Bill of Rights, which focused on the use of AI in criminal justice, social welfare, healthcare, etc., was a good first step in discussing the potential implications of using AI in areas where there may be an outsized risk to fundamental human rights. Yet, even within these sectors, there may be applications where the use of AI does not present an outsized risk – or even, in some instances, any risk to individual rights at all – and so it is important that in developing any future policy intended to address concerns stemming from the use of AI in these sectors, USG takes a risk-based approach, in which it seeks to identify specific civic or consumer problems that require remedies.

There are a wide variety of governance frameworks and best practices that focus on privacy, security, human rights, and responsible AI that create safeguards when used in the development and deployment of biometric technologies. We highlight some of these frameworks in response to question 6 below but believe that many of these frameworks and best practices can be leveraged to address concerns related to the development and deployment of biometric technologies. OSTP and other USG stakeholders considering policies to address biometric technologies should take care to disentangle and deconflict such policy measures from existing policy frameworks, focusing any biometric-specific policies on gaps that aren't addressed elsewhere.

OSTP should seek to align its efforts to develop a Bill of Rights with other ongoing federal agency activities. At the moment, it remains somewhat unclear to us what the Bill of Rights will entail and whether it will result in discrete policy action. For example, the National Institute of Standards and Technology (NIST) is currently developing an AI Risk Management Framework, which will ideally address several areas of relevance to a Bill of Rights. We also think it useful for OSTP to refer to the principles contained in the Office of Management and Budget's *Guidance for the Regulation of AI Applications*. The OMB memo provides a useful backdrop to frame broader federal AI efforts, including those being undertaken by OSTP. In particular, principles related to risk assessment and management, flexible approaches to AI risk management, and public trust in AI are all relevant to this RFI as well as the Bill of Rights efforts more broadly. We also encourage OSTP to align its efforts with the work being undertaken by NTIA on Privacy, Equity, and Civil Rights, which we believe will tie into the development of a Bill of Rights. Finally, OSTP should also reference and integrate other frameworks that are currently in use by federal agencies, including those developed by DOD, ODNI, and HHS so as to align guidance to the extent possible.[3]

[3] Ethical Principles for Artificial Intelligence, available here: https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/; Principles of Artificial Intelligence Ethics for the Intelligence Community, available here: https://www.dni.gov/files/ODNI/documents/Principles_of_AI_Ethics_for_the_Intelligence_Community.pdf; Trustworthy AI Playbook, available here: hhs.gov/sites/default/files/hhs-trustworthy-ai-playbook.pdf

In developing any future policy response on AI-enabled biometric technologies and the Bill of Rights more broadly, we strongly encourage continued stakeholder engagement, particularly with the developers, designers and deployers of AI technology. We appreciate that OSTP has sought to engage with potentially impacted communities early in the development of the Bill of Rights process as evidenced by the recently completed event series and listening sessions, as well as this RFI. While civil society and human rights groups were well-represented on the panels during those sessions, and while we appreciate the opportunity to provide written input on AI-enabled biometric technologies, we strongly encourage additional conversation with those stakeholders who are developing, designing, and deploying AI systems. Such conversations will provide a robust, well-rounded understanding of the landscape and allow for exchange between all stakeholders in the AI ecosystem.

Specific Responses

Before providing specific responses to several of the prompts under question 6, we think it prudent to raise one foundational issue, which is that in the United States, there is not currently a set of criteria or a methodology that can help stakeholders determine whether a particular application of AI technology is high-risk. We view high-risk applications as applications in which a negative outcome could have a significant impact on people, especially as it pertains to human rights, safety, discrimination, or freedom. A set of criteria developed in conjunction with stakeholders would be useful in further devising policy approaches or risk mitigation techniques for high-risk applications. In light of this, we have encouraged NIST, in its work to develop an AI RMF, to develop a methodology or categorization that can help stakeholders determine the risk level of a specific AI use case and then take steps based on that identification to mitigate that risk. This is something that we have advocated for more broadly, encouraging stakeholders to work together to characterize "high-risk" applications of AI, including by identifying the appropriate roles for AI developers and users in making risk determinations.

The balance of our response is focused on question 6, which asks about existing governance programs, practices, and procedures that may be applicable to the use of AI-enabled biometric technologies. We do not focus on a particular use case, but instead offer general thoughts on existing practices that may be widely applicable.

6) Governance programs, practices, or procedures applicable to the context, scope, and data of a specific use case, including information related to:

As a general matter, the USG should encourage an approach to the development of AI systems that promotes fairness and non-discrimination. Such an approach is relevant to AI systems across the board, not just for AI-enabled biometric technologies. In taking an ethical design approach, one perspective worth considering is espoused in the Guidelines set forth by the European High-Level Experts Group, which propose seven foundational principles that characterize a trustworthy AI system, including human agency and oversight, transparency, privacy and data governance, robustness and safety, diversity,

non-discrimination and fairness, societal and economic well-being, and accountability.[4] Although these principles are applicable to AI systems generally, some may be specifically worth focusing on in the context of a high-risk application of AI-enabled biometric technologies.

When considering best practices to address many of the below areas, we encourage the USG in the first instance to look to voluntary, consensus-based international standards and best practices. For example, ISO/IEC JTC 1 SC 42 is undertaking work on developing standards for aspects of AI, including an AI systems process management standard, which demonstrates that a company is undertaking practices that address risks related to bias, fairness, inclusiveness, safety, security, privacy, accountability, and explainability (the "Artificial Intelligence Management System (AIMS) standard").[5]

There are also a variety of frameworks that have been developed which may be useful in managing risks associated with the use of biometric technologies, including the NIST Privacy Framework and NIST Cybersecurity Framework, along with other AI-specific frameworks. Other domestic frameworks include the DOD's Ethics Principles for AI[6], the Intelligence Community's Principles of AI Ethics[7] and the OMB's AI Regulatory Guidance[8].

Additionally, countries and organizations around the world have developed frameworks to help guide the development and use of AI. We highlight the OECD AI observatory which serves as a repository that references various national and global efforts on AI- specific frameworks.[9] We also recommend that OSTP consider the following frameworks as it develops a Bill of Rights for an Automated Society or other policy measures: JTC 1 SC 42 Standards Work[10], IEEE Position Statement on AI[11], IEEE 7010-2020: Assessing the Impact of AI on Human Well-Being[12], the European Commission High Level Experts Group Ethics Guidelines for Trustworthy AI & AI Assessment List for Trustworthy AI[13], the Considerati

[4] See HLEG Ethics Guidelines here: https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html
[5] See progress of the standard here: https://www.iso.org/standard/81230.html
[6] Ethical Principles for Artificial Intelligence, available here: https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
[7] Principles of Artificial Intelligence Ethics for the Intelligence Community, available here: https://www.dni.gov/files/ODNI/documents/Principles_of_AI_Ethics_for_the_Intelligence_Community.pdf
[8] Guidance for the Regulation of Artificial Intelligence Applications, available here: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf
[9] See OECD AI Observatory here: https://oecd.ai/en/.
[10] [Link to JTC 1 SC 42 Standards Work]
[11] IEEE Position Statement on Artificial Intelligence, available here: https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE18029.pdf
[12] IEEE 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being, available here: https://standards.ieee.org/standard/7010-2020.html
[13] Ethical Guidelines for Trustworthy AI, available here: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai; Assessment List for Trustworthy Artificial Intelligence, available here: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Artificial Intelligence Impact Assessment (AIIA)[14], Australia's AI Ethics Framework[15] & Actions Plan[16] and Singapore's Model AI Governance Framework.[17] We expand upon these frameworks in our comments responding to NIST's AI Risk Management Framework and would encourage OSTP to review those comments for a fuller understanding of each framework.[18]

However, if there is concern that existing frameworks and best practices are not sufficient to mitigate the risks identified for specific uses of AI-enabled biometric technologies applications, we encourage the USG to undertake an extensive analysis of the current landscape, mapping different standards and frameworks to existing risks so as to better understand where there may be gaps that need to be filled.

- *Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, assessments, strategies, etc. to mitigate potential harm/risk of biometric technologies*
- *Best practices or insights re: design and execution of pilots or trials to inform further policy developments*

In the response we provided to NIST on the AI RMF, we recommended that the development of the AI RMF be grounded in experience and evidence gathered via policy prototyping.[19] We believe such an approach could be useful to address concerns related to biometric technologies as well, where a variety of stakeholders can come together to co-create governance frameworks, including regulation and voluntary standards. Developing and testing governance frameworks in a collaborative fashion allows policymakers to see how such frameworks can integrate with other co-regulatory tools such as corporate ethical frameworks, voluntary standards, conformance programs such as those for testing and certification, ethical codes of conduct, and best practices. This method has been successfully used in Europe to test an AI Risk Assessment framework, leading to several concrete recommendations for improving self-assessments of AI.[20]

---

[14] The Artificial Intelligence Impact Assessment, available here: https://www.considerati.com/static/default/files/documents/pdf/Artificial%20Intelligence%20Impact%20Assessment%20-%20English[2].pdf

[15] Australia's Artificial Intelligence Ethics Framework, available here: https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework

[16] Australia's AI Action Plan, available here: https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf

[17] Singapore Model AI Governance Framework, available here: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

[18] ITI Response to AI Risk Management Framework, available here: https://www.nist.gov/system/files/documents/2021/09/14/ai-rmf-rfi-0058.pdf

[19] Ibid.

[20] See OpenLoop *AI Impact Assessment: A Policy Prototyping Experiment*, available here: https://openloop.org/wp-content/uploads/2021/01/AI_Impact_Assessment_A_Policy_Prototyping_Experiment.pdf

- *Practices regarding data collection (including disclosure and consent), management (including data security and sharing), storage (including timeframes for holding data), review, and monitoring*

In general, companies may use techniques such as anonymization, pseudonymization, deidentification and other privacy enhancing technologies (PETs) as well as Privacy Preserving Machine Learning (PPML), which ensures that data can be used to train algorithms and perform AI tasks without breaching privacy. Industry is also exploring the use of "federated learning," which aggregates data in ways so that the individual data points are kept private, but AI can be performed on the aggregate with minimal loss of accuracy.

Beyond that, because AI operates in an existing policy and regulatory framework, personal data and related privacy concerns must be taken into account. Indeed, there are laws worldwide that govern the ways in which biometric data, in particular, can be stored and processed. For example, the GDPR prohibits the processing of biometric data for the purpose of uniquely identifying natural persons (with some exceptions). In the absence of a comprehensive privacy law in the United States, states like California, Washington, and Virginia have also passed privacy protection laws, which implicate biometric data and govern the ways in which this sensitive data can be used. To enable trust and interoperability and to facilitate research to develop stronger privacy and security guarantees, we continue to advocate for the development of a national privacy law in the United States, consistent with *ITI's Framework to Advance Interoperable Rules on Privacy*.[21] Indeed, such a law may help to provide a concrete mechanism to address some of the underlying concerns signaled by the prompts in this RFI, including around consent, use, and redress.

- *Performance auditing and post-deployment impact assessments*

In certain high-risk settings, performance auditing and post-deployment impact assessments may be appropriate. However, we do not recommend requiring auditing and post-deployment impact assessments for *all* AI-enabled biometric technologies, as this would be out of step with a risk-based approach. Indeed, as we have referenced above on several occasions, not all uses of these technologies inherently present a risk to human rights. At this point, however, we believe there are more questions than answers around such a mechanism, including which standards an impact assessment would test to, how impacts would be judged, whether such an audit would be voluntary, who would undertake the audit, among others. We therefore encourage the USG to further explore these concepts, and questions, in conjunction with relevant stakeholders, including developers and deployers of AI technology. Doing so will help ensure that any policy that is developed strikes an appropriate balance between protecting privacy and civil liberties, while also allowing for innovation.

[21] ITI Framework to Advance Interoperable Rules on Privacy, available here: https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules%28FAIR%29onPrivacyFinal_NoWatermark.pdf

- *Practices re: use of biometric technologies in conjunction with surveillance technologies*

It is worth considering the risk-based approach taken in the EU AI Act, which classifies biometric identification and categorization of natural persons as high-risk, and as a result imposes additional obligations on developers seeking to place such systems on the market.[22] However, the way in which biometric technologies is defined matters, as not every use of biometric technologies is inherently high-risk. We believe that the definition should be understood as clearly targeting biometrics-based technologies that (i) involve the processing of biometrics of an indiscriminate number of individuals and require comparing an individual's biometrics to the biometrics of many other individuals stored in a database to identify said individual (i.e., one-to-many matching or identification) as opposed to one-to-one matching or verification which involves comparing two biometric templates usually assumed to belong to the same individual and in which no link with the actual identity is established; and/or (ii) cover situations where biometrics are used to identify individuals without their knowledge, rather than a situation where a well-informed individual deliberately chooses to verify their identity based on their biometrics in order to transact or otherwise interact with a service provider or a government service. We note, though, that in leveraging this definition, it is important to evaluate whether and to what extent a risk is posed by this sort of biometric technology using other criteria as well, including the impact of the decision the AI-enabled biometric technology application might have on an individual or group of people.

The Act also bans the use of real-time biometric identification by law enforcement in publicly accessible spaces, though there are specific exceptions to the ban. As we noted in our response to the consultation on the AI Act, we recognize there are serious risks to fundamental rights that can be posed by government use of AI for surveillance purposes. At the same time, it is also important to recognize that there are public safety and national security benefits that may come from allowing responsible deployment with strict, meaningful safeguards.

Managing risks in these operations is possible through clearly defined processes and controls such as human review, sufficient confidence scoring (for instance by assigning a percentage of accuracy to any output), judiciary supervision, clear use policies, reasonable boundaries around data retention, and transparency measures. Additional transparency requirements on the user of the AI system (for instance related to when, where and how the AI system is used, how the data is processed and stored and for how long) may be a solution to enhance safeguards for the safe and responsible deployment of such systems.

[22] See Proposed Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) And Amending Certain Union Legislative Acts here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

- *Practices for public transparency regarding use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate*

Transparency is important in facilitating trust in AI technologies, particularly those that may implicate fundamental human rights. In our *Global AI Policy Recommendations,* we explore the idea of explainability as one way to enable transparency. Our recommendation regarding explainability, however, speaks more broadly to transparency of AI systems, as opposed to public transparency. That being said, meaningfully explainable AI systems can play an important role in providing an opportunity for impacted entities to understand how and why a system may have arrived at a certain outcome. While explainability will not be useful in every instance, we believe that for high-risk use cases, especially, explainability can act as one safeguard. However, explainability may not always be possible. We appreciate that the USG, through NIST, has already started to undertake work to consider appropriate practices around explainability with the publication of its *Four Principles of Explainable AI*.

In the context of privacy, transparency -- whereby the providers of an AI solution are able to declare how data is being used – also matters. Gaining increased visibility into data sets is important in facilitating trust in a system, such as through a better understanding of where the data came from, how it was cleaned, and what features were used to train an algorithm, etc. However, while increasing visibility can provide additional insight into why a model may have behaved in a certain way or resulted in a certain outcome, we need to approach consideration of transparency in a measured and targeted fashion to avoid unintended consequences.

5) Exhibited and potential benefits of a particular biometric technology

Although there has been a significantly negative focus on facial recognition technology, it is worth noting that such technology – when using the best algorithms – is a powerful tool to help users verify their identity and to prevent fraud. With the right privacy and transparency practices, facial recognition can be valuable when the technology operates on a personal device. This method of on-device facial recognition is deployed in systems used to unlock device such as smartphones, as well as for biometric-based authentication more generally. Since 2000, NIST's Face Recognition Vendor Testing Program (FRVT) has assessed capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. In a 2019 study, NIST found that the most accurate *identification* algorithms have "undetectable" differences between demographic groups.[23] This is encouraging as industry continues to innovate and improve upon this technology.

Additionally, many of our everyday tasks require verifying our identity in the digital world (for example to fill in our tax return online or to sign into our e-banking app). At the same time, malicious actors have been developing new ways to commit fraud and accomplish

[23] See NISTIR 8271: Face Recognition Vendor Test Part 2: Identification, available here: https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49

nefarious purposes. Combinations of data attributes that resemble a "real person" can be purchased or stolen and used to create a false digital identity or a nefarious actor may create multiple identities with different information (name, date of birth, address, etc.). Using biometric-based technologies can prove to be very useful to detect such bad actors, as stealing or altering a biometric identifier is much more difficult.

In the payment authentication space, the financial industry is gradually moving away from knowledge-based authentication tools given their limited security (passwords or PINs can be stolen), and is investigating the possibility of leveraging authentication solutions that rely on biometrics. Biometrics can serve as the basis for a reliable authentication method and have several advantages over knowledge-based authentication, including reduced risk of social engineering, and reduced transaction failure and abandonment rates (and consequently reduced harm to consumers).

Other beneficial use cases of biometric technologies include voice recognition in personal and home devices that fosters convenience, allows consumers to conduct their daily lives more seamlessly, and makes life easier for people with certain disabilities. In the new world of hybrid work, facial recognition also makes working from home easier in online video conferencing systems, where it helps to facilitate background blur and background replacement.

***

Once again, we appreciate the opportunity to provide input on OSTP's RFI on AI-enabled biometric technologies. To the extent this information is used to inform the development of a Bill of Rights for an Automated Society, we encourage OSTP to focus on high-risk uses of AI-enabled biometric technologies, leverage existing standards and frameworks, align its efforts with other ongoing federal agency activities, and continue robust, diverse stakeholder engagement. We agree that facilitating trust in an era of digital transformation is essential and that important questions related to AI need to be addressed to help foster that trust. At the same time, it is important to keep in mind that there are beneficial uses of biometric technologies and encourage OSTP to consider how to support continued innovation should it seek to devise policy in this arena. Please view ITI as a resource on this matter; we are always happy to provide our perspectives.

Sincerely,

[redacted]

John S. Miller
Senior Vice President of Policy
and General Counsel

[redacted]

Courtney Lang
Senior Director of Policy

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Innocence Project

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

INNOCENCE PROJECT PUBLIC COMMENT ON WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY REQUEST FOR INFORMATION PUBLIC AND PRIVATE SECTOR BIOMETRIC TECHNOLOGIES JANUARY 14, 2022

The Innocence Project is pleased to respond to the White House Office of Science and Technology Policy's (OSTP) *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies*. Our submission focuses on the racially disproportionate harms that artificial intelligence (AI) enabled biometric technologies may generate in their application to the criminal legal system and their capacity to increase risks for wrongful convictions. Police surveillance technologies based on biometric data for use in recognition or for inferences of cognitive and/or emotional state are not currently required to meet scientific or social impact standards. Consequently, even if a biometric technology was proven to be highly accurate, the social implications of its use and any disparities it exacerbates cannot be fully understood without evaluating its application in the context of the American criminal legal system.

For nearly 30 years, the Innocence Project[1] has worked to exonerate the innocent and to prevent wrongful convictions through systemic reform. In cases where we have proven innocence, misapplied forensic science contributed to 52% of the wrongful convictions.[2] The vast majority of our exonerations were achieved by the power and strength of forensic DNA evidence. However, we have watched with concern as—through technologies like Rapid DNA and familial searching—DNA applications have expanded beyond truth seeking instruments into tools of surveillance that target innocent people, exacerbate racial disparities, and promote the unsupported notion that criminality is genetic.[3] Based on these decades of experience, the Innocence Project takes the position that, in addition to meeting scientific metrics of validity and reliability, the research and development of criminal legal system applications must simultaneously assess social impact, considering ethical, legal, and social implications, and capacity for just and equitable implementation. Any framework for implementing AI enabled biometric information for

[1] The Innocence Project works to free the innocent, prevent wrongful convictions, and create fair, compassionate, and equitable systems of justice for everyone. Founded in 1992 by Barry C. Scheck and Peter J. Neufeld at the Benjamin N. Cardozo School of Law at Yeshiva University, the organization is now an independent nonprofit. Our work is guided by science and grounded in antiracism.

[2] Innocence Project, *Overturning Wrongful Convictions Involving Misapplied Forensics*, Innocence Project(2021), https://innocenceproject.org/overturning-wrongful-convictions-involving-flawed-forensics/ (last visited Feb 27, 2021).

[3] ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA (2015); Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. LAW REV. 59 (2010); NANCY GERTNER ET AL., *Report on S.2480, "An Act Permitting Familial Searching and Partial DNA Matches in Investigating Certain Unsolved Crimes" and Related Recommendations Pertaining to G.L. c.22E Governing the Massachusetts Statewide DNA Database* (2021).

[redacted] [redacted]

investigative purposes in the criminal legal process must simultaneously address both the scientific underpinnings of the technology as well as their social consequences.

The Innocence Project's primary concern with blanket intelligence systems and surveillance technologies is the impact these tools have on **suspect development**. Because the possibility for wrongful conviction begins once an innocent person becomes a person of interest, expansive surveillance increases wrongful conviction risk exposure.

Many extant and emerging biometric technologies have been criticized for their lack of evidence base and/or lack of accuracy. However, even if scientific advancements fine tune the accuracy of these tools, we must also consider their potential harm to society. With respect to biometric technologies and suspect development specifically, that potential harm includes profoundly racially disparate impacts. Indeed, emerging technologies must be considered in the context of how surveillance has historically been used in this country as a tool of social control, one which has had the effect of disproportionately criminalizing Black people in America by baking racial biases into the structure of our criminal legal systems.[4]

Biometric data based on speech, facial images, and genomic information have also largely been collected without consent from socially targeted groups and stored for law enforcement use.[5] These structural racial biases feed back into the administration of law enforcement and shape the crime data generated. These data are then fed into algorithmic technologies. Regardless of the quality of the algorithm or the AI tool, the use of systematically biased data may generate skewed or inaccurate outcomes that promote false narratives regarding the criminality of entire communities of color. Such false narratives create or reinforce cognitive biases that further impact how these communities are perceived (as "trouble zones") and then treated by law enforcement.[6]

The use of technology to process biometric data is erroneously promoted as "objective," able to bypass cognitive biases and the frailties of human learning. But biometric technologies cannot be separated from either the biases that inform their creation or from the policing systems that administer them. Their applications to society and the data these technologies collect will reflect

[4] *See* SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015)(provided examples of how lantern laws and branding were used as early forms of surveillance of Black and indigenous people and that racializing surveillance "signals those moments when enactments of surveillance reify boundaries, borders, and bodies along racial lines, and where the outcome is often discriminatory treatment of those who are negatively racialized by such surveillance.") ; *See* KHALIL G. MUHAMMAD, THE CONDEMNATION OF BLACKNESS: RACE, CRIME AND THE MAKING OF MODERN URBAN AMERICA (2010) ("New statistical and racial identities forged out of raw census data showed that African Americans, as 12 percent of the population, made up 30 percent of the nation's prison population. Although specially designed race- conscious laws, discriminatory punishments, and new forms of everyday racial surveillance had been institutionalized by the 1890s as a way to suppress black freedom, white social scientists presented the new crime data as objective, color- blind, and incontrovertible").

[5] George Joseph & Debbie Nathan, *Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints*, The Intercept, January 30, 2019, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/ (last visited Nov 30, 2020); Jan Ransom & Ashley Southall, *'Race-Biased Dragnet': DNA From 360 Black Men Was Collected to Solve Vetrano Murder, Defense Lawyers Say (Published 2019)*, The New York Times, March 31, 2019, https://www.nytimes.com/2019/03/31/nyregion/karina-vetrano-trial.html (last visited Dec 13, 2020); Richard Van Noorden, *The ethical questions that haunt facial-recognition research*, 587 Nature 354–358 (2020).

[6] Rashida Richardson, Jason M Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N. Y. UNIV. LAW REV. 42.

the disparities, flaws, and biases of those law enforcement practices.[7] Accordingly, big data-driven technology can promulgate a vicious cycle that amplifies rather than solves systemic racial biases.

Biometric technologies play an especially troubling role in criminal investigative applications to the extent they serve as "suspect development systems" which the government uses to "manage vague or often immeasurable social risks based on presumed or real social conditions" and "subjects targeted individuals or groups to greater suspicion, differential treatment, and more punitive and exclusionary outcomes."[8] The damage done by front-end technologies which expose communities of color to greater suspicion can be extraordinarily difficult to undo.[9] Once an innocent person becomes a person of interest through the use of blanket intelligence systems and surveillance technologies, tunnel vision routinely sets in and no amount of exculpatory evidence can derail an investigator's conviction of the innocent person's guilt. Exonerations demonstrate this dynamic: Pre-trial *exculpatory* DNA results had been explained away or dismissed in 28 of the first 325 DNA exonerations in the United States between 1989-2014.[10]

In order to narrow the entry point for innocent people into a criminal legal system,[11] it is the Innocence Project's position that investigative biometric technologies must meet the same standards of accuracy and reliability expected of court admissible evidence and must further demonstrate their capacity for just and equitable application prior to their implementation in the criminal legal system. To require anything less is tantamount to facilitating the experimentation of these technologies on society. This is a painful and intolerable risk. The narrative that policing strategies and due process will weed out innocent people prior to conviction has been disproven by thousands of wrongful convictions. That narrative also dismisses the seriousness and harm of collateral consequences of arrests. There is no dispute that Michael Oliver, Robert Williams, and Njeer Parks' wrongful arrests and pretrial detention were the byproduct of both a flawed facial recognition system as well as flawed policing.[12] But for the fact these men held tightly to their innocence and their unjust arrests were recognized, they could have been wrongfully convicted. At this time, we cannot know how many people were wrongfully arrested based on these technologies

[7] *Id.*

[8] Rashida Richardson & Amba Kak, *Suspect Development Systems: Databasing Marginality and Enforcing Discipline*, 55 UNIV. MICH. J. LAW REFORM (forthcoming), https://www.ssrn.com/abstract=3868392 (last visited Jul 8, 2021).

[9] Rebecca Brown, *3 Ways Lack of Police Accountability Contributes to Wrongful Convictions*, INNOCENCE PROJECT (2020), https://innocenceproject.org/lack-of-police-accountability-contributes-to-wrongful-conviction/ (last visited Aug 30, 2021).

[10] Emily West & Vanessa Meterko, *INNOCENCE PROJECT: DNA EXONERATIONS, 1989-2014: REVIEW OF DATA AND FINDINGS FROM THE FIRST 25 YEARS*, 79 ALBANY LAW REV. 717–795 (2016).

[11] Kent Roach, *Four models of the criminal process*, 89 J. CRIM. LAW CRIMINOL. CHIC. 671–716 (1999); Herbert L Packer, *Two Models of the Criminal Process*, 113 UNIV. PA. LAW REV. 68 (1964); NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, *The Trial Penalty: The Sixth Amendment Right to Trial on the Verge of Extinction and How to Save It* 331–368 (2019), https://online.ucpress.edu/fsr/article/31/4-5/331/109303/The-Trial-Penalty-The-Sixth-Amendment-Right-to (last visited Aug 11, 2021).

[12] Kashmir Hill, *Wrongfully Accused by an Algorithm*, The New York Times, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (last visited Jun 25, 2020); Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, Detroit Free Press, July 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ (last visited Oct 26, 2020); Kashmir Hill, *Flawed Facial Recognition Leads To Arrest and Jail for New Jersey Man - The New York Times*, New York Times, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html (last visited Apr 10, 2021).

and the fact that Mr. Oliver, Mr. Williams, and Mr. Parks were eventually able to demonstrate their unjust arrests should provide no comfort that these errors can be comprehensively surfaced.

Given this Administration's emphasis on scientific integrity and racial equity, future federally funded research initiatives in the criminal legal system should support not only evaluations of validity and reliability, but also of justice and equity measures.

Precedent exists for evaluating emerging technologies for measures beyond validity and reliability. In 1993, when the National Human Genome Research Institute was created, Congress mandated that not less than 5% of the budget be set aside for research on the ethical, legal, and social implications (ELSI) to address the issues raised by rapidly advancing genomic technology.[13] Over the years, the ELSI research program focused on public education, clinical integration, and regulation of genomic technologies, as well as on issues of privacy and consent. However, the ELSI program left the critical evaluation of genomic technologies understudied from another critical perspective: the social and political environment in which these technologies are developed, the role of discriminatory design, the dynamics of power that shape them, and the inequalities they breed.[14] Academics and advocates have called for or have developed privacy, surveillance, equity, as well as racial justice impact assessments for surveillance technologies.[15]

The Innocence Project believes that ethical, legal, and social implications; civil liberties; and racial justice and equity should be centered in the evaluation of surveillance technology and evaluated as **justice & equity (JE) impact assessments**. We also recommend that assessments be developed through a process that integrates the perspectives of affected communities and should be mandated for surveillance technologies **before** they are implemented. JE impact assessments can include, among other evaluations:

- Efficacy and accuracy. Even if a technology is used for investigative purposes only, what degree of accuracy would we demand?

[13] E. Hanna, *The Ethical, Legal, and Social Implications Program of the National Center for Human Genome Research: A Missed Opportunity?*, *in* Society's Choices: Social and Ethical Decision Making in Biomedicine (Ruth Ellen Bulger & Harvey V. Fineberg eds., 1995), https://www.ncbi.nlm.nih.gov/books/NBK231976/ (last visited Feb 23, 2020); Jean E. McEwen et al., *The Ethical, Legal, and Social Implications Program of the National Human Genome Research Institute: Reflections on an Ongoing Experiment*, 15 Annu. Rev. Genomics Hum. Genet. 481–505 (2014).

[14] Captivating technology: race, carceral technoscience, and liberatory imagination in everyday life (Ruha Benjamin ed., 2019); Sara M. Grimes & Andrew Feenberg, *Critical Theory of Technology*, *in* The SAGE Handbook of Digital Technology Research 121–129 (2013), http://methods.sagepub.com/book/the-sage-handbook-of-digital-technology-research/n9.xml (last visited Jun 11, 2021); Browne, *supra* note 2.

[15] David Wright & Charles D. Raab, *Constructing a surveillance impact assessment*, 28 Comput. Law Secur. Rev. 613–626 (2012); Critical Platform Studies Group et al., *Algorithmic Equity Toolkit* (2020), file:///C:/Users/sarah/Downloads/aekit_print.pdf; International Association of Chiefs of Police, *Privacy impact assessment report for the utilization of license plate readers* (2009), https://www.aclu.org/sites/default/files/field_document/33225-33317_FOIA_No._12-00328_Privacy_impact_assessment_report_for_the_utilization_of_license_plate_readers_publication.pdf (last visited Nov 15, 2021); National Association of Criminal Defense Lawyers, *Garbage In, Gospel Out* (2021), https://www.nacdl.org/Document/GarbageInGospelOutDataDrivenPolicingTechnologies (last visited Sep 16, 2021); Laura M Moy, *A TAXONOMY OF POLICE TECHNOLOGY'S RACIAL INEQUITY PROBLEMS*, 2021 Univ. Ill. LAW Rev. 55 (2021).

- Privacy and civil liberties. Does the technology impact privacy, civil liberties, or constitutional rights?

- Discrimination, disparate impact, and harms to groups of people based on their identity or poverty status? Does the technology subject people to harm based on their immutable characteristics or life circumstances?

- Duty to correct and notify. Are there procedures in place to identify, correct, and remediate errors as well as a process to notify affected parties?

- Transparency and accessibility. When this technology is used against a person, what information is disclosed and are there meaningful opportunities and resources available to verify or challenge the result?

- Less invasive alternatives. What is the stated problem that this technology aims to address? Are there less invasive alternatives or alternatives that promote the legitimacy of police investigations and the fairness of the criminal legal system?

- Procurement and institutional policies. The manner in which a technology is procured or contracted can create institutional incentives for performance or limit public access. How do these institutional practices affect the technology's implementation?

The evaluations should be developed by a task force of technologists, racial justice experts, civil liberties experts, researchers, community members, and other criminal legal system stakeholders. No amount of validation testing, standards development, or technical solutions will ensure the just and equitable application of surveillance technologies in the American policing system. While the development of a framework is an important first step to raising awareness regarding the harms that these technologies can impose on society, the application of the framework will always be limited when the social, political, economic, and structural solutions required for justice are out of the scope of a proposal. As JE impact assessments are conceptualized, they can facilitate the establishment of justice and equity measures that researchers can use to guide the development and testing of emerging technologies.

The International Association for Chiefs of Police (IACP) acknowledged in its 2014 Technology Policy Framework that "[t]echnological advances have made it possible to monitor and record nearly every interaction between police and the public" and police agencies are faced with how to select technologies that will achieve the greatest overall public safety benefits.[16] Critically, the IACP policy states, "Just because a technology *can* be implemented, does not mean that it *should* be." As a society, we would do well to remember these words.

[16] International Association of Chiefs of Police, *IACP Technology Policy Framework January 2014* (2014), https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf (last visited Sep 2, 2019).

Thank you in advance for your consideration of the feedback we respectfully offer. The Innocence Project looks forward to working with OSTP and the Biden Administration to advance equity in science and technology in the criminal legal system to ensure their simultaneous contributions to public safety, strengthening communities, and the just and equitable administration of justice.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Institute for Human-Centered Artificial Intelligence at Stanford University

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Stanford University
Human-Centered
Artificial Intelligence

Response to Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

The Stanford Institute for Human-Centered Artificial Intelligence (HAI) offers the following submission for consideration in response to the Request for Information (RFI) by the White House Office of Science and Technology on public and private sector uses of biometric technologies. While our intention with this response is to examine the uses of biometric technologies as per the RFI, we also take the implications of broader artificial intelligence (AI) technologies into consideration. Biometrics and AI are uniquely intertwined. We can decouple these two technologies only to an extent and must understand both the full impacts of AI and how the biometric paradigm disproportionately affects marginalized groups and exacerbates inequities. Following Dr. Eric Lander and Dr. Alondra Nelson's recent call for a bill of rights to safeguard the American public against powerful technologies in an opinion piece for *Wired*,[1] we produce this set of six principles that recommends:

- Ensuring AI-powered biometric systems are developed and deployed in a manner that supports fundamental democratic values with respect to the rule of law, basic civil liberties, and universal human rights.
- Safeguarding fairness and rights to nondiscrimination.
- Ensuring transparency and explainability during development and due process rights in application.
- Strengthening participation of civil society organizations in important AI use and governance conversations.
- Embedding accountability measures into system design.
- Enhancing citizen education in relation to AI and its impacts.

Ensuring AI-powered biometric systems are developed and deployed in a manner that supports fundamental democratic values with respect to the rule of law, basic civil liberties, and universal human rights

AI is arming governments with unprecedented capabilities to track, surveil, and monitor individuals.[2] For example, the pervasive tracking of individuals in public spaces via surveillance cameras, voice recognition systems, and social media not only interferes with individuals' rights

[1] Eric Lander and Alondra Nelson, "Americans Need a Bill of Rights for an AI-Powered World," *Wired* (2021), https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.
[2] Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," *Journal of Democracy* 30, no. 1 (2019): pp. 40-52, https://doi.org/10.1353/jod.2019.0003.

to privacy, but also affects their rights to freedom of speech, expression, and association.[3] The use of such technologies by law enforcement potentially alters how individuals exercise such rights, including fundamental democratic guarantees of lawful social and political participation and protest. In short, biometric tracking can chill the potential of participatory democracy.[4] Moreover, nation-states with known human rights abuses and unaccountable government institutions can exploit the power of AI and biometrics, which poses a direct threat to open democratic societies.[5]

Therefore, incorporating democratic and human-centered values in both public and private uses of AI should be the central concern in developing and deploying AI-powered biometric technologies. First, it is important to identify democratic principles that developers of AI systems should abide by, namely the rule of law, civil liberties, and universal human rights. The benchmark of democratic principles rather than democratically sanctioned policy is essential here. All governments must recognize that "democracy supporting technologies" does not simply mean developers complying with legislation or rules passed by a government of a democratic society, which could include illiberal democracies or democracies facing significant stress and decline.[6] The key tension is to navigate between companies adhering to the decisions made by governments in democratic societies and adherence to a set of democratic ideals. Building institutional arrangements for the latter is far more difficult and far more important.

In the United States, the commercial sector has been the primary incubator of AI innovation, but leaving AI technology free to develop without guardrails presents a wide range of dangers. Steps to embed democratic and human-centered values into AI development could include updating existing regulations on antitrust and nondiscrimination or enhancing rule-of-law practice such as designating oversight agencies to monitor and audit AI systems.[7] Moreover, funding academic research or public-private partnerships with an emphasis on incorporating democratic principles could foster the protection of individual liberties, human rights, and data privacy during the development phase.

Finally, building a pro-democracy technology alliance to coordinate strategies against the abuse of AI-powered biometric technologies can slow the development of AI-enabled digital

---

[3] Toni M Massaro, Helen Norton, and Margot E Kaminski, "SIRI-OUSLY 2.0: What Artificial Intelligence Reveals About the First Amendment," *Minnesota Law Review* 101 (2017): p. 2481, https://scholarship.law.umn.edu/mlr/179; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Books, 2016); Jeramie D. Scott, "Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space," *Journal of Business & Technology Law* 12 (2017): p. 151, http://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2; Joel R. Reidenberg, "Privacy in Public," *University of Miami Law Review*, 69, no.1 (2014): https://repository.law.miami.edu/umlr/vol69/iss1/6; Woodrow Hartzog and Evan Selinger, "Surveillance as Loss of Obscurity," *Washington and Lee Law Review*, 72, no.3 (2015): pp.1343-87, https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/10.

[4] Feldstein, 2019.

[5] Nicholas Wright, "How Artificial Intelligence Will Reshape the Global Order," *Foreign Affairs*, November 24, 2021, https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

[6] For example, the Freedom House published democracy ratings and scores for more than 100 countries, which show some so-called democratic countries with lower scores due to the absence of or decline in political rights and civil liberties: https://freedomhouse.org/report/summit-democracy/2021/summit-democracy-ratings-scores.

[7] Karl Manheim and Lyric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy," *Yale Journal of Law & Technology* 21 (2019): p. 106, https://yjolt.org/sites/default/files/21_yale_j.l._tech._106_0.pdf.

authoritarianism.[8] President Biden convened the inaugural Summit for Democracy in December 2021 that brought together leaders from government, civil society, and the private sector to tackle challenges confronting democracies and bolster democratic institutions. Specifically, the summit participants recommended we "invest in the development, use, and governance of technology that advances democracy and human rights."[9] Failure to bolster democratic institutions in the face of rapidly developing AI would diminish their relevance, and the private sector and authoritarian governments would become more powerful.

Ideas to Explore

- Update antitrust and civil rights regulations and enhance rule-of-law practice to compel the private sector to adopt a democracy-supporting and individual-rights-protecting vision of AI science and technology.
- Increase investment and fund academic research or public-private partnerships in AI-powered biometric innovations infused with democratic values.
- Support norm-setting efforts on AI-powered biometric technologies at the international level to support human rights and rule of law.
- Coordinate with other democratic countries and global civil society organizations to promote democratic values in AI and place export controls and human rights sanctions with its allies to deny authoritarian regimes resources used to develop mass surveillance technologies.

Safeguarding fairness and rights to nondiscrimination

From healthcare and education to finance and the environment, governments and industries around the world are embracing AI-powered approaches to doing business and solving social problems. AI applications have the potential to reduce discrimination caused by structural and systemic inequities as well as human subjectivity, yet they can also introduce or exacerbate bias leading to discriminatory decisions that create injustice and undermine public trust in AI. Research has shown that AI-powered biometric technologies have disproportionate impacts on women, underrepresented racial and ethnic groups, the LGBTQIA+, the economically disadvantaged, and people with disabilities.[10]

For example, a hiring algorithm used by Amazon to screen résumés scored the applications of men higher than those of women—including by downgrading résumés that contained words like "women's" and degrees from all-female colleges.[11] In addition, researchers have found major

[8] This is part of the recommendations in the National Security Commission on Artificial Intelligence (NSCAI) final report: National Security Commission on Artificial Intelligence, *Final Report* (Washington, D.C.: 2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[9] "Summit for Democracy Summary of Proceedings," The White House (The United States Government, December 23, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/23/summit-for-democracy-summary-of-proceedings/.

[10] David Danks and Alex John London, "Algorithmic Bias in Autonomous Systems," *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence*, 2017, https://doi.org/10.24963/ijcai.2017/654; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018): pp. 1-15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Ben Hutchinson et al., "Unintended Machine Learning Biases as Social Barriers for Persons with Disabilities," *ACM SIGACCESS Accessibility and Computing*, no. 125 (October 2019): p. 1, https://doi.org/10.1145/3386296.3386305.

[11] Jeffrey Dastin, "Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women," Reuters, October 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bia

commercial facial recognition systems, built on the processing and analysis of biometric data (specifically, face images), often perform far more accurately on lighter-skinned faces compared to darker-skinned faces and on faces of male individuals compared to faces of female individuals.[12] They performed worst of all on the faces of Black women.[13] Moreover, it is important to acknowledge that discrimination is not simply non-recognition, or being unseen. In other words, it is not just a problem of data or solving accuracy. We must address issues outside of the technology realm, such as certain populations being overly-surveilled by institutions of power.[14]

State governments are increasingly allowing or requiring AI-powered risk assessment tools in criminal justice sentencing decisions,[15] which raises important concerns about explainability, equal protection, and due process. Due process is a constitutional right provided by the Fifth and Fourteenth Amendments that ensures fairness in legal proceedings and safeguards defendants against erroneous deprivations of life, liberty, and property. Using such tools may introduce bias into the decision-making of sentencing without any potential for explaining a black-box decision, thereby undermining the due process right.[16] For example, if a dataset is missing input from particular populations or infected by past discriminatory practices, using that dataset to build an AI-powered sentencing tool may yield results that are unfair or inequitable to certain underrepresented or protected groups.

Therefore, designing fair algorithms is more important than ever. One of the challenges in making AI systems fair lies in deciding how to make mathematically tractable the ideal of "fairness." The case of the COMPAS algorithm, a proprietary algorithmic-based risk assessment tool developed to help parole boards assess recidivism risks, provides an example of such a challenge. A study by ProPublica found that while the tool correctly predicted recidivism for Black and white defendants at roughly the same rate, it misclassified the Black and white defendants over a two-year follow-up period.[17] Developers of the COMPAS technology argued that the algorithm was fair since it predicted the same likelihood of recidivism across all groups regardless of race.[18] But the ProPublica study shows that Black defendants are more likely to be classified as higher recidivist risks than white defendants, and Black defendants who do not re-offend are predicted to be riskier than white defendants who do not re-offend.

---

s-against-women-idUSKCN1MK08G; Rob Reich, Mehran Sahami, and Jeremy M. Weinstein, *System Error: Where Big Tech Went Wrong and How We Can Reboot* (New York, NY: Harper, an imprint of HarperCollinsPublishers, 2021).

[12] Buolamwini and Gebru, 2018.

[13] Buolamwini and Gebru, 2018.

[14] Ruha Benjamin, 2019, *Race After Technology: Abolitionist Tools for the New Jim Code* (Polity, 2020); Catherine D'Ignazio and Lauren F. Klein, *Data Feminism* (Cambridge, MA: The MIT Press, 2020)

[15] John Lightbourne, "Damned Lies & Criminal Sentencing Using Evidence-Based Tools," *Duke Law & Technology Review* 15 (May 14, 2017): p. 327, https://scholarship.law.duke.edu/dltr/vol15/iss1/16.

[16] Black-box here refers to the system or model not being able to explain its output or decision, see: Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2016).

[17] Jeff Larson and Julia Angwin, "How We Analyzed the COMPAS Recidivism Algorithm," ProPublica, May 23, 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

[18] Julia Dressel and Hany Farid, "The Accuracy, Fairness, and Limits of Predicting Recidivism," *Science Advances* 4, no. 1 (2018), https://doi.org/10.1126/sciadv.aao5580.

While there has been much research on how to quantitatively evaluate fairness, there is no general consensus.[19] The problem is twofold. First, defining fairness is not an easy task—there can be multiple reasonable conceptions of fairness. The normative approach to ensure fairness treats everyone the same. But such an approach fails to take into account that not everyone starts off on equal ground, with equal resources and access to the same opportunities.[20] For example, consider the question of public school funding. It might seem that equal per pupil funding is what fairness requires. But do children with special needs—physical or cognitive handicaps—deserve identical funding as children without special needs? Fairness here seems to require greater funding for those with special needs. So to promote fairness and achieve equity, one should not aim to treat everyone the same, but to remove structural barriers to equal access to the opportunities, with the recognition that even this alone is insufficient to mitigate systemic inequities that persist. In other words, equal access is but one, if essential, step towards "fairness."

Second, fairness could be construed as the property of an individual or of groups.[21] In the example of criminal justice sentencing, the former means defendants with identical criminal histories receive the same predictive score when reviewed by algorithms, whereas the latter refers to the share of ethnic minority defendants who are rated with the same level of recidivist risk as that of ethnic majority ones. While both conceptions of fairness seem reasonable and both have limitations, it is challenging to adopt both at the same time when designing algorithms.[22]

Where there is no singular definition of fairness, AI systems designed to maintain the status quo—as the COMPAS algorithm is set up to do—have the potential to perpetuate and exacerbate inequality. Therefore, to build fair AI systems, we need to define and quantify what we mean by a fair outcome—that is, truly equal access to resources at the beginning and attention to the backend impacts, whether or not there were claims a process was "fair."

Ideas to Explore

- Identify fairness considerations and approaches up-front, and involve multi-stakeholders, such as experts in the relevant domain and across disciplines, in the conversation.
- Explore a legally viable path for algorithmic fairness under current constitutional doctrines.[23]
- Develop testing and monitoring mechanisms to detect and mitigate fairness-related harms.

[19] Mulligan et al., "This Thing Called Fairness: Disciplinary Confusion Realizing a Value in Technology," Proceedings of the ACM on Human-Computer Interaction 3, no. 119 (2019): p.119, https://dl.acm.org/doi/10.1145/3359221.
[20] Benjamin, 2019; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019); Safiya Umoja. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018); Neda Atanasoski and Kalindi Vora, *Surrogate Humanity: Race, Robots, and the Politics of Technological Futures* (Durham: Duke University Press, 2019).
[21] Reich, Sahami, and Weinstein, 2021.
[22] Reich, Sahami, and Weinstein, 2021.
[23] Daniel E. Ho and Alice Xiang, "Affirmative Algorithms: The Legal Grounds for Fairness as Awareness," *The University of Chicago Law Review Online*, October 30, 2020, https://lawreviewblog.uchicago.edu/2020/10/30/aa-ho-xiang/.

Ensuring transparency and explainability during development and due process rights in application

Many elements of the rule of law and democratic societies rely on access to information. Transparency facilitates public discourse, evidence-based policymaking, regulatory oversight, judicial review, and journalistic scrutiny.[24] In the case of AI-powered biometric technologies, understanding how AI systems work and how algorithms arrive at their decision promotes public trust in the responsible use of such technologies and ensures democratic norms during development and application.

However, private companies often keep crucial information about the inner workings of AI systems under wraps. This makes it difficult to understand exactly how biometric information is processed and where errors in biometric data analysis may originate. The black-box nature of AI systems, or not knowing how an algorithm reaches its conclusion, only adds to this opacity. This results in an information gap that prevents the public from knowing or responding to any AI missteps. Employers, for example, are increasingly using video surveillance and webcams that collect biometric information like eye movements or facial expressions to track worker performance.[25] Without understanding how those technologies work, employees are unable to get a justification or explanation of an AI-based decision and lose their ability to appeal to such a decision as a result.

While we might not know how an AI system produces unintended results, we can know what was intended for the system in the first place. Requiring the transparency of training data and procedure, documentation detailing performance characteristics, and iterations of algorithms, for example, sheds light on the explainability of AI systems. Moreover, access to reliable explanations for different audiences is equally important. The "right to explanation" clause in the European Union General Data Protection Regulation (GDPR) requires businesses to provide rationales for decisions made by the AI system.[26] Such an explanation could be used, for example, as a basis for the public's right to appeal against an automated decision.

Ideas to Explore

- Develop audit trail requirements and documentation of AI-powered biometric systems that cover all steps of the AI development process, which could include model architecture, training data, records of exhibited bias and previous predictions, etc.
- Require private companies to provide a right to explanation of decisions made by automated or AI systems.

[24] Beth Simone Noveck, "Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency," *Yale Human Rights and Development Law Journal*, 2017, https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=2208&context=fac_articles_chapters.
[25] Darrell M. West, "How Employers Use Technology to Surveil Employees," Brookings Institution, January 5, 2021, https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/.
[26] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," EUR-Lex, May 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

- Implement executive and legislative actions to mandate developers of AI systems to provide access for auditing via independent regulatory agencies, such as the Federal Trade Commission (FTC), or third-party organizations.
- Implement bias and safety bug-bounty programs, allowing individuals to report algorithmic bias or security vulnerabilities to an organization and receive rewards or compensation, for AI systems to increase incentives for broader scrutiny of AI systems.

Strengthening participation of civil society organizations in important AI use and governance conversations

To help address the challenges AI-powered biometric technologies raise, the role of civil society is more important than ever. Civil society consists of nongovernmental and not-for-profit organizations outside the public and private sectors "that have a presence in public life [and] express the interests and values of their members and others, based on ethical, cultural, political, scientific, religious or philanthropic considerations."[27] Such organizations bring important perspectives to discussions over how to harness the power of AI to benefit all parts of society while also minimizing any negative impacts on protected groups. Civil society also forms an important bulwark against authoritarian and unaccountable governments.

Civil society has a history of advocating a human-centered approach on behalf of underrepresented or marginalized populations.[28] For example, in the face of new emerging risks during past industrial revolutions, organized associations, such as faith-based charities and labor unions, and other friendly societies, helped improve worker conditions and reduce new emerging risk.[29] Today, civil society can play a similar role to shape the future of biometric technologies.

As governments and private companies confront the issue of engaging with the public and earning their trust when deploying AI-powered biometric technologies in sensitive sectors like healthcare and finance, civil society can bring balance and perspective to the conversation. It can fill blind spots and ease fears among those who stand to lose the most in a world dominated by unchecked algorithms and data.

Ideas to Explore

- Mandate federal and local governments to consult representatives from community and civil society organizations when developing rules and regulations related to AI.
- Require private companies to conduct stakeholder consultations with civil societies and seek out their guidance during the development of AI technologies to augment human capabilities and ensure the inclusion of diverse developers of AI systems, representative datasets, and nondiscriminatory practices.

Embedding accountability measures into system design

[27] "Civil Society," World Bank, n.d., https://www.worldbank.org/en/about/partners/civil-society/overview.
[28] Wendy Pojmann, *Migration and Activism in Europe since 1945* (Palgrave Macmillan, 2016).
[29] World Economic Forum, *Civil Society in the Fourth Industrial Revolution: Preparation and Response*, 2019, https://www.weforum.org/whitepapers/civil-society-in-the-fourth-industrial-revolution-preparation-and-response.

The democratic governance of AI-powered biometric technologies requires strong accountability mechanisms to keep these systems in check—for instance, so others can intervene in the event of dangerously incorrect decisions. This goes hand in hand with transparency: While the preceding transparency and explainability point focuses on developers, it is also essential for third parties to be able to access that information and hold systems accountable in response. A lack of accountability can be incredibly dangerous in certain settings, such as with opaque AI applications making recommendations or decisions in a medical setting.[30]

Part of this is technical. Independent, third-party organizations need access to AI system data and code to run technical audits or impact assessments. New York City, for example, adopted a law to require third-party bias audits of algorithms used by employers in hiring or promotions.[31] Third parties like researchers, civil society groups, community organizations, and regulators also need access to transparency and explainability information used internally by an organization, so they can fully understand and assess the design and deployment of AI-powered biometric technologies. Industry can also embed accountability mechanisms into system design, such that human interventions are possible (e.g., in clinical settings and law enforcement settings) as necessary.

Other parts of internal accountability regimes, however, are not technical. Companies developing AI tools need not only internal ethical guidelines (e.g., policies on transparency and explainability) but also human involvement in accountability structures, such as "rank-and-file employee representation on the board of directors, external ethics advisory boards, and the implementation of independent monitoring and transparency efforts."[32] Congress, for example, has introduced bills in the past few years to mandate companies to conduct annual audits or impact assessments of AI algorithms.[33]

Ideas to Explore

- Implement executive and legislative actions to allow third-party auditor access to AI data and source code, as well as other transparency and explainability information, for the purposes of external researcher, civil society, and regulator assessments.
- Consider best practices that could be recommended to industry for embedding accountability mechanisms to test the outcome or results of its AI systems.

Enhancing citizen education in relation to AI and its impacts

[30] Helen Smith, "Clinical AI: Opacity, Accountability, Responsibility and Liability," *AI & SOCIETY* 36, no. 2 (2020): pp. 535-545, https://doi.org/10.1007/s00146-020-01019-6.
[31] "Automated Employment Decision Tools," The New York City Council, December 11, 2021, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=ID.
[32] Meredith Whittaker et al., "AI Now Report 2018," AI Now Institute, December 2018, https://ainowinstitute.org/AI_Now_2018_Report.pdf.
[33] Congress.gov. "H.R.2231 - 116th Congress (2019-2020): Algorithmic Accountability Act of 2019." April 11, 2019. https://www.congress.gov/bill/116th-congress/house-bill/2231; Congress.gov. "Text - S.2968 - 116th Congress (2019-2020): A bill to provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement." December 3, 2019. https://www.congress.gov/bill/116th-congress/senate-bill/2968/text.

Understanding of AI is becoming a more important part of modern civic participation as AI-powered biometric applications are already shaping how citizens receive political advertisements, political news, and voting information around elections through social media platforms. Akin to the rapid emergence of computer science (CS) coursework in secondary schools, developing and enhancing education around AI and biometrics would empower citizens to better participate in the emerging policy and civic discourse around these technologies. Notably, this can also occur through government agencies doing public outreach, exploring curricula in public schools, and supporting related research in higher education. It is incumbent upon the federal government to initiate, design, and promote educational programs to better inform the American public on the ethical and rights-based challenges of AI and biometric technologies.

More than half of US high schools now offer CS courses, in light of the growing role of software in daily life and in recognition of the growing value of exposure to programming.[34] There are still troubling inequities in the quality, accessibility, and tailoring of this education across racial, gender, and socioeconomic class lines. For instance, one study found that significant performance gaps in CS coursework emerge between male and female students as early as 10 years old.[35] Nonetheless, this kind of education exposes citizens at an early age to CS, which touches every aspect of their lives. This can increase familiarity in general by engaging with powerful technologies, and it also gives future voters substantive exposure to software that shapes daily life. It must be done, however, with substantial focus on technology ethics—something missing in many current CS education programs—and in this case, with a focus on the ethics of designing, developing, and deploying AI and biometrics systems. This should include understanding the ethical implications of these technologies, the ethical frameworks and policies in place around their development, and what future ethics should look like, from engineers to regulators.

CS and AI coursework are also becoming increasingly important in higher education. According to the 2021 AI Index, the number of undergraduates completing CS degrees in 2019 is three times higher than the number in 2010.[36] On the graduate level, the number of AI and machine learning-specialized CS PhD graduates among all new CS PhDs in 2020 is 8.6 percentage points larger than in 2010—the most significant growth, relative to 18 other specializations.[37]

AI is a multidisciplinary field. It is important to develop and enhance AI education programs outside of the CS domain, including humanities, arts, and social sciences. Citizen education is increasingly necessary to enable democratic participation in the age of AI. Understanding these technologies is increasingly vital for everyday life.

---

[34] Alyson Klein, "More than Half of High Schools Now Offer Computer Science, But Inequities Persist," *Education Week* (November 5, 2021), https://www.edweek.org/teaching-learning/more-than-half-of-high-schools-now-offer-computer-science-but-inequities-persist/2021/11.

[35] Jennifer Tsan, Kristy Elizabeth Boyer, and Collin F. Lynch, "How Early Does the CS Gender Gap Emerge?," *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, 2016, https://doi.org/10.1145/2839509.2844605.

[36] Daniel Zhang et al., "The AI Index 2021 Annual Report," March 2021, https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf.

[37] Zhang et al., 2021.

Ideas to Explore

- Build AI themes, including AI ethics and the technology's impact on society, into Department of Education recommendations on technology and CS education.
- Engage with civil society to understand best practices and substantive options for AI educational programs.
- Conduct a study on existing CS and other multidisciplinary education programs related to AI nationally to understand equity and inclusion issues so as to inform the development of AI education.
- Ensure executive branch policies on AI are communicated clearly to the public, with discussion of their possible impacts on society and on communities.

As lead authors, we proudly submit this response on behalf of our colleagues and the Stanford Institute for Human-Centered Artificial Intelligence (HAI).

Michele Elam
William Robertson Coe Professor of Humanities, Stanford University
Faculty Associate Director, Stanford Institute for Human-Centered Artificial Intelligence (HAI)

Rob Reich
Professor of Political Science, Stanford University
Faculty Associate Director, Stanford Institute for Human-Centered Artificial Intelligence (HAI)

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Integrated Justice Information Systems Institute

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

RESPONDENT INFORMATION AND BACKGROUND

a. Organization and Respondent

Respondent Name:

Maria Cardiellos

Executive Director

[redacted]

Respondent Address:

Integrated Justice Information Systems Institute (IJIS)

20110 Ashbrook Place, Ste. 150

Ashburn, Virginia 20147

[redacted]

http://www.ijis.org/

Type of Organization:

Private Nonprofit

b. Organization Overview

The Integrated Justice Information Systems Institute (IJIS) was founded in 2001 as the result of the Department of Justice's (DOJ) interest in engaging private sector participation in the advancement of national initiatives affecting justice and public safety and more recently homeland security (including school safety) and health and human services. We are a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity. IJIS is the only national membership organization that brings together the innovative thinking of the private sector and practitioners, national practice associations, and academic organizations that are working to solve public sector information and technology challenges. IJIS advocates for policies,

processes, and information sharing standards that impact our safety and security; build knowledge on behalf of our stakeholder groups; and, connects the organizations and leaders within the communities of interest.

Additionally, IJIS provides a trusted forum within and across our areas of focus where resources are developed, collaboration is encouraged and public sector stakeholders can realize the benefits of technology and the power of information to keep our communities safe, healthy, and thriving. We assist in government sectors by bringing industry to the table in a constructive role and continuing to drive toward achieving high regard for the companies that are dedicated to helping the public sector find high-value solutions. IJIS is funded through a combination of federal grants, industry contributions, and partnership agreements.

Finally, IJIS is an active member of several committees, forums, etc., in support of the public sector mission joining practitioners and providers at the many working tables. Examples include the DOJ Global Advisory Committee, the IACP CJIS Committee, and the many IJIS Advisory Committees that include the IJIS CJIS Committee, the Law Enforcement Advisory Committee, the Court and Corrections Advisory Committees, and the Technical Architecture Committee – all these include practitioners, services providers, academia and research experts nationwide.

c. The State of Biometric Technologies

As industry, practitioners, and policymakers, we all tend to forget the amount of time it takes to perfect certain technologies, even in the field of biometrics. Once a new technology is developed, it takes decades to understand its true effectiveness, develop proper policy, and fully understand proper usage and legal implications. For example, fingerprints were first used in law enforcement in the late 1800s to early 1900s with the first official fingerprint card being developed in 1908. The FBI did not form an identification division for another 16 years in 1924. It took another 56 years for the first Automated Fingerprint

Identification System (AFIS) database to be developed. Currently, there are over 70 million cards with 700 million fingerprints in AFIS. Even today, these computerized generated matches are often followed by human verification in major cases.

Likewise, the first usage of DNA in law enforcement was in 1986. However, it took years of debate, legal policy reviews, ethical discussions, and technology advancements before the courts would accept DNA as evidence. DNA technology has advanced rapidly since its first use in a criminal case 40 years ago. Now many states require DNA collection for sex offenders and felony offenders. There is still much policy work to do in the field of DNA collection to close collection gaps and auditing to ensure that legislation is fully met. Evidence retention policies are a critical need for law enforcement to protect this evidence and retention policies to use DNA technology successfully.

Fingerprints and DNA are just two examples of biometric technologies that took decades to fully develop. Given that technology and research have advanced significantly we should expect newer identification technologies such as facial and retina recognition to take time to mature and perfect much quicker than fingerprints, but perfection requires the use, testing, policy development, ethical review, and clear governance.

d. IJIS Differentiators / Uniqueness

IJIS recently celebrated the milestones and all of the accomplishments in our 20-year history. Our success is built on our community of collaboration that represents our public and private sector members; our practitioner community nationwide as well as our subject matter experts that balance operational realities with proven results; our research and academic partners that contribute innate skills that assess and evaluate value; national membership organizations that represent public sector domains spanning justice, health and wellness, school safety, technology, and so many others; and, proven leaders in their fields demonstrating initiative management and implementation skills nationwide with so many success stories.

Given this array of talent that IJIS can offer in support of the DHS OSTP effort, our community organization is such that we engage the best resources from the different communities nationally to best respond to the goals and objectives of the given request for service. Such is the case with this RFI – we could recruit and/or issue a call for participation from our membership to support any of the defined topic areas. Understanding the critical value of governance in the constitution, vision definition, buy-in and support, policy adherence as well as long term implementation and support – "governance programs, practices, and procedures (applicable to the context, scope, and data use of a specific use case)." is that topic area upon which the IJIS response will focus.

d. Governance Programs, Practices, or Procedures

Law enforcement, courts, corrections, and policymakers require clear guidance and policy when implementing new technologies. This can only be achieved with proper governance. Governance is important to evaluate technologies and to establish standard operating procedures within legal limits that govern how and when technology should be used. Users of these technologies must be provided a strict set of rules by which they must operate. Those rules, often referred to as Standard Operating Procedures (SOPs), guide the use of the technology, how it is conducted, and to ensure its success. These policies and practices provide clear guidance, manage expectations, and reduce frustrations.

As part of the RFI, the following are the stated priorities that must be considered when proposing a governance methodology. Though not a one-to-one correlation, the IJIS proposed governance model addresses the intent of each concern.

i. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;

ii. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

iii. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;

iv. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;

v. Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);

vi. Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);

vii. Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems; and,

viii. Practices for public transparency regarding the use (including notice of use), impacts, opportunities for contestation, and redress, as appropriate.

The stated purpose of the RFI is to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or might be, impacted by their use or regulation. To ensure the comprehensive review, assessment, adherence to and implementation, and support of a solution that will meet the policy, operational and technical needs of a user community (relative to defined use cases), a proven governance model is critical to success. IJIS *has successfully used* a proven governance model that founded the success of over twenty (20) national programs across the nation in support of information sharing (several funded by DHS, DOJ OJP, BJA,

BJS, and others). This *proven model/methodology is comprised of four (4) pillars of success* that will effectively respond to supporting any implementation or advances made in the usage of biometric technologies to support specific use cases within the public safety domain. They include the following:

Policy and Governance ensures the gathering and analyzing of information on the missions, goals, strategies, policies, and operational challenges reflected of the participating domains, agencies, stakeholders, etc.;

Business Processes and Operations ensures alignment of business processes and operations with existing and/or new policies and governance models. It will also support the definition and address the priorities of the proposed Steering Committee depicted in the provided graphic.

Systems and Technologies will focus on determining what solutions are in place, how they can be improved or enhanced, and providing guidance related to the development and implementations of biometric technologies and data access across agencies, domains, etc. to ensure alignment with operation and policies; and,

Outreach and Communications (O&C) will ensure that – as progress is realized on the policy, operational, and technical fronts – proper messaging is developed to support education, engagement, participation, and ultimately new technologies that might otherwise cause consternation to any constituent groups. The proper education and socialization plan is so critical to the success of these efforts that IJIS will engage expert practitioners, partner organizations, and other resources including those from the field as needed. Each messaging tool (in the format of training, TA, or other support interactions) will build upon—new knowledge, current and emerging best practices, developed toolkits, and other resources that are integrated and replicable—helping the program remain at the forefront in providing critical services to all stakeholders.

Though specific goals and objectives would be developed to support a successful governance model in

support of advancing the proper usage of any new biometric technology, IJIS' experience has shown high-level goals should address no less than the following intentions:

1) Ensure engagement of the key constituencies to be directly or indirectly impacted by the new technology implementation. Commitment or buy-in of executives from each of the participating domains/organizations (as part of the proposed Executive Steering Committee depicted) will ensure the support of supporting members of those agencies (to comprise the Subject Matter Expertise (SME) Council, as well as the Policy, Operational and Technical Working Groups also depicted.
2) Ensure the successful alignment of mission needs with existing and newly developed processes, policies, and technologies.
3) Ensure the constitution of both an Audit and Evaluation program components to measure the progress, impact, and necessary improvements warranted over time.
4) Given the progress that is sought during the initiative, ensure the proper and timely communication is delivered consistently and effectively to all participating domains, agencies, practitioner groups nationally, and the public that will benefit from the overall educational impact.

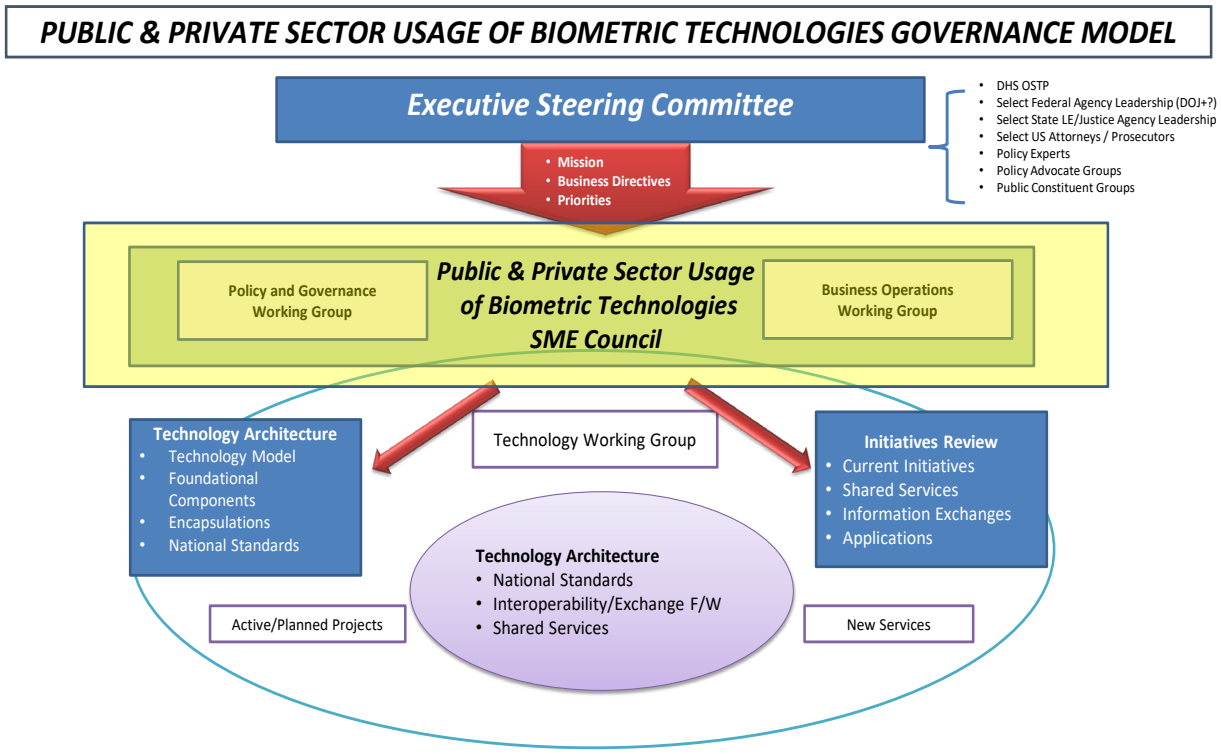
The overarching "steps" – and services available to support same from the IJIS Institute – to constitute the proposed governance model include the following:

Standup a National Public and Private Sector Biometrics Technologies Steering Committee

Success requires a multidisciplinary approach led by stakeholders that represent the landscape of services offered, as well as the populations to be served. Leadership, vision, buy-in, engagement, and even education are all critical aspects of a successful governance model to address emerging solutions, be that on a local level let alone a national perspective. Leaders in each of these fields or domains should

constitute the Executive Steering Committee, as well as provide Subject Matter Expertise (SMEs) to support other aspects of the governance model and program implementation if necessary.

A representation of the proposed governance model is provided below. The graphic depicts the critical components to include the Steering Committee as discussed above, along with the supporting SME Council that will be organized into three subgroups to address Policy and Governance, Business and Operational issues, as well as Technology and Architecture needs. It is important to note that this governance body is not a transitional entity to address any specific project alone. ***It is a governance structure that should be codified to address the critical needs of Public and Private Sector Usage of Biometric Technologies nationwide.***



<u>Support the Development of Priorities for the National Public and Private Sector Biometrics Technologies Steering Committee</u>

The IJIS Team proposes to work with the National Public and Private Sector Biometrics Technologies

Steering Committee to develop a comprehensive assessment, review, implementation (if appropriate), and evaluation of biometric technologies used in the public and private sectors. Though one can anticipate the challenges that are evident in responding to such an effort, the proposed working sessions with the Steering Committee will not only identify the priorities as they exist today but will enable us the dialogue to identify and address operational efficiency opportunities, and policy guidelines that will impact the outcomes in the future. Each of the intended Committee members will bring a vast array of diverse experiences that collectively represent national trends, challenges, and gaps to be addressed. The IJIS Team proposes to work with Steering Committee members to

a) convene critical players that make up the participating members;

b) facilitate a dialogue to identify the common gaps that members experience when trying to implement and/or consider such technologies;

c) assess the operational and policy implications that impact a common solution;

d) design a solution that meets the collective needs of the community, and

e) outline a plan for implementation of a pilot to validate its effectiveness.

Subsequent support/activities that can be provided – but exceed the direct constitution of the governance model (though the committees would be engaged) - including the design and development of minimum guidance to be made available to both public and private sectors on the implementation and use of biometric technologies; the constitution of a national model repository to server as a resource bank for future implementations; the development of model policies to be used by participating implementation agencies; the assembly of a training and technical assistance resources that can guide agencies in the development of related programs; and the possible development of web-based resource center providing actionable resources, templates, and relevant content around research, policy, and governance, business process and operations, best practices, lessons learned, voices from the field, and systems and

technologies, as well as serve as a library of comprehensive training.

e. Conclusion

IJIS Institute has a proven success record of employing a methodology that constitutes the engagement of disparate user groups/domains, etc. on the federal/state/local levels, the facilitation of same to arrive at a design/development (with our private sector partners) / implementation/support of a solution that will meet the needs of the champion agency/domain. Critical success factors will always be founded on a governance structure that supports policy assessment/development/adherence at all levels of participation (FSLT). Our record of over twenty years delivering solutions nationwide that remain in operation today is proof of our success.

Though there is much more detail to provide and/or suggestions to offer in the evaluation of responses to this DHS OSTP RFI, the page limitation mandates that this narrative be brought to a conclusion. IJIS has successfully supported DHS and other federal partners with numerous national initiatives that include the Nationwide Suspicious Activity (SAR) Initiative (NSI), the National Fusion Center Initiative, the current CAD to CAD Interoperability initiative and so many others. We look forward to the opportunity to support this valuable effort and to tailor a solution-set that meets the priorities of the public and private sectors' use of biometric technologies properly and successfully nationwide.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

International Association of Chiefs of Police

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200 | Alexandria, VA 22314, USA | [redacted] | www.theIACP.org

January 14, 2022

VIA ELECTRONIC SUBMISSION: [redacted]

The Office of Science and Technology Policy (OSTP)
Eisenhower Executive Office Building
725 17th Street, NW
Washington, D.C., U.S

Re: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (Document Citation: 86 FR 56300)

Introduction

The International Association of Chiefs of Police (IACP) is the world's largest and most influential professional organization for law enforcement leaders. With more than 31,000 members in 165 countries, the IACP is a recognized pacesetter in global policing, committed to advancing safer communities through thoughtful, progressive law enforcement leadership.

While all policing decisions are fundamentally made by humans, the law enforcement community often uses appropriate technologies to help identify potential investigative leads which would otherwise be overlooked or extremely expensive and time-consuming to find. Literally millions of crimes would go unsolved and their victims left without justice were it not for certain technological and scientific processes which the computer age continues to provide. Additionally, digital evidence is pervasive, voluminous and extremely complex. Protecting the innocent requires an exacting and robust application of technology.

This is especially important in the current law enforcement environment. There are many challenges facing police leaders, including difficulties maintaining and hiring a police force, increasing crime, pandemic pressures, and justice reform expectations. Therefore, law enforcement executives need to take advantage of new technologies wherever possible to help alleviate these new challenges. All while maintaining the agency's legitimacy and trust in the communities they serve. New public safety endeavors must be thoughtfully considered. Any technology must bring significant benefits to our communities that greatly outweigh risks. Especially when applied and managed within a mature policy and quality control context.

Our response to the Office of Science and Technology Policy's (OSTP) Request For Information (RFI) is therefore based on where law enforcement has been with biometric technologies, where it is today and what we can see in the near future, especially regarding the enhancements Artificial Intelligence (AI) adds to such processes to assist in policing our communities. As will be set forth in greater detail below, the IACP strongly believes that AI-assisted biometric technologies are providing, and will continue to provide, substantial contributions to public safety in a wide range of disciplines. Any efforts to limit or burden the deployment or use of these technologies should be carefully balanced against the harm that the technologies are preventing.

Over the past three decades, the technology industry has risen to the challenges of the policing community. Initially focused on the first wide-scale biometric identifier (fingerprint matching), the technologies have transformed the successful prosecution of crime based upon not only eyewitness testimony and/or suspect admissions but also scientific study and digital evidence. The development of fingerprinting changed policing so much that virtually all criminal identification and background/history checks require the use of fingerprint-based lookups utilizing automated technologies as the first and primary step. In more than five decades of wide scale usage, the justice community and the public have completely accepted the use of fingerprinting as a trusted and important clue in criminal investigations. Fingerprints are so mainstream they are used for everything from clearing volunteers to work with children to providing top secret clearances for access to the most important critical homeland security information.

However, it is important to understand that Biometrics and Artificial Intelligence have been separate concepts to the law enforcement community until the last decade. In our response, we do not specify the intrinsic value or problems with any specific technology, but instead address how law enforcement, and specifically the IACP, understands and values the merger of these technologies, plus how we need to strongly encourage police agencies worldwide to deploy them appropriately, fairly, and with full transparency so that the necessary pillars of community trust, citizen support, and public privacy are strongly maintained.

Law Enforcement History in Biometrics

The law enforcement community's interest in biometrics is primarily in the ability of the technology to automate and improve the quality of currently manual processes. By its nature, law enforcement routinely involves the observation and identification of persons, property, and objects. The growth in both the population and the number and sophistication of crimes has challenged the ability of law enforcement agencies to fulfill their basic charge with the limited human and technological resources they possess. Consequently, law enforcement has integrated advanced communications and computer technology to improve operations, from radio technology in the 1930s to centralized computerized criminal information databases in the 1960s and 1970s. Just as those technologies helped make law enforcement more effective, efficient, and responsive to the community, tools that make use of artificial intelligence will further enhance policing services.

An Example of Biometrics in Law Enforcement

A key example has been the rise of the use of fingerprints in law enforcement. Beginning in the late 19th and early 20th century, fingerprints were discovered to be effectively unique biometric identifiers.

Latent prints are fingerprints present at a crime scene but not easily captured or imaged. A latent fingerprint examiner handles capture and identification processes, including taking photos of fingerprints or utilizing different methods of latent fingerprint identification in the crime scene and identifying the fingerprints by running them against the automated fingerprint systems.

Besides their use in crime scene forensics, they also had a powerful use in the Criminal Identification (CI) activity of law enforcement. Knowing the identity of an individual involved in an incident is key to understanding the nature of a crime and the individual’s possible prior acts. Consequently, at the time a suspect is booked in jail, fingerprints are captured to determine the person's identity. This is

important if the subject has used other names (aliases) for previous arrests identification. Most importantly, the fingerprints are captured for the purposes of recording the arrest and/or conviction information in a permanent file associated with that person. Finally, captured fingerprints will typically be used to determine the person's prior arrest and conviction record.

Initially local agencies and later the Federal Bureau of Investigation (FBI) began cataloging criminally involved fingerprints in America. By 1971, the FBI had over 200 million fingerprints on file. The quantity and size of this catalog demanded a technology solution to be able to take a subject's fingerprints and be able to compare them to the full catalog that the FBI possessed. This has resulted in several generations of systems that were initially developed to handle fingerprint comparison. These systems, until recently, evolved without the use of todays' AI. The latest iteration is the FBI's Next Generation Identification system. NGI handles not only fingerprints, but other biometrics, such as facial, retinal, and iris comparisons.

Operationally, these next generation systems have been able to handle the demands of growth. However, there are limitations. Unless a perfect set of data is presented, such as a quality fingerprint scan for a criminal history check, it is very likely a precise result of the search cannot be made. This results in either a low quality match or a candidate list of possible matches. At this point a certified fingerprint expert needs to become involved to evaluate the output of the biometric systems. To limit or remove any bias that may exist, blind identification - the confirmation of a latent print examiner's conclusion by another competent examiner who has no expectation or knowledge of the prior conclusion - is used.

The algorithm's limitations made a fundamental requirement for human intervention and review of any "match" before returning information to the requestor. This has become ingrained into the environment, such that even today on any potential match, the question arises "did a fingerprint examiner review and agree with the results?" Without that agreement by an uninvolved, certified examiner, there is no expectation the identification will hold up in Court.

Resulting Policy and Protections

Once fingerprint comparison became an accepted practice, there grew a need to create and maintain best practices based upon the latest technology, science, and accepted principles. Fingerprinting was the basis upon which the first forensic professional organization, the International Association for Identification (IAI), was formed in 1915. In 1977, this group developed the first professional certification program for forensic scientists, the Certified Latent Print Examiner program, which issued certificates to those meeting stringent criteria.

Human experts with these certifications provide a buffer and a control for the computerized biometrics systems. Furthermore, the experts provide legal accountability in situations where the results of a technology system may be in question. The IACP and law enforcement community understand that no technology is perfect, but the value of the technologies with human supervision is powerful and compelling.

No member of the public is ever charged with a crime based solely on the output of these fingerprint systems and processes. Instead the information produced is treated merely as a "lead" for the

investigative process. This concept, though different for each technology, is a fundamental guiding principle for the use of these technologies in law enforcement.

Lessons Learned from Automated Fingerprint Technology

There are several important lessons which are drawn from the law enforcement experience with fingerprints and helpful to guide use of other biometrics technologies and AI:

1. Automated Systems are Powerful – The growth of biometric identification both in subject identification and crime forensics has been possible because of the "automation" of the processes. When humans are the primary factor in the workflow, things become slow and error-prone.
2. System Limitations Must be Understood – The better the data, the better the results. When the data is limited or suspect - for example, in forensics - more human involvement is needed to ensure the quality and integrity of the system.
3. The Data Gallery Must be Protected – The gallery is the basis against which a present item is compared. This means the data, whether it is fingerprints or photos, must be of high quality and appropriate. Otherwise, the automation will fail with poor quality and less "narrowing" of possible matches.

There are other desirable outcomes from the adoption of biometric and fingerprint technology. Some individuals who were wrongly convicted using less technologically effective methods were released and convictions reversed. Furthermore, in these cases the actual perpetrator was identified for the first time through fingerprints. Without fingerprint technology, it is very likely these convictions would not have been overturned, with the wrong individual being incarcerated for a crime they did not commit. Similar positive outcomes have occurred with the development and deployment of DNA-based technologies. We expect that these new AI technologies will continue to find perpetrators that could not be identified with older technologies and processes. What is clear from our experience in law enforcement is that the best outcomes combine a human component, which ensures accountability, with the efficiencies gained through the use of automated systems.

Evolution of Artificial Intelligence

Artificial Intelligence (AI) is not a new concept. Scientists have been studying and conducting AI research in many forms since at least the 1940s. A recent report to Congress prepared by the Congressional Research Service noted that "the field" of AI research began in 1956, but an explosion of interest in AI began around 2010 due to the convergence of three enabling developments: (1) the availability of "big data" sources, (2) improvements to machine learning approaches, and (3) increases in computer processing power. This growth has advanced the state of Narrow AI, which refers to algorithms that address specific problem sets like game playing, image recognition, and navigation. All current AI systems fall into the Narrow AI category. The most prevalent approach to Narrow AI is machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets. During the training process, the computer system creates its own statistical model to accomplish the specified task in situations it has not previously encountered. Experts generally agree that it will be many decades before the field advances to develop General AI, which refers to systems capable of human-level intelligence across a broad range of tasks.

Nevertheless, the growing power of Narrow AI algorithms has sparked a wave of commercial interest, with U.S. technology companies investing an estimated $20-$30 billion in 2016. Some studies estimate this amount will grow to as high as $126 billion by 2025. For purposes of this document, we are only concerned with Narrow AI.

Use of AI in Law Enforcement

This significant investment has brought forward new applications of AI to help law enforcement better utilize such things as Automated License Plate Recognition (ALPR) and Facial Recognition (FaceRec) technologies. It is important to realize that although much of law enforcement activities do focus on suppressing criminal activities, policing involves a broader array of services. For example, the police often interact with law-abiding citizens who may be at risk or in danger due to mental impairment or their status as a reported missing person. Experience shows many of the biometrics technologies have been useful for helping the police assist the public by being able to identify individuals in a non-intrusive way.

The lack of intrusiveness of biometrics also creates different challenges for law enforcement. Privacy advocates have legitimate concerns that these systems can be used for constant surveillance. In general, law enforcement does not operate that way today in the United States. However, the right approach is to provide transparency of how the biometric technology is being used by the agency through policy documents that can be shared with the public. Tools such as regular audits can provide supporting evidence that systems are being used in a manner that is consistent with agency policy.

The law enforcement professionals that make up the IACP can point to many direct and substantial public safety benefits made possible by AI-assisted biometric technologies. We are also well aware that the public has legitimate concerns about ensuring that these technologies are deployed in a way that is responsible, proportional, and respectful of civil liberties. Since these truths exist together, we support the OSTP's commitment to soliciting input from all stakeholders on how biometric technologies can best serve the public interest.

The law enforcement community has more than twenty years of experience with computer biometrics. The awareness of the limitation of the technologies has led to procedures, practices, and policies to protect both the integrity of law enforcement operations and the rights of individuals.

Key Guiding Principles for the Use of Biometric/AI in Law Enforcement

Any change in a technology can be difficult for an organization or group to absorb without some guiding principles to serve as a lens to evaluate and critique it. Therefore, based on previous experience, we can offer clear principles for law enforcement using these tools:

- These systems are only tools; however, they offer great efficiency improvements by automating tasks that were previously manual and yielding helpful insights and patterns that might otherwise go undetected. Automation in law enforcement should always include the important element of human verification and validation.
- Agency governance of AI technology in law enforcement must be clearly defined, codified in policy, and oversight rigorously exercised to build and preserve the public’s trust.

- Accountability, in a legal sense, can only apply to human beings in law enforcement. This means an agency must own the technology they deploy. They are ultimately responsible for how it is deployed and used operationally.

The IACP has had extensive experience in applying new technology to law enforcement activities. All police agencies deploying such technologies need to document and codify the policies of use. Because of this primary need, IACP has created a formalized framework to address new technology implementations.

IACP Technology Policy Framework

As the leading professional organization for law enforcement, we seek to provide guidance to law enforcement agencies both within the United States and worldwide. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology *can* be implemented does not mean that it *should* be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

Addressing these challenges is paramount because the array of available technologies is expanding. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe. Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and liberties of individuals, and upholding the privacy protections afforded to the data collected, stored, and used is essential to ensure effective and sustainable implementation and to maintain community trust. Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance.

A short form of the key principles of the IACP Technology Policy Framework:

1. **Specification of Use –** Precisely define the intended use of all agency technology to include the agency's detailed purpose and objectives as well as description of use that is prohibited.
2. **Policies and Procedures –** Develop appropriate and reasonable technology controls with common sense supporting procedures and guidelines.
3. **Privacy and Data Quality –** Describe how the integrity of the technology and resulting data will be ensured. Conduct both privacy and quality assessments for all employed technology.
4. **Data Minimization and Limitation** – Articulate how reasonable minimization of data collection and use is ensured and why overreach should not be a concern.

5. **Performance Evaluation –** Explain how the agency will periodically evaluate the performance and the value of the technology not only to the agency but foremost to the community.
6. **Transparency and Notice –** Design and implement technology with a reasonable ability to allow for public transparency. Even when certain data or details cannot be reasonably made public, ensure transparency of the existing controls and oversight are publicly available.
7. **Security –** Describe how the technology and related data is protected in terms of risk management and security. Ensure both positive and negative outcomes are shared with the community.
8. **Data Retention, Access and Use –** Ensure that data retention is planned with a view of the technology life cycle, minimal access and legally intended use. Plan for adequate retention to support oversight and transparency; however, preclude that data retention does not exceed acceptable and intended use.
9. **Auditing and Accountability --** Codify enterprise-wide accountability from authorization to operate, through continuous monitoring, and regular audit of all use.

These nine principles are the base concepts that are important for any new technology to be deployed by law enforcement. Each item can be discussed extensively with any technology; however, there are considerations unique to AI.

Specific Principles and Concerns for Biometric/AI Technology

The principles discussed above should be used to guide development of the following areas of attention before biometric or AI technologies are deployed:

Technology Use Policy

Many of the biometric technologies, because they are non-intrusive, do not get the rigorous review of conditions of appropriate use. Agencies need to consider when it is appropriate to use technology in question. Many times this will/should be dictated by law and agency policy. However, because the law often takes time to catch up with technology, we can expect there will be situations that the executive and legislative branches of governments at all levels will need to weigh in.

More specific to agencies is the need to determine which personnel are authorized to use a technology. This should be a function of need, training, and certification.

Protecting Privacy of the Public

This is probably the most difficult aspect of Biometric/AI technology use. The public has the right to express concern about the power of government even though they freely share biometric information with social media sites, who have stated that they are using the same or even more sophisticated technology for facial recognition.

Mass image capturing and usage, such as that which is collected from red-light cameras or surveillance video, is another citizen concern. Similarly, images and data residing in popular social media systems and other publicly collected facial image repositories do not inherently violate privacy laws, but use of these image galleries by the government often leave the public very uncomfortable.
Context is everything in these situations. Looking for an abducted child is going to be perceived by most of the public as an appropriate use of a public image capturing. In contrast, looking for people who

haven't paid their parking tickets by using traffic cameras is generally not well regarded. This is further reason policy is key to guiding law enforcement staff as to appropriate and publicly acceptable usage of biometric technology.

Appropriate Reference Data Gallery/Sources

The gallery images (reference database of known persons/entities), especially in a facial recognition application, that should be used by law enforcement are those of a high quality. This usually means that they are collected in controlled environments, or post-processed to obtain quality without damaging the image information. Examples of this would be booking workstations when subjects are arrested and processed.

Reference data and test/probe images acquired from third party entities need to be treated as suspect and vetted appropriately.

Security

A quality data gallery must be adequately protected and secured as it is a prized compilation. Such a valuable data collection will attract parties interested in accessing, copying, or stealing the information. As exemplified by the 2015 hacking of the U.S. Office of Personnel Management, the combination of biometric, demographic and biographic information is of supreme interest to foreign military and intelligence agencies seeking to identify employees and personnel in sensitive roles.

Training/Certification

Training is a multifaceted issue. Certainly there are the basics of how to use the technology, and the need for professional and use certification when those exist. However, equally important is understanding the applicable laws, regulations, and policy that apply to the technology.

Audits

Audits are a common practice in law enforcement, especially in the Criminal Justice Information Systems (CJIS) environment. The CJIS environment commonly deals with criminal histories and usually will facilitate access to information regarding driver's licenses and vehicle registrations. The easy access for a sworn or civilian agency employee provides a temptation for misuse. The knowledge of an audit process can be a deterrent to bad behavior, or even uncover training and use case issues that were not clearly understood by the agency when the technology was deployed.

Furthermore, agencies need to implement Quality Management controls. These controls track the usage, success and failures of the technology. These controls start with policy statements that precisely define the intended use, avoided use, and adequate controls/oversight to ensure integrity of both.

Audits provide transparency to the public and are a key tool for law enforcement agencies to maintain community trust.

Balancing Policy Against Use

Ultimately, we want to ensure technologies assist officers and investigators in most efficiently solving crimes. Agencies and regulators have to be careful not to implement technology use policies that are so restrictive that the public benefits are all but diminished. Consideration should be given to balancing both risk and efficiency when developing policy. If a policy creates hurdles that make the use of

technology exceedingly difficult or impractical, end users may avoid using the tool(s), thus squandering the potential public benefit of this technology.

Any national policy recommendation on the use of AI-assisted technologies should identify the benefits of a technology as clearly and emphatically as its risks or other possible collateral impacts. The government should carefully identify and quantify the tangible public safety benefits of particular technologies, both in terms of cases solved and efficiencies realized, as well as describing potential harms. Mitigating controls should be carefully crafted to limit real and measurable abuses of the technology, rather than theoretical dangers.

Discussion of Individual AI Technologies in Law Enforcement

Our response to the RFI so far has been focused on law enforcement's long history of biometric technology usage and the formalized method through the IACP Technology Policy Framework agencies should be using.

Artificial intelligence is currently being used in a wide variety of applications in policing today, some of which extend beyond just biometrics.

Several current and envisioned uses of AI in law enforcement include:

- Criminal Investigative Use
  - Automated detection of victims and perpetrators in video data from seized cell phones and computers in sexual exploitation investigations
  - Detection of objects and people in video data during criminal investigations
- Field Operations and Criminal Investigation Use
  - Automated facial image comparison, fingerprint comparison, retina comparison, and DNA profile comparison for lead generation in criminal investigations and identification of incapacitated individuals
- Evidence Processing and Privacy Protection
  - Automated redaction of sensitive objects and Personally Identifiable Information (PII) in video recordings
  - Automated removal of illicit images and videos of victims
  - Expedited review of video recordings, including videos voluntarily shared with law enforcement by members of the public
- Training and Education
  - Detecting law enforcement officer and private citizen sentiment in audio data of police interactions for the purposes of problem behavior detection and officer training
- Non-Biometric Uses
  - Automated license plate recognition and comparison for investigative lead generation
  - Remote detection of weapons using imaging radar data prior to arresting a person and during responses to people in crisis
  - Cybersecurity threat detection, mitigation, and investigation
  - Automated gunshot detection and location to reduce shooting response times
  - Recognition of patterns in criminal justice data including arrest reports, narratives, and criminal history records

In all of the applications listed above, technology is being used as a tool to gather or synthesize information for law enforcement purposes. However, similar to virtually every other police technology tool or system, AI-derived information must only be seen as a piece of evidence about criminal activity or citizen identity. The conclusions of an AI-assisted biometric system should not be understood as stand-alone proof of a particular fact. It can and should be understood as an investigative lead generation tool, and when properly corroborated and supplemented by human actors, one of the many building blocks of probable cause.

Conclusion

AI-enhanced capabilities have increased significantly during the past decade, as computing power, automated processing, and storage capacities have increased. While new public safety benefits can be achieved, challenges must be met and addressed prior to the implementation of new technologies. Police users of these systems should have a solid understanding of AI and specifically machine learning to fully comprehend both its potential positive and negative impact on the community. Failure to fully comprehend the power of biometrics and AI could leave law enforcement legally vulnerable and unaware of valid citizen concerns.

In utilizing biometric/AI applications, agencies should be cognizant of technology limitations and remain diligent in their adherence to principles outlined in the IACP Technology Policy Framework and established standards when available. Responsible use, operational transparency, protection of data, and documented verification of results will also continue to be critical for successful adoption and public acceptance of AI technologies as public safety tools - much the same way they were for the successful development and use of fingerprint systems.

Most importantly, as powerful and impressive as AI-enhanced technologies may seem, when used as investigative tools, the results they generate are only leads or starting points. Most importantly, it is the police officer, detective, investigator, or analyst who must consider that lead and corroborate it with other gathered evidence and testimony while comparing it to the requirements of law which guide our community's behavior. Only after careful investigation and impartial human deliberation of all the facts can a decision be made to question, detain, exonerate, or arrest a person. No matter the wonderment of computer technology and its many current and future advancements, it is the trained and ethical law enforcement professional who must stand before a judge and jury to swear to the innocence or guilt of a fellow citizen. In our noble profession, we must always fight to provide justice to victims of crime and we believe that AI technologies enable law enforcement to be more effective and efficient in accomplishing that goal.

Sincerely,

International Association of Chiefs of Police (IACP)
44 Canal Center Plaza, Suite 200, Alexandria, VA 22314
Respondent Type: not-for-profit 501c(3) organization

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

International Biometrics + Identity Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

International Biometrics+Identity Association

Office of Science and Technology Policy
The White House
1650 Pennsylvania Avenue, NW
Washington, DC 20502

January 14, 2022

Submitted Electronically via email to: [redacted]

Subject: OSTP Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (*Federal Register* Document No. 2021-21975)

On behalf of the International Biometrics + Identity Association (IBIA) and its membership, we are pleased to submit this information to OSTP in response to the Request for Information (RFI) regarding "Public and Private Sector Uses of Biometric Technologies" (*Federal Register* Document Number 2021-21975).

Information Requested

Our responses provide an overview of the specific use of biometric technologies in the public and private sectors, as requested in RFI topics 1 through 6.

Topic 1: Descriptions of use of biometric information for recognition and inference.

Biometrics are unique physical (anatomical or physiological) or behavioral characteristics which can be used to identify individuals. Biometric technologies capture, process and measure these characteristics electronically and compare them against existing records to create a highly accurate identity management capability. As previously mentioned, common physical biometric indicators in use today include fingerprints, faces,[1] irises, voices, and DNA, among many other modalities.

Biometrics have been around for over 100 years in various forms around the world and for various use cases. In the U.S., the techniques of measuring fingerprints, latent fingerprints, and palm prints grew in popularity among the law enforcement community in the early 20th century. The modern digital version of biometrics in use today by law enforcement or national security professionals was developed about 45 years ago. The technology has progressed rapidly in the past 20 years, largely due to heavy investment in research and development. This progression has also accelerated in the last 10 years due to advancements in computing technology that made practical the deep neural networks associated with machine learning approaches to biometrics.

[1] For more information, *see* https://www.ibia.org/download/datasets/5733/IBIA%20Facial%20Recognition%20Use%20Cases%20FINAL.pdf.

Topic 2: Procedures for and results of data-driven and scientific validation of biometric technologies.

Such procedures largely fall into two categories: algorithm testing and full system testing. Our member companies do both types of testing, both by performing internal tests and by submitting their algorithms and systems to independent, third-party testing entities.

Most biometric algorithms (including those of our member companies) are subjected to the objective and public testing of the National Institute of Standards and Technology (NIST). NIST has been researching, testing, and developing standards for biometric technologies for six decades.[2] NIST testing, which uses known and repeatable data, has demonstrated that top-performing face recognition,[3] iris recognition,[4] and fingerprint[5] algorithms can achieve accuracy rates of over 99%. For face recognition technologies, NIST has specifically evaluated algorithm performance across age groups, racial groups, and sexes. Of particular note, NIST has found that the top-performing algorithms exhibit "undetectable" differences in false positive error rates across demographic groups based on race and sex.[6]

For most biometrics other than DNA, statistical results of testing are often graphically displayed in the form of Receiver-Operator Characteristic (ROC) or Detection Error Tradeoff (DET) curves. ROC curves show how an algorithm performs as its discrimination threshold is varied. That is, how the true positive rate of matching or identification (sometimes called "accuracy") varies as the acceptable false positive ("impostor") rate is increased. DET curves show how the false negative rate (truthful match rejected) varies as the false positive rate (impostor accepted) varies. Such curves help an operator set an algorithm threshold that is optimal and acceptable for their application, process, and risk tolerance. For a specific example of the application of such testing technique for face recognition, see the IBIA analysis of NIST testing of demographic differentials in IBIA member algorithms.[7]

Operational performance[8] of biometric technologies also depends on environmental conditions that vary across use cases and functional applications. The impact of such factors on overall biometric technology performance can be more objectively quantified in testing, such as Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Biometric

---

[2] https://www.nist.gov/programs-projects/biometrics

[3] https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

[4] https://pages.nist.gov/IREX10/

[5] https://www.nist.gov/programs-projects/fingerprint-vendor-technology-evaluation-fpvte

[6] P. 8 – https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[7] https://www.ibia.org/download/datasets/5725/IBIA%20Diversity%20Data%20Analysis%20Unabridged%20FINAL.pdf

[8] Assessing operational performance often entails evaluating not only accuracy but also factors including capture rate, failures to enroll, and speed of operation.

Rally tests, which measure biometric technologies' full system performance.[9] These Biometric Technology Rallies, which DHS S&T typically holds at the Maryland Test Facility (MdTF), include diverse test subjects and environmental factors that are present in a variety of operational settings, including TSA and CBP security checkpoints in airports. Even in these environments, DHS S&T Biometric Rally tests have demonstrated biometric technologies' high accuracy rates. Of particular note, recent face recognition technology Rally tests have demonstrated that top-performing face recognition technologies are over 98% accurate at identifying individuals wearing face masks and are over 99% accurate at identifying individuals who are not wearing face masks.[10]

For DNA use in human identification, a number (currently 20 for FBI CODIS) of genomic loci with so-called short tandem repeat sequences, or STRs, is used for comparing DNA samples. The probability of match for two DNA samples at each locus can vary by population sub-group, so population statistics ("popstats") are used to qualify the probability of match. These popstats are derived from genetic population models developed over the years. In practice, a DNA match is further qualified by the number of loci detectable in the sample vs the reference DNA profile. Like other biometric modalities, the data and science behind DNA uses for human identification are well-developed.[11]

Topic 3: Security considerations associated with a particular biometric technology.

Generally, the use of biometric factors in identity management increases the security of the systems that use such factors in both logical and physical security applications. In logical security applications, we cite NIST FIPS-201 section 6.3.2 where it states that the addition of a biometric for logical access control imparts "HIGH" or "VERY HIGH confidence."[12] The use of such techniques can prevent breaches due to threats from insiders sharing or using credentials from others to gain access to more compartmentalized data to which they aren't entitled. While this is true and effective for preventing access intrusions "through the front door", cyber threats due to network intrusions or unwitting user installations of malware can present a much more serious challenge. There is no biometric panacea for prevention of cyber-intrusions, and there is no substitute for diligent cyber hygiene, effective cyber policies, and effective automated cyber intrusion tools. Multi-factor authentication using biometrics is one layer in what needs to be a multi-layered cybersecurity defense.

Much has been made of so-called "presentation attacks" using fake or spoofed biometrics. Defense against this type of attack is why FIPS-201 insists on in-person biometric enrollment, so the operator can verify that the biometric(s) presented by the subject at enrollment is (are) indeed genuine and not fake. Subsequent detection of impostors using a valid enrolled subject's biometrics (e.g. fake fingerprint, print-out of a face, contact lens covering iris) are either detected by in-person witness, or automated sensor actions such as liveness detection. Methods of

---

[9] https://www.dhs.gov/science-and-technology/biometric-technology-rally

[10] https://mdtf.org/Downloads/MatchingSystemResults.pdf

[11] https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet

[12] https://nvlpubs nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

liveness detection vary by biometric modality. For example, to mitigate the printed face attack, the sensor must detect eye blinks or eye motion or changes in facial expression or aspect. Newer iPhones image the face in 3 dimensions, which effectively counters the 2-dimensional printed face attack. For fingerprints, the sensor may do liveness detection by sensing galvanic skin response, skin spectral response, or subcutaneous blood flow. Painted contact lenses as an iris spoofing approach are detected in infrared imaging, and even more advanced iris spoofing detection techniques are being developed.[13] Replay attacks (recording someone's voice and replaying it to spoof speaker verification) can be detected both through spectral (frequency) analysis as well as by prompting the speaker to speak voice segments that could not have been recorded earlier (as well as adding other identification factors like a PIN or texted security code – leveraging the power of multi-factor authentication).

For physical security, we cite the example of CBP's use of facial biometrics for matching to passports.[14] "This enhanced process using facial biometrics only takes a few seconds and is more than 98 percent accurate." As noted in the IBIA paper cited previously, the 98% accuracy cited by CBP is far superior to the typical human trying to do facial matching or recognition. "To date, more than 119 million travelers have participated in the biometric facial comparison process at air, land, and seaports of entry. Since September 2018, CBP has leveraged facial biometrics to prevent more than 1,100 impostors using genuine travel documents from illegally entering the United States at air and land ports of entry."

Topic 4: Exhibited and potential harms of a particular biometric technology.

Answers to this question could fall across two different categories, depending on the interpretation of the question. One category is potential harms of the technology itself, and the other is harm that could occur from the applications of the technology.

To the first category, we are not aware of any exhibited or potential harms of the biometric technology by itself. The infrared illumination required by iris recognition is harmless. The use of contact-style fingerprint readers in high-volume public applications is sometimes cited as a potential source of contagion, but that hasn't proven to be the case for SARS-CoV-2, which is transmitted via inhaled microdroplets. Some contact fingerprint readers have UV sanitizing illumination that turns on between uses of the readers, thus sanitizing them. In other cases, the operators simply swab the capture platen with alcohol between uses, which both sanitizes and cleans the surface for better capture of the next fingerprints.

For the second category, as with any technology, people can misuse it. To counter this, the IBIA has developed ethical principles and best practices, detailed in our responses to Topic 6 sub-paragraphs. In short, we don't support uses of biometrics to oppress a country's citizens or to discriminate against any class of people or suppress First Amendment rights to free speech and assembly. We don't support real-time uses of biometrics for surveillance (e.g. in conjunction

---

[13] https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool html&r=5&f=G&l=50&co1=AND&d=PTXT&s1=9,934,436&OS=9,934,436&RS=9,934,436

[14] https://www.cbp.gov/newsroom/local-media-release/cbp-expands-simplified-arrival-four-ports-entry-washington-state

with video surveillance) unless authorized by court order, similar to wiretap restrictions. However, forensic biometric analysis after crimes have been committed should always be allowed, as in the case of the Capitol insurrection or the Boston Marathon bombing. Proposals to ban the technology mean that urgent uses of the technology for forensics after emergent events may not be possible.

To be clear, identity verification such as performed by TSA or CBP in the course of their legal obligations is **not** surveillance (see Topic 6f). Use of biometrics by companies for such things as security, convenience and attendance recording should always be allowed, so emerging state restrictions (such as BIPA[15] in Illinois) are inappropriate and should be preempted by Federal law.

Topic 5: Exhibited and potential benefits of a particular biometric technology.

One of the most striking use cases that illustrates the benefits of biometrics is in the case of travel under pandemic conditions. For example, the TSA has developed self-service credential verification stations ahead of checkpoints, which allow passengers to insert their own ID into a machine and have their face (unmasked at that point) matched to the image. TSA has also piloted face matching without the credential, leveraging capabilities first demonstrated and now widely deployed by CBP. The system developed by CBP is called "Simplified Arrival", and some people characterize it as "your face is your passport". [16] In both the TSA and CBP cases, travelers can verify their identities without having to interact closely with officers, thereby saving time, increasing accuracy, and maximizing hygiene. If you've ever been on a cruise ship, you know how much time it takes to embark and debark the ship, particularly if customs and immigration processing is required. Face recognition simplifies and speeds the process. Based on feedback from participating cruise lines, CBP reports a reduction of debarkation times as much as 30%, with a concomitant improvement in passenger satisfaction survey scores vs. non-biometric debarkation processing.

Generally, travelers appreciate touchless processing, and biometric sensors are available for touchless processing using face recognition, iris recognition, fingerprint recognition, voice recognition, and gesture recognition. Other environments where touchless biometrics are beneficial include chemical or biological hazard areas, nuclear or explosive materials processing, and applications that require hands-free for other purposes.

The benefits of fingerprints, latent prints, and DNA are well-known for forensic purposes, and consumers are increasingly willing to use fingerprint or face recognition technologies to unlock their smart phones and other devices. Voice processing, or more specifically voice verification, has been used for some years in verifying the voices of callers for financial transactions or remotely providing government services.[17] Behavior biometrics are used for continuous authentication of computer system users, and to detect insider threats based on indicative

---

[15] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[16] https://www.cbp.gov/sites/default/files/assets/documents/2018-Aug/Simplified_Arrival_Fact_Sheet.pdf

[17] https://www.ato.gov.au/general/online-services/voice-authentication/

changes in behaviors. Face and image recognition technologies have also helped officers generate investigative leads for crimes including bombings, insurrections, as well as human and child trafficking.

Topic 6: Governance programs, practices or procedures applicable to the context scope, and data use of a specific use case.

IBIA has published a number of documents outlining our views on governance programs and best practices that help mitigate risks and support the benefits that biometric technologies can produce. A significant example of this is our "Ethical Use of Biometric Technology"[18] white paper, which we believe is foundational for our industry.

Topic 6a: Stakeholder engagement practices for system design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies to mitigate the potential harm or risk of biometric technologies.

There are numerous and diverse applications of biometric technologies, and more will emerge over time. For that reason, it must be left to the use of a specific application to evaluate how to appropriately apply these general principles, taking into consideration the: a) application; b) purpose of the application; c) risks and consequences of abuse; d) personal and non-biometric data used; and e) legal and regulatory constraints, including privacy laws. There are no less than 29 federal laws that include privacy provisions, and diverse and proliferating laws being proposed and enacted at the state level.

Given the complexity and diversity of both the technology and the legal/ethical considerations, IBIA focuses on education and outreach to encourage enlightenment and diversity of dialogues on these important topics. To this end, IBIA and its members have participated and, in many cases, led the efforts to engage stakeholders and advocate for guidelines regarding policies, laws, principles and best practices. Examples include:

- **NTIA General Framework for Privacy** - IBIA Participated in the Department of Commerce, National Telecommunications and Information Administration (NTIA), Multi-Stakeholder Process to develop and publish a general framework for the commercial use of facial recognition titled the "Privacy Best Practice Recommendations for Commercial Facial Recognition Use."[19]
- **Annual connect:ID / Identity Week Conference** – IBIA co-sponsors this annual event that brings together government, academia, industry, privacy and policy experts all for the express purpose of discussing not only the latest trends in the technology, but also best ways to test, deploy, and enhance the technology in support of our customers and their missions. We also host specific panels on the ethical use of automated identity data as a social good.[20]

---

[18] https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf

[19] https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology

[20] https://www.terrapinn.com/exhibition/identity-week-america/index.stm

- **Active Member of the Future of Privacy Forum** – IBIA has been an active member of the Future of Privacy Forum for 5 years. We have had a strong, collaborative relationship. Together, we have worked with FPF to co-develop papers on privacy issues, biometrics and identity technology, and education efforts.[21]
- **Publication of White Papers and Industry Best Practices Guidance** - IBIA routinely publishes white papers on privacy policy principles, ethical use, impact of demographics, security and safeguarding data, industry best practices, and implementation guidance for use cases of biometric and identity technologies. [22]
- **Participation in Public Discourse and Debate** – We have testified before various Congressional Committees on various topics relating to biometric technologies over the past 10 years.[23] [24]

Topic 6b: Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments.

We are not aware of published best practices in this area, though the industry and most users follow some generally accepted principles which may vary depending on the use case and biometric modality (or modalities) employed. For example, for a biometrically enabled travel lane (ship debarcation, airport immigration, security checkpoint, jetway boarding), the trial or pilot should be limited in scope, with alternative travel lanes (e.g. "opt-out"), well-advertised, and attended by observers and helpers who can note difficulties and assist travelers who encounter trouble moving through the trial lane. "Well-advertised" can be local signage, instructional videos on display screens, recorded announcements, and public notice (e.g. websites and social media) all the way to formal notices of proposed rulemaking (NPRM) in the Federal Register. Comments from the public on the pilot both before (e.g. in response to a solicitation of comments on an NPRM) and after experiencing the pilot (e.g. satisfaction surveys) inform the results of the trial and help the organizers make improvements and respond to needs and feedback. This valuable feedback can be utilized in associated policy development.

Topic 6c: Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices.

See our response to topic 6h. Both our commercial best practices and Government PIAs and SORNs address these topics.

Topic 6d: Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use.

---

[21] https://fpf.org/

[22] https://www.ibia.org/resources/white-papers

[23] https://science house.gov/hearings/the-current-and-future-applications-of-biometric-technologies

[24] https://docs house.gov/Committee/Calendar/ByEvent.aspx?EventID=105757

While biometrics are not secret, most agencies and companies treat them as personally identifiable information (PII), especially in conjunction with associated biographics. Therefore, the best practice is to protect such data by encryption at rest and encryption in transport. Access to the data is protected by mandatory (e.g. classification level) and discretionary (e.g. need to know) access control (often both logical and physical), usually enforced by required multi-factor authentication as referenced in Topic 3. Security logs record who has accessed the data, for what purpose and when, and periodic audits verify that the logs have recorded activity that is permitted (or not). Automation is available to monitor the logs for suspicious activity so that immediate alerts are generated between audit periods. This approach mitigates the insider threat (an authorized user who abuses the system). Operationally, automated workflow systems can ensure multiple levels of review are conducted in accordance with policy (e.g., automated biometric system finds candidates, which go to an examiner to refine, which go to a supervisor for review and approval or rejection).

Topic 6e: Performance auditing and post deployment impact assessment (including benefits relative to current benchmarks and harms).

See our response to topic 6h. IBIA advocates best practices to include post-deployment audits of operations to ensure that proper procedures are being followed, that the system operates as intended, and there is no abuse or insider threat. We do recommend that operators periodically review current performance testing on biometric systems (e.g., through recent NIST testing publications) and consider upgrades where advancements show pronounced benefits (e.g. security, accuracy, throughput, response times, cost) over legacy systems.

Topic 6f: Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage).

This question implies that the author considers biometric technologies to be surveillance technologies, and this is not the case. Surveillance is using humans or automation to persistently observe an environment to derive intelligence, detect adverse behavior, or – when recorded – to forensically analyze circumstances leading up to an event of interest (perhaps for purposes of attribution). There are many forms of surveillance, including aerial imagery, data mining, social network analysis, computer, communications, RF (including RFID and geolocation), geophysical, audio (e.g. gunshot detection and location) and video surveillance. The most common form of surveillance in civilian use today – video monitoring of roads and cities – is very useful for traffic flow monitoring, security monitoring, and emergency dispatch awareness – but this infrastructure will also be foundational to some functions of smart city evolution. However, city surveillance with real-time facial recognition should be governed by policy and law and used in limited (perhaps only court-prescribed) circumstances. We tend to think of these types of applications for identifying criminals or terrorists, but there are other applications of the technology, like finding missing children, identifying exploited children, and identifying trafficked, missing or disoriented adults (e.g., with amnesia, dementia or Alzheimer's disease). Facial recognition is always warranted for forensic analysis after an emergency event, especially when no other useful evidence is immediately found, and the need is urgent.

A facial recognition system is designed to present matching candidates from its accessible gallery(s) of faces to that of the subject of interest. Contrary to popular belief (or urban legend), there is no single comprehensive government database of faces of US citizens, nor is there any unified national surveillance system. If the facial recognition gallery(s) do not have a face already enrolled, the system cannot match or identify the subject of interest.

As for record linkage, linking a person's biometric (face) to other information, while possible, is less useful to a (cyber) criminal than linking a Social Security number to a birthdate. The latter can be used to steal a person's identity, while a face or fingerprint by itself cannot. Indeed biometrics, when available, can expose such subterfuge, as in the 1,100 cases cited previously where CBP has discovered people attempting to enter the country with fraudulent or stolen passports.

Topic 6g: Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems.

Biometrics (e.g. fingerprints, DNA) have been admissible in court for years (albeit usually with a human examiner to provide testimony). Presumably, this question refers to face recognition, not by eyewitness, but by machine (algorithmic) search. There is precedent for admissibility of "predictive coding" in court.[25] However, as the technology is rapidly evolving, it is reasonable to expect that legal precedent will evolve as well. The issues of explain-ability, fairness, and trustworthiness apply here, and this is an active topic of development for many applications of machine learning (sometimes known as AI/ML).[26] Meanwhile, the FBI and others are treating machine-generated candidates in facial searches only as investigatory leads, especially where there is a paucity of other leads. That is, it isn't actionable evidence, and certainly not evidence of guilt. Other more traditional evidence must be discovered to confirm (or negate) such leads before more serious law enforcement actions are taken. We believe that this "human in the loop" operation is likely to remain the standard for the foreseeable future, and the process must be backed up by policy, training, oversight, access control, and periodic audit.

Topic 6h: Practices for public transparency regarding: Use (including notice of use), impacts, and opportunities for contestation and for redress, as appropriate.

For Government applications of biometrics, transparency is assured through the required publication of Privacy Impact Assessments[27] [28], and System of Records Notices.[29] [30] PIAs, for example, contain information on a system that includes a description, the information in the system, sources of information, threats to privacy, purpose and use of the system, why the

---

[25] https://scholar.google.com/scholar_case?case=6856971937505165396&q=da+silva+moore+v.+publicis&hl=en&scisbd=2&as_sdt=2,44&as_ylo=2012

[26] https://www.leidos.com/enabling-technologies/artificial-intelligence-machine-learning

[27] https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29

[28] https://www fbi.gov/services/information-management/foipa/privacy-impact-assessments

[29] https://www.dhs.gov/system-records-notices-sorns

[30] https://www.justice.gov/opcl/doj-systems-records

information is being used, legal authorities for operation, how long the information will be retained, with whom it will be shared, requirements for notice, consent and redress, security controls, and applicability of the Privacy Act. Regarding SORNs, from the DHS citation, "a system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the *Federal Register*."

For commercial uses of biometrics, IBIA has developed "Privacy Policy Principles" that provide general guidelines use of biometric technologies and data, while allowing implementers and operators to customize their approaches based on the biometric technology application(s) used and the potential risks and benefits associated with the given use-case.[31] In these Principles, IBIA recommends that implementers and operators of commercial biometric technology develop and publish privacy policies incorporating a Collection Limitation Principle, a Purpose Specification Principle, a Data Quality Principle, a User Limitation Principle, a Security Safeguard Principle, an Openness Principle, and an Accountability Principle. Others have developed similar frameworks and principles. A useful reference for law enforcement uses of face recognition technology is the Bureau of Justice Assistance Face Recognition Policy Development Template[32].

Conclusion

Thank you for giving us this opportunity to present this submittal to you and your colleagues at OSTP. IBIA is dedicated to the ethical use of biometrics and welcomes opportunities to participate in multi-stakeholder dialogues and to serve as a resource to policymakers and media outlets interested in discussing and working to address these important topics. We look forward to continuing the dialogue and working with your Office and other organizations and individuals who have also provided comments and insight for this RFI.

For More Information, Please Contact:

Robert A. Tappan
Managing Director
International Biometrics + Identity Association
[redacted]

[31] https://www.ibia.org/download/datasets/5717/IBIA%20Privacy%20Policy%20Principles%20FINAL.pdf

[32] https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

International Business Machines Corporation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

600 14th St. NW, Suite 300
Washington, D.C. 20005

January 14, 2022

Executive Office of the President
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Subject: OSTP RFI, Docket No. 2021-21975, RE: "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies"

Dear Director Lander:

On behalf of International Business Machines Corporation (IBM), we welcome the opportunity to respond to the Office of Science and Technology Policy's (OSTP) request for information (RFI) regarding "Public and Private Sector Uses of Biometric Technologies" (hereafter, "biometrics RFI").

Although IBM no longer offers general purpose facial recognition technology (FRT), we believe it is important for policymakers to embrace a balanced, precision regulation approach to managing the risks associated with new technologies. We are offering these comments in that spirit. In particular, this submission aims to (1) improve some of the proposed definitional language, (2) provide insights from our own internal governance mechanisms aimed at promoting trust in technology, and (3) offer reasonable policy recommendations to address potential risks of deployed FRT systems.

IBM commends OSTP for its work on this timely and important topic. We thank you in advance for considering these comments and welcome the opportunity to engage with the agency as it moves forward in this process.

Respectfully,

Christina Montgomery
Chief Privacy Officer
IBM Corporation

IBM Response to the "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies"

IBM appreciates the opportunity to respond to OSTP's biometrics RFI. As a company with a long history bringing technological innovations to market, we recognize the importance of taking a considered approach to the introduction of new technologies into society.

As our Chairman and CEO, Arvind Krishna, noted in a June 2020 letter to Congress, IBM no longer offers general purpose facial recognition technology or analysis software, and we oppose its use as a tool for mass surveillance, racial profiling, and other violations of basic human rights and freedoms.[1] Nonetheless, we do have a number of definitional, governance, and policy recommendations for OSTP to consider as part of this biometrics RFI.

Definitions

IBM concurs with the biometrics RFI's definition of "biometric information" as "any measurements or derived data of an individual's physical (*e.g.,* DNA, fingerprints, face or retina scans) and behavioral (*e.g.,* gestures, gait, voice) characteristics." However, we believe it is important to distinguish between the different uses of biometric technologies for "recognition" purposes, as the implications can be fundamentally different.

As defined in the biometrics RFI, "recognition" is used to refer to *both* "verification" and "identification." Given the implication of these applications are substantially different, OSTP should break out these concepts into separate categorical distinctions. For example, FRT systems, while broadly referencing these types of "recognition" features, can be more accurately broken down into the following three categories based on applications and use-cases:

- *Face Detection* – systems capable of detecting and distinguishing one object from another.

[1] IBM CEO's Letter to Congress on Racial Justice Reform, 8 Jun. 2020, available at https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/.

- *Facial Authentication* – systems capable of comparing and validating the features of, e.g., a face image with those stored in a single, previously-stored profile (also commonly referred to as "1-to-1" matching).
- *Facial Matching* – systems capable of comparing and validating the features of, e.g., a face using features of a face image to those stored in a larger database of other images (also commonly referred to as "1-to-many" or "1-to-n" matching).

Given the clear distinctions in particular applications of biometric verification and authentication systems, we believe a more appropriate delineation here would be to strike the use of "recognition" as a header definition and instead define "verification" and "identification" as separate and distinct categories. This would help alleviate confusion regarding the differences in both intended uses and possible implications of these different applications. This distinction is an important feature of biometric technologies that OSTP should emphasize in its work deliverables from this RFI process. In this context, it will also be important for the agency to clearly delineate between identifiable versus non-identifiable biometric information (or anonymized versus personally-identifiable biometric information) usages.

Governance Programs

Any new technology presents both benefits and challenges. To effectively maximize the former while mitigating the latter, it is imperative that companies deploying those technologies take their social responsibilities seriously. The best way to manage those responsibilities is for responsible corporate actors to embrace internal governance processes and structures that ensure in-house stakeholders are accountable to the company's principles and values.

To that end, IBM has built an internal AI Ethics Board that is charged with ensuring we hold ourselves accountable to our corporate values, and the promises we make to society to deploy trustworthy AI systems. The AI Ethics Board is a centralized body composed of a cross-disciplinary team of professionals that aims to foster a culture of ethical, responsible, and trustworthy technology development and implementation. Its responsibilities include providing a centralized governance mechanism for reviewing and issuing decisions regarding our technology ethics policies, practices, communications, research, products, and services.

To assist in the effectuation of its mission, the Ethics Board is composed of both senior level executives with clear decision-making authority, as well as a broad network of AI "focals" – individuals representing the many divisions and

stakeholders within IBM, from human resources, government and regulatory affairs and research to business units – who help to facilitate internal AI ethics education, contribute to the development of internal best practices, and provide feedback and guidance to the board.

Internal governance processes like these are one important feature of companies operationalizing their responsible stewardship of new technologies. But companies also need to make sure they have other guardrails in place to safely shepherd new technologies into the real world. As a further example of IBM putting our values into practice, last year we shared publicly a set of specific, actionable guardrails informing whether and how we would develop new technologies to help address the challenges presented by COVID-19. These include:

- Requiring **data transparency** around collected information, how the information will be used, and who has access to it;
- Restricting the **specific purpose** for which data can be used;
- Prioritizing **data minimization** practices;
- Designing and deploying solutions with **privacy and security built-in**;
- Requiring **humans-in-the-loop** for any decision-making process that would have legal impacts on an individual; and
- Ensuring all applications of our technological solutions are **lawful, fair, inclusive, and non-discriminatory**.[2]

These same governance mechanisms and guardrails can – and should – also be applied to the development, use, and deployment of biometric technologies.

Policy Recommendations

In November 2019, the IBM Policy Lab released policy recommendations for how policymakers could help society maximize the benefits of facial recognition technology while mitigating the potential risks of its misuse, without the need to resort to blanket bans.[3] However, many of these recommendations can also be applied to other biometric technologies. Even as this technology continues to advance and improve, these recommendations will remain relevant and evergreen as effective tools for managing the most pressing concerns associated with its deployment.

[2] Christina Montgomery, "Using Data Responsibly to Tackle a Global Emergency," 18 June 2020, available at https://www.ibm.com/blogs/policy/using-data-responsibly-to-tackle-a-global-emergency/.
[3] Christina Montgomery and Ryan Hagemann, "Precision Regulation and Facial Recognition Technology," 5 Nov. 2019, available at https://www.ibm.com/policy/facial-recognition/.

- **Require organizations to notify and obtain an individual's consent prior to using biometric information to verify their identity.** How, when, and where obtaining consent occurs will look different based on the context in which biometric technologies are deployed. However, in most cases the responsibility for acquiring that consent and providing the relevant notice will ultimately rest with the organization that is deploying the technology.
- **Regulate the export of biometric technologies, such as FRT, by including them on the Department of Commerce's "dual use" control list.** The Commerce Control List (CCL) aggregates those "dual use" products that could be used for either commercial or military applications. This list is then used to inform decisions regarding how tightly to control, or whether to prohibit, the export of sensitive technologies to particular countries based on the intended use-case. Given the CCL already includes other biometric technologies, such as fingerprint and voice print identification and analysis scanners, the Department of Commerce should similarly include FRT on this list – in particular, FRT capable of "1-to-many" matching – to prevent bad actors from using these technologies in a way that would violate basic human rights.
- **Establish disclosure and human-in-the-loop requirements for law enforcement use of biometric information used for identification purposes.** Although there can be reasonable law enforcement use cases for biometric systems, there is also a clear need to balance the needs of public safety institutions with privacy and civil liberties. To aid in promoting greater trust and acceptance of this technology, law enforcement agencies should be required to disclose its use in regularly published reports submitted to the Department of Justice or state attorneys general. Additionally, law enforcement agencies should require human involvement and validation at multiple points in any investigative process making use of biometric information to ensure meaningful context and appropriate safeguards are provided.

Conclusion

IBM commends OSTP for its work on this timely and important topic. We thank you for considering these comments and welcome the opportunity to engage with the agency as it moves forward in this process.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

International Committee of the Red Cross

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

ICRC response to White House Office of Science and Technology Policy Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

January 2022

Prepared by

Laura Walker McDonald, Senior Advisor, Digital Technology and Data Protection
International Committee of the Red Cross (ICRC) Regional Delegation for the United States and Canada

Descriptions of use of biometric information for recognition and inference

Many humanitarian organisations have experimented with the use of biometric identification in recent years.[1] This development is the subject of much debate[2]; but is in part the result of increasing pressures to improve the accuracy and cost-effectiveness of aid delivery, and to know more about recipients of aid.

The ICRC is committed to working at the cutting edge of technology, where doing so enables the organisation to better conduct its activities, and help people affected by conflict. The ICRC has long been using biometrics in limited use cases, for example in forensics and the restoration of family links, and by putting fingerprints on the travel documents it issues. The organisation uses DNA profiling to help identify human remains to determine the fate of the missing, and is employing facial recognition technology to help people find their family members.[3]

However, the ICRC's role requires it to also be alert to the potential risks of technology for affected populations. For example, the ICRC has raised concerns relating to the military applications of certain emerging technologies, in particular autonomy,[4] AI and machine learning.[5] The ICRC sees the protection of personal data whose disclosure could put its beneficiaries at risk, or otherwise be used for purposes other than those for which it was collected, as an integral means of preserving its

[1] For overviews, see Nyst et al, 2018. *Biometrics in the humanitarian* sector, Oxford, Oxfam. Available at https://policy-practice.oxfam.org/resources/biometrics-in-the-humanitarian-sector-620454/ Accessed 01/14/2022; or ICRC, 2021, *Digitharium Month #7*, Geneva, Available at https://www.icrc.org/en/digitharium/digitharium-month-7, Accessed 01/14/22

[2] See for example : Reuters, 2019, *Yemen's Houthis 'Yemen's Houthis and WFP dispute aid control as millions starve'*, Available at https://www.reuters.com/article/us-yemen-security-wfp/yemens-houthis-and-wfp-dispute-aid-control-as-millions-starve-idUSKCN1T51YO, Accessed 01/14/2022; The New Humanitarian, 2019, *Head to Head: Biometrics and Aid*, Available at https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid, Accessed 01/14/2022; Radio Free Asia, 2018, available at *'Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps*', accessed 01/14/22

[3] Hayes, B. & Marelli, M. 2019, *Reflecting on the International Committee of the Red Cross's Biometric Policy : Minimizing Centralized* Databases, AI Now Institute, Available at https://ainowinstitute.org/regulatingbiometrics-hayes-marelli.pdf, accessed 01/14/22

[4] ICRC (2021), *ICRC position on autonomous weapon systems*, Geneva, Available at https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems, accessed 01/14/22

[5] ICRC (2021), *ICRC Position Paper: Artificial intelligence and machine learning in armed conflict: A human-centered approach*, Geneva, available at https://international-review.icrc.org/articles/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-913, accessed 01/14/22

neutrality, impartiality, and independence, as well as the exclusively humanitarian nature of its work. The organisation has sought to highlight data protection challenges in humanitarian action through its Data Protection Framework[6] and 'Digitharium' public events series.[7] As such, the ICRC has set limits on the uses and management of biometric data – for example, not retaining fingerprint information in any database – and has published a Biometrics Policy.[8]

Within those limits, ICRC is exploring the potential to expand its use of biometrics in carefully considered ways.

Humanitarian aid organisations like the ICRC are under pressure to provide aid to as many people as possible, in a global context of growing numbers of crises, of increasing severity, and shrinking aid budgets. Humanitarian needs often surpass available resources. If we can ensure that each person receives only their fair share of aid, and that the people who receive aid are the people our programs planned to reach, we are better able to make the best use of our budget and help as many people as possible. In a humanitarian context, this is not an easy challenge: many individuals are unable to prove who they are, or are part of a marginalized group, whose private information is of extreme sensitivity. Often, aid recipients are given a card and a pin code or a password, but these can be forgotten or lost, or stolen and used by another person.

Biometric identification systems in aid programmes could allow us to 'identify' and/or 'deduplicate' aid recipients, to ensure that each person receives the right kind and amount of aid, without requiring them to have or show other forms of identification. See page 7 below for more information about the research and development we are conducting.

Exhibited and potential harms of a particular biometric technology:

Biometric data is extraordinarily powerful. It creates a permanently identifiable record of an individual – an individual cannot renew or change their biometric identifiers. It is also over purposed by nature: a rich set of data points which is more than what is required for authentication[9].

"Function creep"

Every biometric sample can reveal a lot about the data subject – for example, an iris scan can reveal some health conditions, and facial or voice recognition may reveal ethnicity, age or gender. This kind of 'function creep' is difficult to prevent at collection, opening up the possibility that the data will ultimately be used in ways that aid recipients do not want, understand or consent to. The data protection principles of purpose limitation and data minimization cannot, therefore, be respected. Such rich and personal information poses a unique risk mitigation challenge, because as technology develops, new capabilities and new purposes might be found for the data. This means that risk analysis and mitigation practices, and ethical and practical policies, need to plan for risks and purposes that have not been identified yet.[10]

---

[6] ICRC (2020), *The ICRC Data Protection Framework*, Geneva, available at https://www.icrc.org/en/document/icrc-data-protection-framework, accessed 01/14/22
[7] ICRC (undated), *Digitharium*, available at https://www.icrc.org/en/digitharium, accessed 01/14/22
[8] ICRC (2019), *The ICRC Biometrics Policy*, Geneva, available at https://www.icrc.org/en/document/icrc-biometrics-policy, accessed 01/14/22
[9] Graf, V. & Sukaitis, J., (2021), *Biometrics in humanitarian action : a delicate balance,* Geneva, Available at https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/, accessed 01/14/22
[10] See for example Oxfam comments during the Digitharium debate on biometrics, linked at note 1 above.

Misidentification: Biometrics are also not infallible, particularly in humanitarian crisis contexts where populations often differ from the test subjects used to develop such technologies. For example, while exploring the potential of facial recognition technologies to aid in reuniting families with their loved ones, the ICRC was confronted with recurring racial, gender and age biases of several facial recognition algorithms, leading to both false negative and false positive results. Families can open a tracing request for a missing person with the ICRC or with a national Red Cross and Red Crescent Society, like the American Red Cross. They provide information about the missing person, including photographs. In this context, facial recognition could enable case workers to more easily identify possible matches across large databases. While none of this process is automated and humanitarian experts are always 'in the loop' to use their judgement about whether or not the match is likely to be correct, one can imagine the distress a wrong match could cause to an already suffering family.

Data retention, transfer and proliferation

Humanitarian organizations are under implicit – and at times, explicit - pressure from donors, which are increasingly demanding "end-to-end auditability", and making more-and-more humanitarian funding contingent on demonstrable anti-fraud and accountability processes, to explore biometrics technology. Though donors usually stop short of explicitly requiring the use of biometrics, such systems appear to offer – and are certainly marketed as – the most attractive means of satisfying multiple humanitarian programming requirements. Biometrics are also playing a central role in the scaling up of cash-transfer programming across the sector, with many financial service providers viewing them as a correspondingly simple way to meet to meet their KYC (Know Your Customer) and other legal 'due diligence' requirements. Both of these modalities imply that some data is retained and/or shared with authorities. Increasingly, humanitarian organizations are complying with this trend.[11]

For the recipients of aid this can be problematic. In various large-scale humanitarian contexts, affected populations have expressed serious concerns about the use of biometrics and potential access to the data by non-humanitarian organisations, particularly for security and migration control.[12] Because biometric data is attractive for these purposes, humanitarian organisations can be requested or required by States to disclose it. They are also vulnerable to cyber-operations by State and non-State actors seeking unauthorized access. In some cases, such as was recently reported in Afghanistan, biometric datasets gathered by non-humanitarian actors could be compromised, handed over or otherwise obtained by non-state armed groups or a new authority during a transition of power. This data could subsequently cause harm to those individuals.[13]

---

[11] For example, see Human Rights Watch (2021), *UN shared Rohingya Data without Informed Consent*, available at https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent, accessed 01/14/22, and related, Holloway, K. and Lough, O. (2021), *Although shocking, the Rohingya biometrics scandal is not surprising and could have been prevented*, ODI, available at https://odi.org/en/insights/although-shocking-the-rohingya-biometrics-scandal-is-not-surprising-and-could-have-been-prevented/, accessed 01/14/22

[12] See, for example, the Reuters article describing protests in Yemen, above at note 2

[13] On Afghanistan biometrics, see Guo, E & Noori, H, (2021), *This is the real story of the Afghan biometric databases abandoned to the Taliban,* in MIT Technology Review, available at https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/, accessed 01/14/22; Jacobsen, K. & Steinacker, K., 2021, *Contingency planning in the digital age: biometric data of Afghans must be reconsidered*, in PRIO Blogs, available at https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/, accessed 01/14/22; Privacy International, 2021, *Afghanistan: What Now After Two Decades of Building Data-Intensive Systems?* Available at https://privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems, accessed 01/14/22

Given the permanent and sensitive nature of the data, and the known challenges for governmental and non-governmental organizations of keeping such data secure over long periods of time, for a donor to require the collection of biometric data runs counter to the do no harm principle. And given that the humanitarian landscape is often confusing for communities and recipients of aid, the collection and subsequent handover of such sensitive data by one humanitarian actor can have knock-on effects for trust and humanitarian access for all actors, however principled their action.

Conclusion – Data Protection and Limited Collection: All actors, including States, must consider the eventualities outlined above in exploring and implementing biometrics technologies and develop comprehensive contingency plans, including for remotely removing or destroying the data at short notice. The best way to defend such sensitive data, however, may be not to collect it in the first place. The ICRC recommends limiting collection of biometric data to that which is strictly necessary, and implementing procedures for data subjects to be able to request removal from the database and measures to protect data subjects whose biometrics have been compromised. The ICRC Policy is available to other actors to use as a resource and a template.

For these reasons, the ICRC has ruled out, for the present, storing biometric data in a centralized location. We are exploring ways to convert biometric data into a second data value that cannot identify individuals, be reverse engineered to reveal the original record or combined with another dataset to reveal a person's identity.

Exhibited and potential benefits of a particular biometric technology:

Biometric identifiers are always with us, in some cases including after death, barring some physical changes due to accidents or, in rare cases, alteration to those traits by choice. They do not require a high degree of literacy to use. As noted above, in a humanitarian emergency, biometrics can be a powerful form of personal identification, not requiring government-issued documentation. This makes it more inclusive, and can reduce risk by allowing individuals to be identifiable as their physical selves, and not linked to an administrative record – so, done well, they can protect privacy in cases where biographic data is extremely sensitive. Some biometric traits, such as palm and finger veins, may not be machine-readable from a distance, preventing some unwanted scanning.

For authentication purposes, biometrics may be one of the only mechanisms that guarantees that the bearer of the credential is the one who was given the credential (e.g. unlike pin or password which can be used by somebody else).

Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case:

Legal and regulatory basis for use of biometrics, and the ICRC biometrics policy

Biometric data are recognised as sensitive in both law and practice.[14] The *EU's General Data Protection Regulation (GDPR)* – which has galvanised jurisdictions across the world into adopting, revising, proposing or considering their own data protection laws – designates biometrics as "special

[14] This section draws heavily on Hayes & Marelli, Facilitating innovation, ensuring protection: the ICRC Biometrics Policy, in *Humanitarian Law & Policy,* ICRC, available at https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/, accessed 1/9/22.

category" data, bringing higher thresholds for both collection and protection of the data.[15] The African Union *Convention* on Cybersecurity and Personal Data Protection,[16] the "modernised" Council of Europe *Convention* on the Automatic Processing of Personal Data,[17] and many national privacy laws also contain special rules restricting the processing of biometric data. Although these rules do not apply to the ICRC, which has adopted a Data Protection Framework that reflect its status as an international organisation, the core principles upon which they are based are the same.[18] In its Handbook on Data Protection in Humanitarian Action, and through its Biometrics Policy,[19] the ICRC fully recognizes the risks introduced by the collection and processing of biometrics data. We strongly believe that protecting data is really about protecting people and if a biometrics-based identification system is designed and deployed without properly applying the fundamental principles of data protection - such as minimizing data collection and retention, purpose limitation, and privacy by design - the risks will outweigh the benefits.

The ICRC Biometrics Policy, adopted by the ICRC Assembly in August 2019, was elaborated over an 18-month period and is the result of extensive research, analysis, consultation and reflection. This process included a review of all situations and scenarios in which the ICRC is processing or considering the use of biometrics, an evaluation of the "legitimate basis" and specific purposes for the processing, and the identification of organisational, technical and legal safeguards.

Establishing a legitimate basis is straightforward where the ICRC processes biometric data in accordance with specific objectives associated with its mandate – for example to identify individuals in its work on Restoring Family Links and determining the fate or whereabouts of the missing – and where particular objectives cannot be realised without using biometrics. In this case the ICRC processes the biometric data as a matter of "public interest" (in the implementation of the ICRC's mandate).

The issue is much more challenging when it comes to using biometrics for beneficiary management and aid distribution, where the processing of the data may not be viewed as an integral part of an ICRC mandate-based activity requiring the identification of individuals. Because the purpose here is primarily linked to efficiency, and insofar as aid can be (and long has been) distributed without the need for biometrics, the ICRC would have to establish that the "legitimate interest" it has in establishing any biometric identity management system does not outweigh the potential impact on the rights and freedoms of the individuals concerned. This balancing test is typical in data protection law whenever a data controller relies on their own interests as a basis for processing.

Token-based systems – a balance?

In its analysis the ICRC found that there was, however, a balance that could be found that would still allow the institution to leverage the advantages that biometric authentication offers in respect to efficiency and effectiveness and ensuring end-to-end accountability in its aid distributions, while minimizing the risks to which its beneficiaries would be exposed.

---

[15] Dentons, 2020, *GDPR Update – Biometric Data*, available at https://www.dentons.com/en/insights/alerts/2020/december/22/gdpr-update-biometric-data, accessed 01/14/22

[16] African Union, 2014, *African Union Convention on Cyber Security and Personal Data Protection,* available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection, accessed 01/14/22

[17] Council of Europe, 2018, *Convention 108+: the modernized version of a landmark instrument*, available at https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108, accessed 01/14/22

[18] See above at note 6

[19] See above at note 8

This balance rests on operations wishing to use biometric data in the registration and verification of beneficiaries limiting the processing to a token-based system. In practice this means that beneficiaries may be issued with, for example, a card on which their biometric data is securely stored, but that the ICRC will not collect, retain or further process their biometric data (and will not therefore establish a biometric database).

The token/card may be used to verify beneficiaries during aid distributions to ensure that the aid reaches those individuals for whom it has been earmarked, but no other use of the biometric data will be possible. If the beneficiary wants to withdraw or delete their biometric data, all they will need do is return or destroy the card. If authorities seek to compel humanitarian organisations in a particular country to hand over the biometric data of beneficiaries, the ICRC will not face such pressure because it will not in fact have this type of data. This solution allows the ICRC to leverage the benefits of biometrics for the purposes of authentication, but not for deduplication, because we can never review our databases for duplicate biometric records.

The organisation continues to participate in research and policy discussions to help drive innovation and industry standards. At present, standards around system interoperability to prevent vendor lock-in, or accountability for performance, are lacking. The revised ISO standard 24745 on 'Biometric Information Protection', due to be published in early 2022, will be a step in the right direction, as would national and supranational regulation like those under discussion for artificial intelligence.

The role of consent

While the ICRC is committed to rendering its data processing as transparent as possible to aid recipients and affected populations, it does not believe that consent provides a legally valid basis for data processing in many emergency situations.

This is because consent to data processing cannot be regarded as valid if the individual has no real choice: for example, where the provision of aid is effectively dependent on the provision of personal information, and consent is therefore unlikely to be "freely given". In addition, the power imbalance and situation of the beneficiary means that there is no real "choice", and the individual is induced to accept what is proposed by a humanitarian organisation. Moreover, where biometrics are concerned, it is extremely difficult to ensure that consent is genuinely "informed", since in many situations the affected population may not be able to fully comprehend the technology, information flows, risks or benefits that underpin the processing of their biometric data.

The Biometrics Policy, in line with the ICRC Rules on Personal Data Protection, requires the ICRC to explain the basis and purpose of data processing to its beneficiaries, including any data-sharing arrangements, regardless of the basis for the processing. The ICRC also seeks to ensure that beneficiaries have the opportunity to ask questions and object to data processing if they so wish, particularly where data may be shared with third parties. If people do not want to provide their biometric or other personal data, or to see their information shared for humanitarian purposes with partners, the ICRC will respect their wishes.

No data sharing for non-humanitarian purposes

The Policy also makes it clear that the ICRC will only use biometric data where it enhances the capacity of the organisation to implement its humanitarian mandate and will under no circumstances share biometric data with third parties, including authorities, that may use them for non-humanitarian purposes. Even where exclusively humanitarian grounds for sharing biometric data can be identified, strict conditions must still be satisfied before the data can be transferred by the ICRC.

The Future, Research and Development

Further to that, the ICRC is committed to the advance of research in the domain of "secure biometrics". In practice, raw biometrics samples (images) are processed before they can be used for authentication. This process of extracting the "features" generate a binary version of the biometric trait which is called a *biometric template*. It is only in this format that a search for matches can be performed, and this often involves a probabilistic comparison (e.g. "the match is 99.3%"). These templates are still very sensitive and personal data and various attacks can be performed against them. For instance, templates can be reversed to reveal the raw biometrics, or templates in two different systems are so similar that they reveal they are linked to the same individual. Last but not least, many systems use templates that are as unique and permanent as the raw biometrics meaning that they cannot be revoked and renewed if compromised.

These *biometrics templates* must be protected and there are several research approaches like *biometrics crypto systems* (i.e. where the biometrics is used as the cryptographic key) or *cancellable biometrics.* Unfortunately, very few commercial actors are actively investing in them and we intend to launch partnerships projects in this area,

About the ICRC

The International Committee of the Red Cross (ICRC) is an impartial, neutral, and independent humanitarian organization working to save lives and protect people in hotspots around the globe. We work with Red Cross and Red Crescent Societies worldwide to deliver relief and protect people from armed conflict and violence. The ICRC is independent from the UN system.

Our work is strictly humanitarian: to assist and protect people affected by armed conflict and violence, ensuring that their basic needs are met. Respect for the law of armed conflict saves lives and limits damage to civilian property, which helps prevent displacement.

Established in 1863, we have worked with states, including the US government, for over a century to develop and apply the law of armed conflict – rules that protect soldiers, civilians, detainees, and the wounded and sick in war.

Find out more about the ICRC at icrc.org.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Inventionphysics

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] method of pattern recognition for artificial intelligence
Date: Wednesday, January 26, 2022 9:47:26 PM
Attachments: 0.pdf

OSTP:

I am respectfully soliciting OSTP to evaluate the method of pattern recognition for artificial intelligence (patent no. 8,880,453) which is described in the accompanying attachment for its respective interests. I propose, for example, that one can use arrays of interconnected exclusive-nor logic gates to store and retrieve patterns of information (e.g., biomarkers for detecting cancer or patterns of information for actuating or controlling a system) instead of neural nets. Wherein, one could eliminate the training, the uncertainty, the mathematical rigor, and the overall programming complexities which can accompany the use of deep neural networks for such a purpose.

Thanks,

Steve Snyder

Company: Inventionphysics, LLC

Address: [redacted]

[redacted]

Phone: [redacted]

Website: >www.inventionphysics.com<

To contact or opt-out email: [redacted]

US008880453B2

(12) **United States Patent**
Snyder

(10) **Patent No.: US 8,880,453 B2**
(45) **Date of Patent: Nov. 4, 2014**

(54) **METHOD OF PATTERN RECOGNITION FOR ARTIFICIAL INTELLIGENCE**

(76) Inventor: **Steven Howard Snyder**, Southfield, MI (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 175 days.

(21) Appl. No.: **13/563,843**

(22) Filed: **Aug. 1, 2012**

(65) **Prior Publication Data**

US 2013/0054504 A1 Feb. 28, 2013

Related U.S. Application Data

(60) Provisional application No. 61/528,413, filed on Aug. 29, 2011.

(51) **Int. Cl.**

G06F 17/00	(2006.01)
G06N 5/02	(2006.01)
G06K 9/00	(2006.01)
G06F 7/60	(2006.01)
G06F 7/02	(2006.01)
G06F 7/501	(2006.01)

(52) **U.S. Cl.**

CPC ***G06F 7/02*** (2013.01); ***G06K 9/00986*** (2013.01); ***G06F 7/607*** (2013.01); *G06F 7/5013* (2013.01)

USPC **706/46**

(58) **Field of Classification Search**

USPC 706/46

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2008/0185919	A1*	8/2008	Snyder	307/149
2013/0054504	A1*	2/2013	Snyder	706/46
2013/0146789	A1*	6/2013	Snyder	250/492.1

* cited by examiner

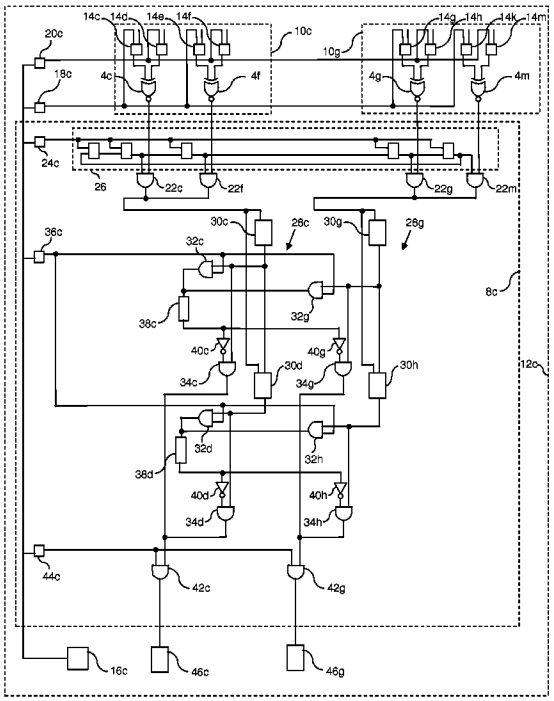
Primary Examiner — Michael B Holmes

(57) **ABSTRACT**

Invention for pattern recognition and artificial intelligence comprising:

1) storing data in parallel by applying a logic level (1) input or a logic level (0) input to one input of each of at least two exclusive-nor logic gates;
2) comparing data in parallel by applying a logic level (1) input or a logic level (0) input to the other input of each of the exclusive-nor gates, wherein each exclusive-nor gate produces a logic level (1) output when both inputs have the same datum input, and each exclusive-nor gate produces a logic level (0) output when both inputs have different datum input; and
3) measuring the outputs of the exclusive-nor logic gates collectively with a measuring apparatus, wherein the percentage of the pattern input for comparison which matches the pattern of data stored in the exclusive-nor gates is directly proportional to the magnitude of the collective output of the exclusive-nor gates.

1 Claim, 11 Drawing Sheets



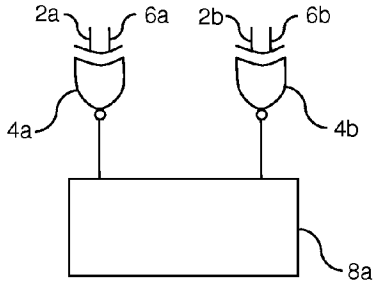


FIG. 1a

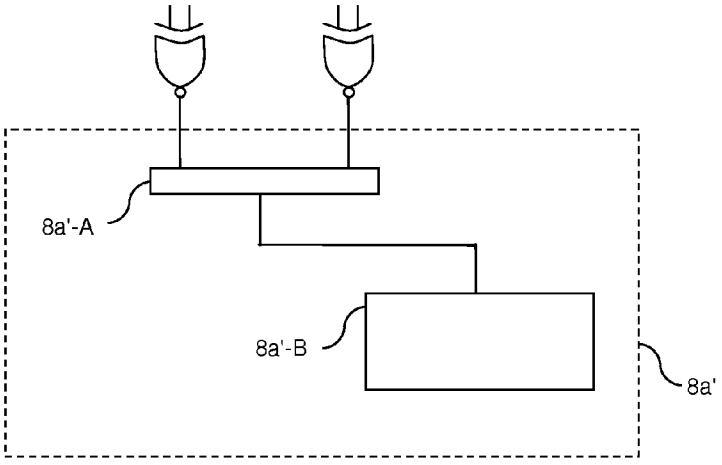


FIG. 1b

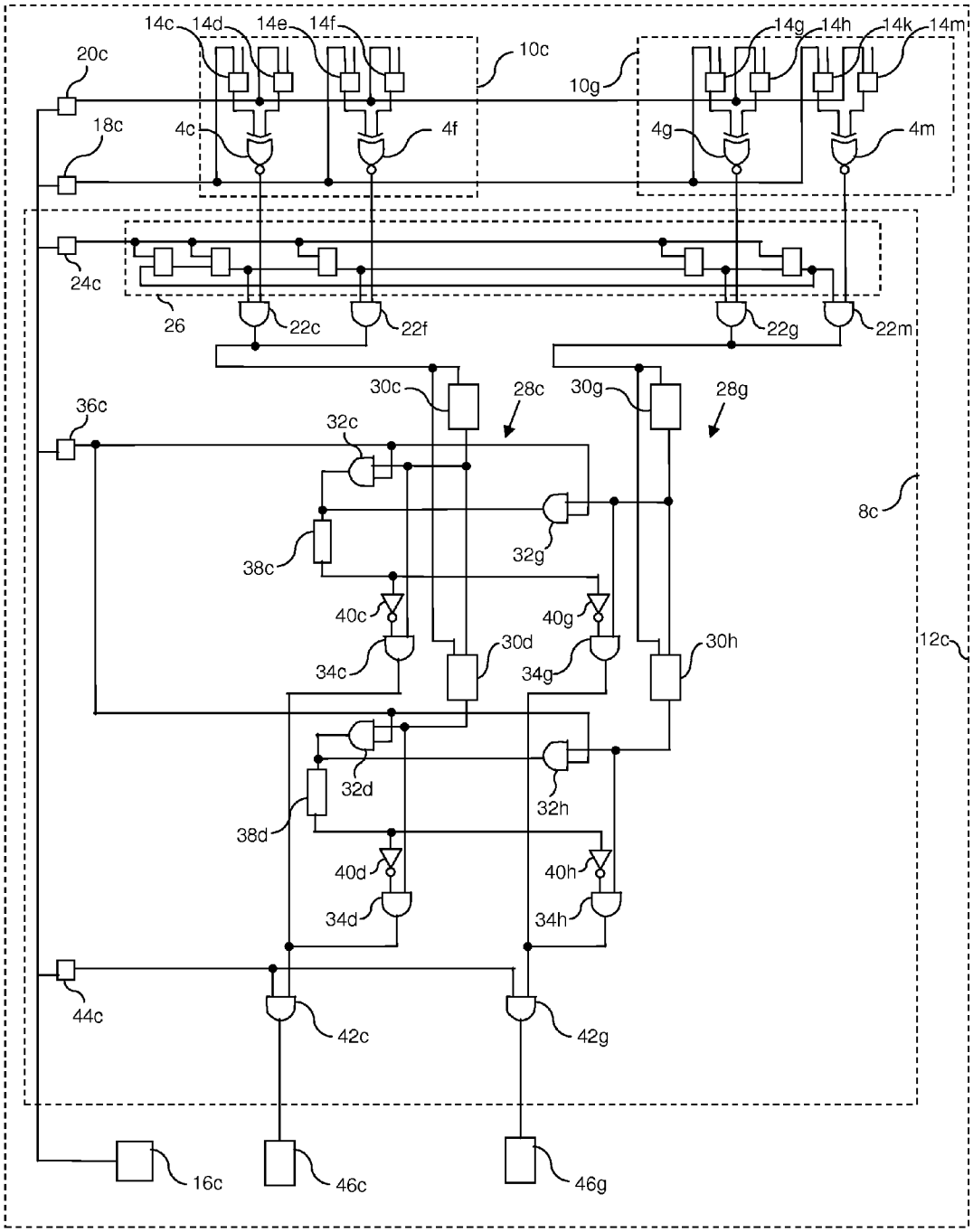

14c
14d
14e
14f
14g
14h
14k
14m
20c
10c
10g
18c
4c
4f
4g
4m
24c
26
22c
22f
22g
22m
30c
28c
30g
28g
36c
32c
8c
32g
38c
40c
40g
12c
30d
30h
34c
34g
32d
32h
38d
40d
40h
34d
34h
44c
42c
42g
16c
46c
46g

FIG. 2a

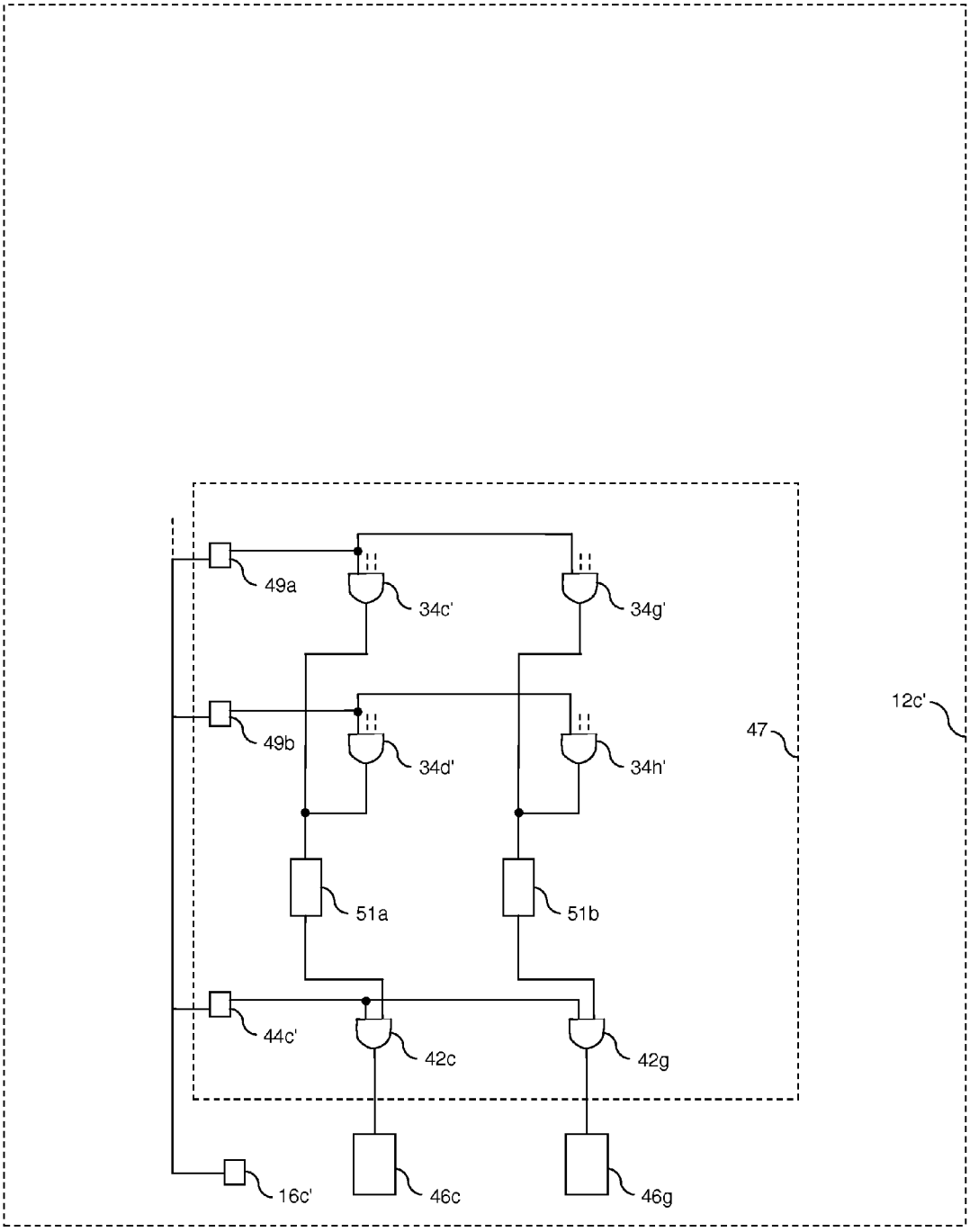


FIG. 2a'

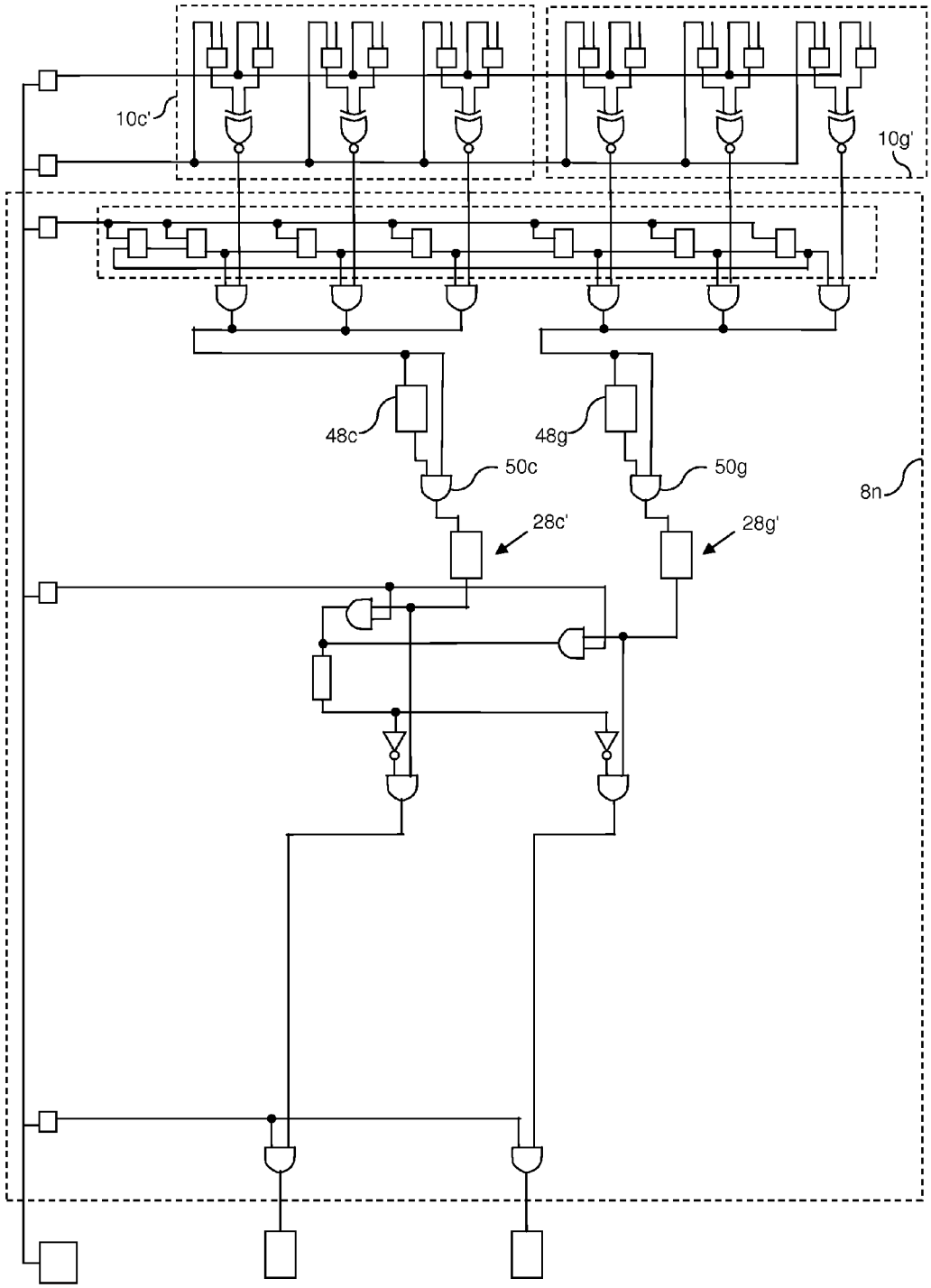


FIG. 2b

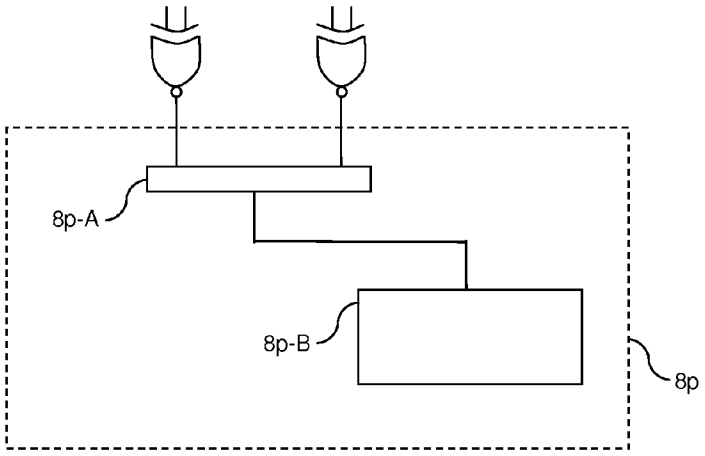


FIG. 2c

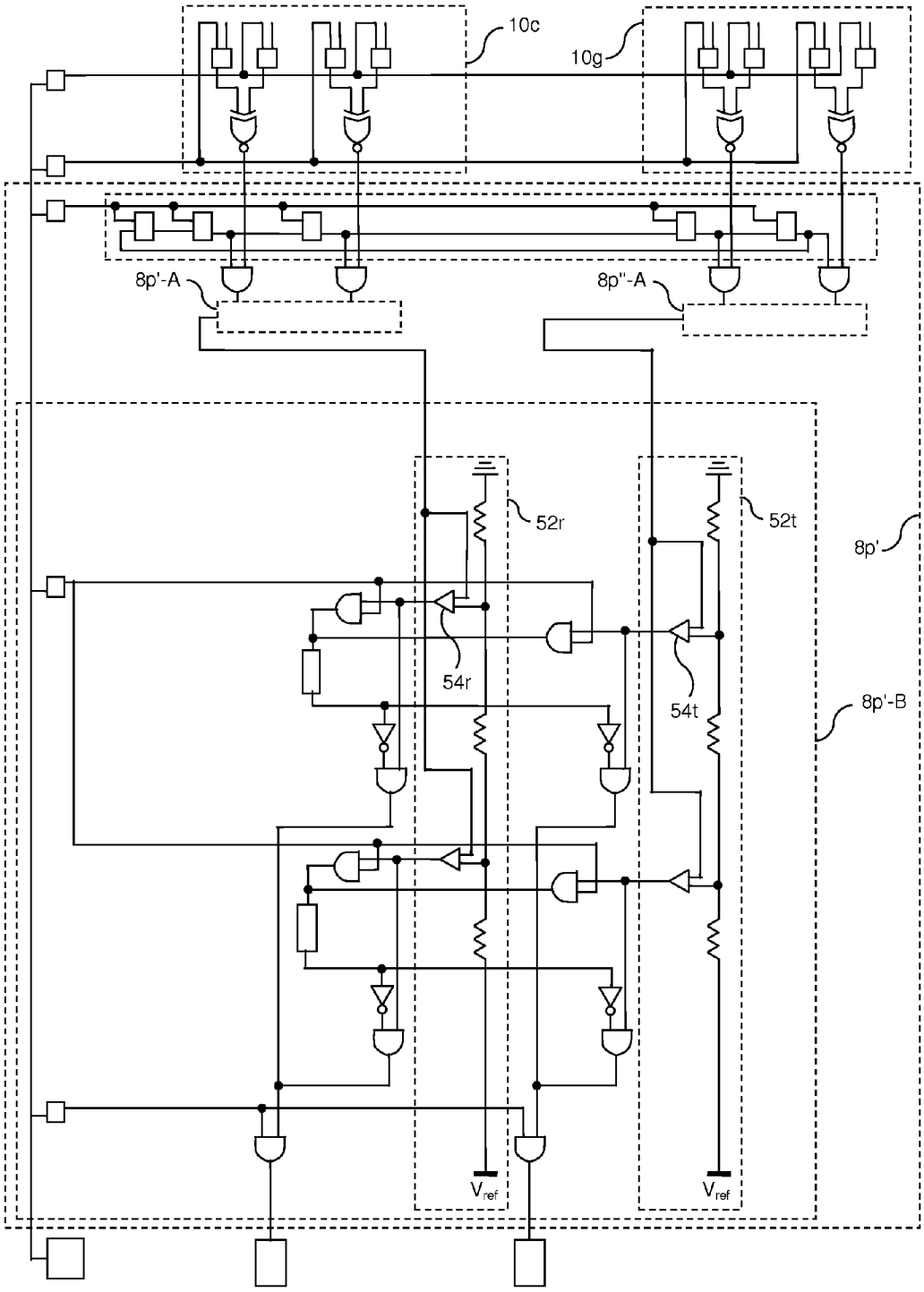


FIG. 2c'

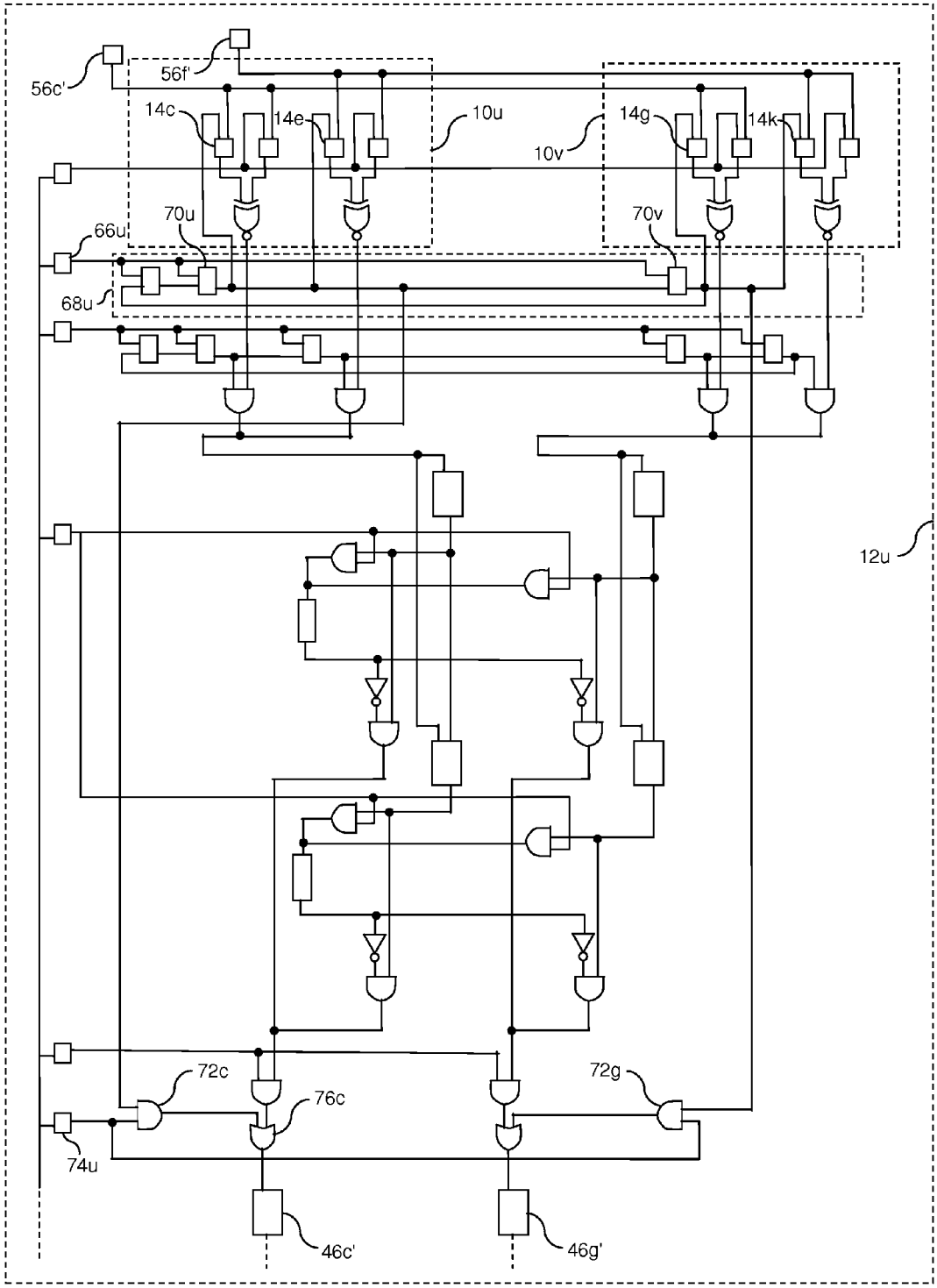

56c'
56f'
14c
14e
10u
10v
14g
14k
70u
70v
66u
68u
12u
72c
76c
72g
74u
46c'
46g'

FIG. 3A

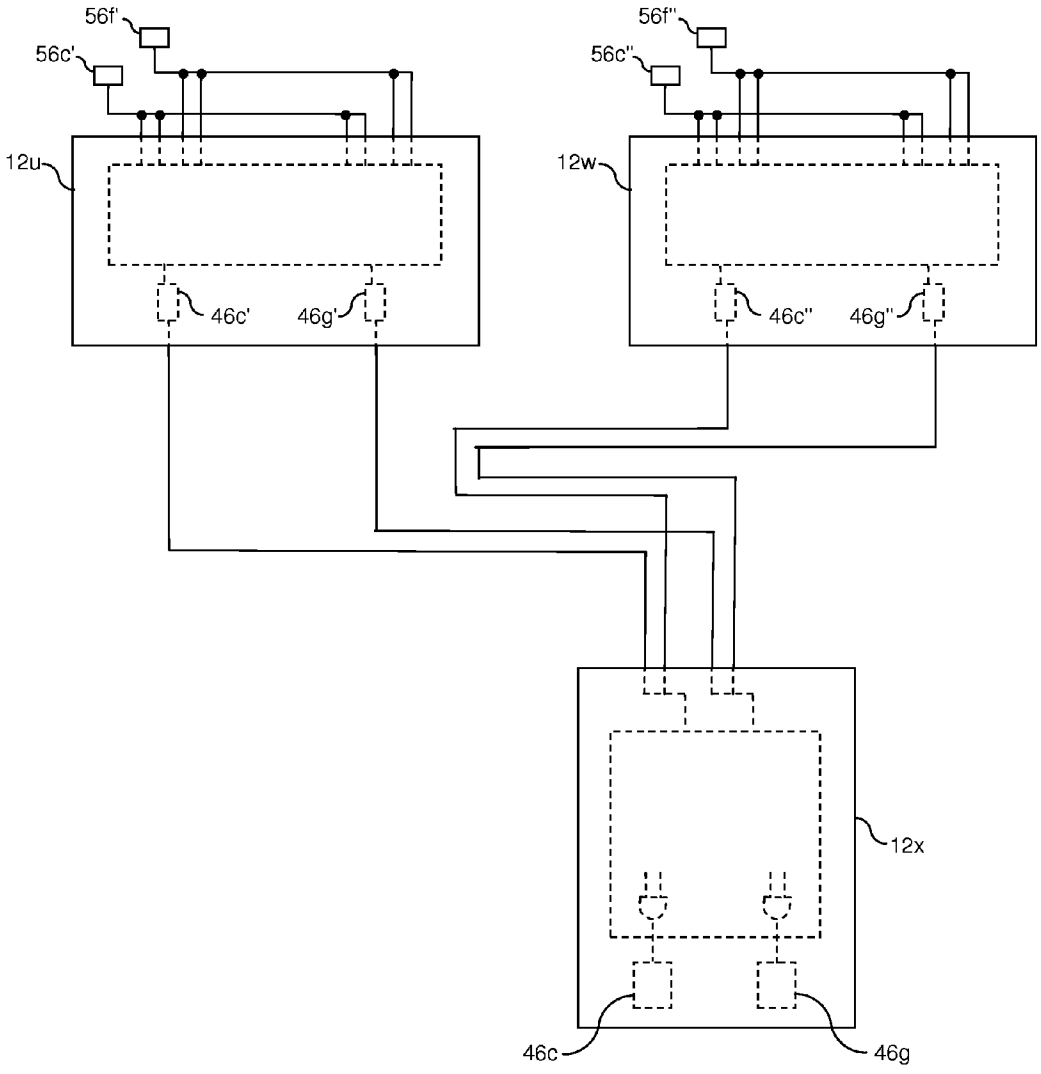


FIG. 3B

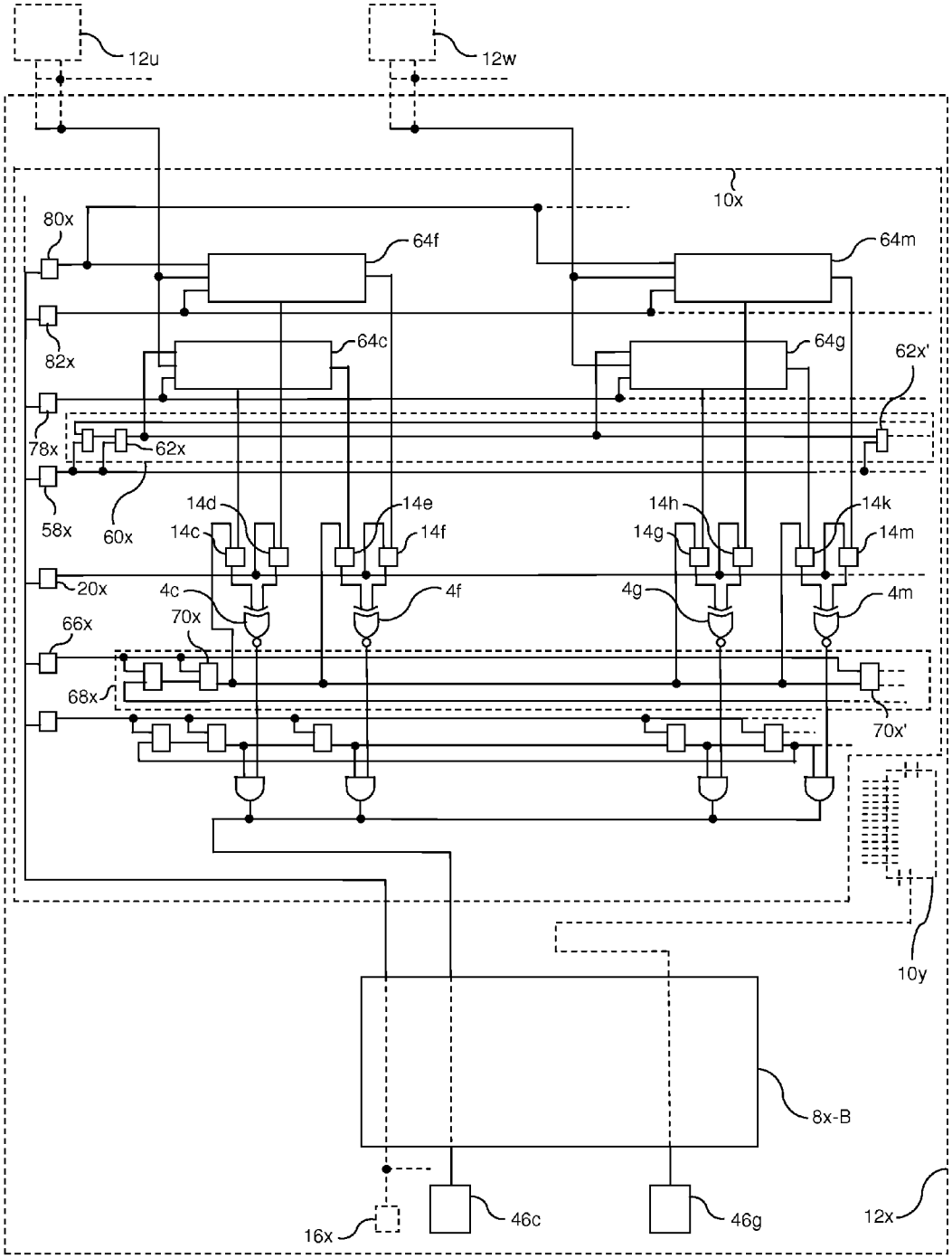

12u
12w
10x
80x
64f
64m
82x
64c
64g
62x'
78x
62x
58x
60x
14d
14e
14h
14k
14c
14f
14g
14m
20x
4c
4f
4g
4m
66x
70x
68x
70x'
10y
8x-B
16x
46c
46g
12x

FIG. 3C

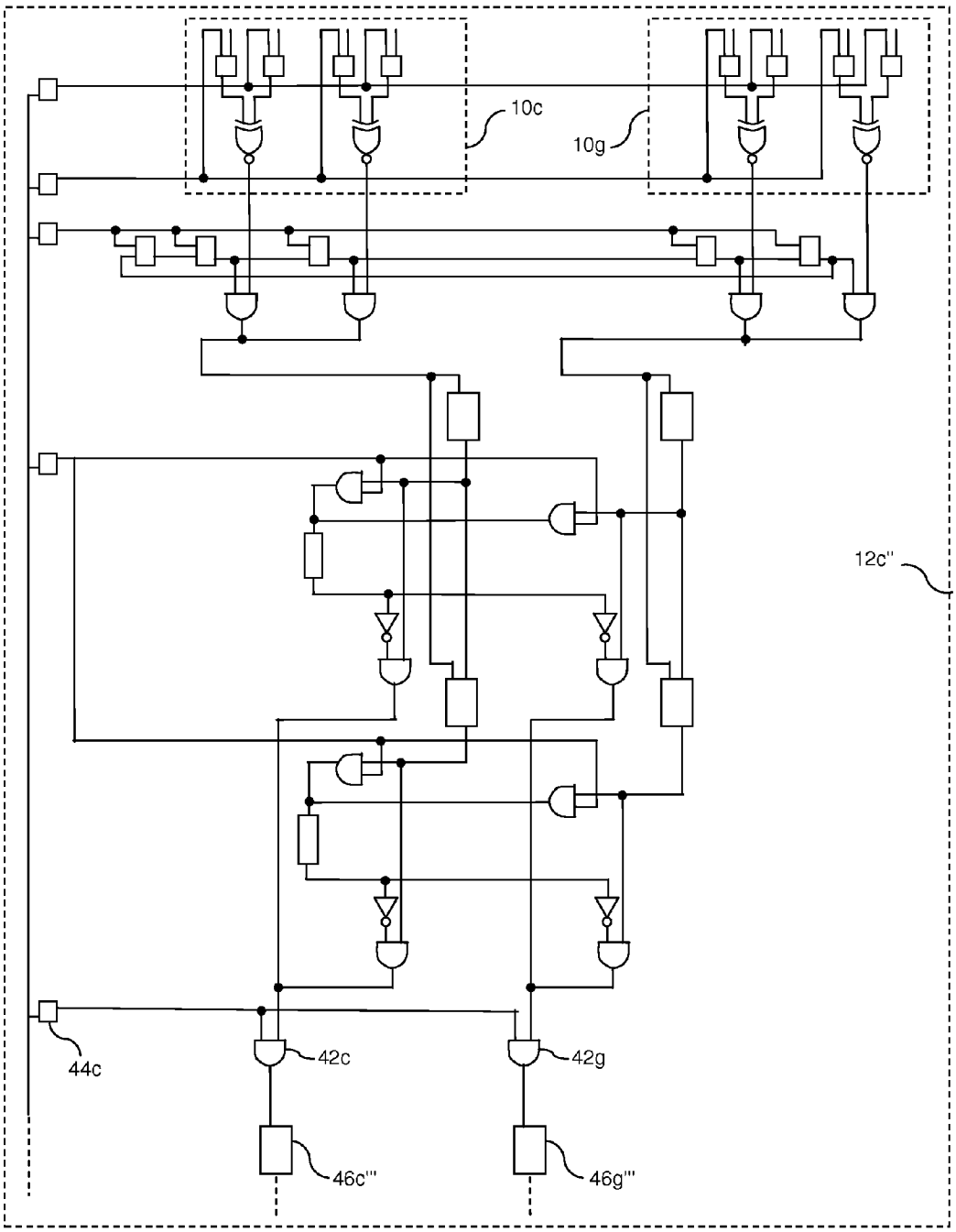


FIG. 4A

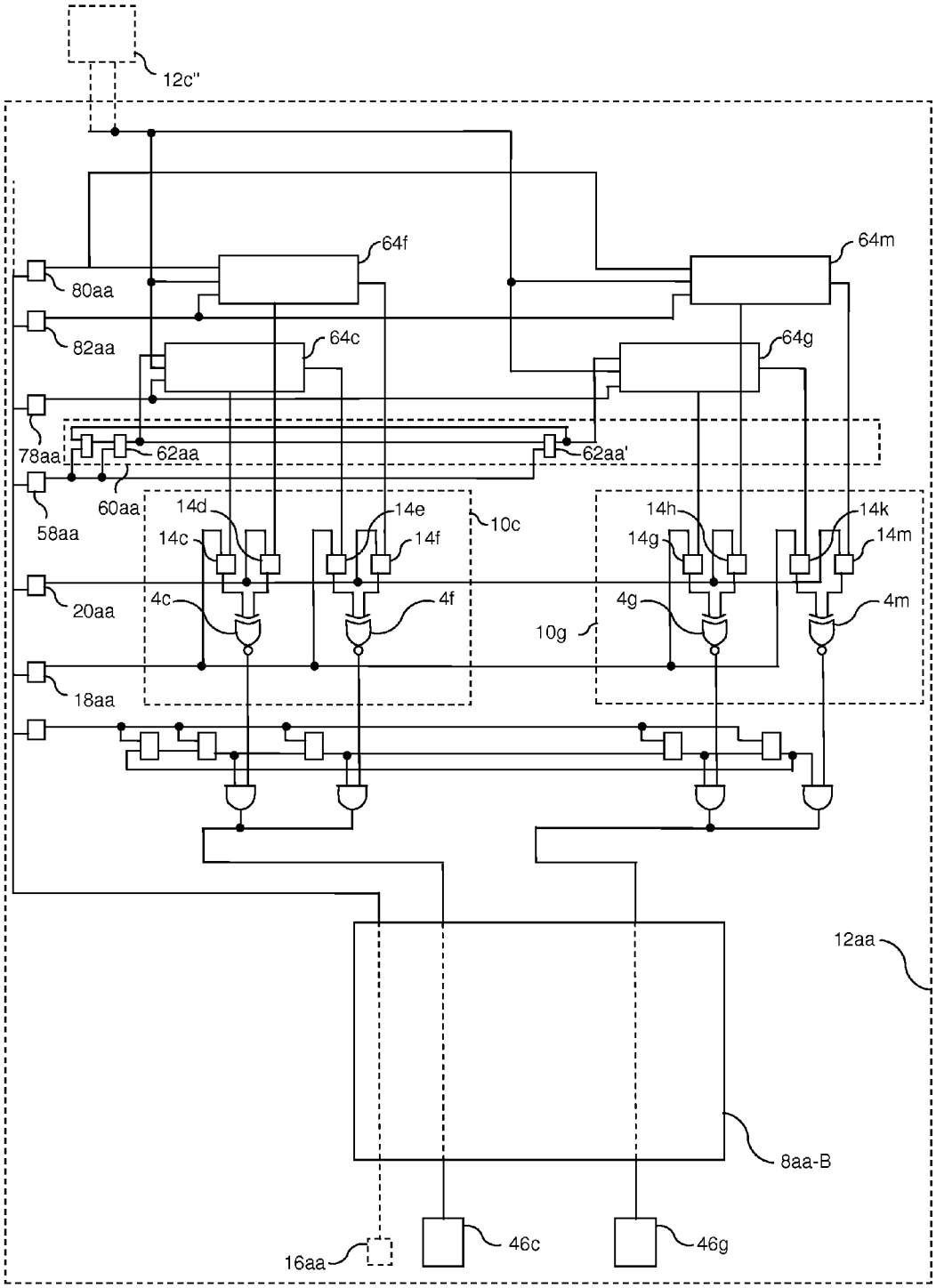

12c''
64f
64m
80aa
82aa
64c
64g
78aa
62aa
62aa'
60aa
58aa
14d
14e
14c
14f
10c
14h
14k
14g
14m
20aa
4c
4f
4g
4m
10g
18aa
12aa
8aa-B
16aa
46c
46g

FIG. 4B

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

iProov

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

iProov Comments in Response to *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies* (2021-21975)

Company Name: iProov
Company Profile: Private sector technical practitioners specializing in Biometric Face Authentication
Contact Person: Joe Palmer
Contact Role: President
Contact Email: [redacted]
URL: www.iproov.com

1. Descriptions of use of biometric information for recognition and inference

The most difficult problem in online identity verification is the establishment of trust. When the whole process is remote, without any human intervention, how do you bind an actual physical person to their digital identity?

Almost always the user is unknown, operating from different locations, via untrusted hardware, running over unsecured networks. Under these hostile conditions, the task is to establish trust (that they are who they say they are) without inconveniencing the remote user/citizen.

To be able to trust a person in a digital channel, an organization needs to assure the identity of the individual remotely. This can be achieved by verifying the individual's details against a government-issued photo identity document such as a passport, identity card, drivers license, or centralized database. The common biometric which is available on all of these trusted documents is the face, making it the best option for a biometric authentication solution.

In a pre-digital era, individuals needed to go into a branch or office to prove that they were the genuine holders of their photo ID document. This approach is costly, inefficient and does not provide a positive customer experience to a population that is used to the convenience and ease of a digital world. Since COVID-19, the drive to digital channels has accelerated dramatically. Organizations have had to quickly respond to consumer demand and provide highly inclusive, barrier-free and secure digital experiences which can be delivered irrespective of the chosen device or platform or, the users' age or ability. The move to digital channels has also led to the rise of digital crimes such as account takeover, account manipulation and application fraud. These are usually executed by using spoof attacks, which can either be a person masquerading as a legitimate user or through the use of a compromised or synthetic identity.

Face verification is the process by which a remote individual presence needs to be confirmed and their identity suitably protected. Unlike facial recognition, face verification delivers direct benefit to the individual, the individual has knowledge and awareness that it is taking place and the individual's privacy can be protected.

Identity verification methods exist to determine if the presented biometric in front of the device sensor is that of a real person AND from the owner of the asserted identity. In order to confirm that the remote user is a real person and not a 2D photo, "liveness detection" is required in the form of a "challenge - response" mechanism to mimic an in-person interaction. The user is presented with a challenge, which requires them to respond appropriately. The resultant response and insights gained from this interaction process, proves their legitimate existence.

Early approaches to liveness detection that also aimed to combat biometric spoof attacks included motion-based or active authentication processes, eliciting voluntary responses from the user. Active authentication processes are defined in ISO 30107-1 as those which elicit a voluntary response such as a movement, smile or blink. Here the individual is presented with instructions that they are expected to read, understand and execute. Such active authentication systems are no longer secure as they are vulnerable to spoofs which monitor and replicate the required movements. In addition, they are non-inclusive, placing a high-level of effort on the user. This approach has proven to be unpopular, resulting in high user abandonment rates.

iProov Genuine Presence Assurance™ verifies that an online user is the **right** person (not an imposter), is a **real** person (not a presented spoof), and that the authentication is taking place in **real-time** (not a digital injection attack).

Patented Flashmark technology uses controlled illumination to provide a simple and effortless challenge - response experience. Technology does the work; the user only needs to look at their device, which looks back at them, and the authentication is complete. This passive and highly secure solution does not require a voluntary action from the user. It is available on any device with a front-facing camera and is designed to eliminate cognitive load on the user.

The key to Flashmark is that it goes beyond relying on user imagery from the camera, by introducing an unpredictable element which is extremely difficult to forge credibly. A random color sequence is automatically generated by servers, not locally by a device. This makes it extremely difficult for attackers to manipulate, replicate or reverse engineer the authentication process. Light reflection analysis enables iProov to determine the genuine presence of the user and confirm that:

- It is a **real** person: liveness detection identifies whether the imagery is from a live, skin covered, three-dimensional human-face shaped object. Also, that it is not a presentation attack such as a mask or a digital image presented to the device camera. This is achieved through the use of;
    - a short video sequence rather than a still image which provides rich insights into a users' 'liveness'

  - models which have been trained on millions of interactions from different populations from around the world
  - machine learning which identifies the subtle cues and micro movements that the human eye is unable to detect
  - the interaction of light on skin in different lighting conditions. This is difficult to fake accurately and manipulated imagery can be identified by analyzing parts of the face as well as skin and texture
- The user is authenticating **right now**: ensuring that the unique sequence of colors is reflecting in an expected way from the user's face within an expected time frame. This enables iProov to confirm that the user is not a digitally injected recording or synthetic imagery such as a deepfake. These attacks bypass the device camera by being digitally injected into the data stream, manipulating the application to believe that the imagery it is receiving is from the device sensor, or sending manipulated imagery from the application.

iProov's Genuine Presence Assurance technology has been deployed across the globe in both the public and private sectors. A selection of our customers includes:

The U.S. Department of Homeland Security: iProov successfully developed an integrated solution to enable travelers to quickly transit remote border ports using their personal devices to report their entry and exit to Customs and Border Protection (CBP) — without requiring the direct engagement of a CBP Officer in person or online — with a secure, privacy-focused mobile application.

"A critical challenge when delivering digital services that require some manner of identity verification is the need to ensure that the entity being verified is a real live human and not a replica or a recording". "The pandemic has accelerated the need for high-value remote digital service delivery, and iProov has now adapted its technology to provide their anti-spoofing solution to a broad range of applications." — Anil John, Technical Director, Silicon Valley Innovation Program, Department of Homeland Security

The UK's National Health Service (NHS): iProov technology has been deployed to verify users signing up for a NHS login across Android and iOS. This enables users in England to create their NHS login remotely, securely and conveniently at a time when they need it most, removing the need for manual and in-person verifications. The NHS App allows for easy and fast access to essential services such as doctor appointments, access to medical records, and ordering repeat prescriptions.

"Over the past couple of months we have seen a surge in demand in people registering for an NHS login as they look to manage their health digitally." — Melissa Ruscoe, Programme Head for NHS Login

The UK Home Office: The EU Settled Status app has been used by more than five million foreign nationals post-Brexit and was developed in collaboration with partners WorldReach and Read ID.

The technology allows secure identity verification and enrollment onto Home Office services using a smartphone app. The process involves biometric matching of the user's selfie against the image read from a user's passport chip, using iProov's unique Flashmark technology to assure genuine presence.

- Over 85% of applicants chose the digital channel
- 99.97% system availability
- More than 2,515 different makes and models of Android and iOS devices have been used to complete the identity verification process

"Having more than 6 million applications to the scheme is an unprecedented achievement and I am delighted that we have secured the rights of so many EU citizens." — Priti Patel, UK Home Secretary

The Singapore Government: Four million Singaporeans can now access digital government services online using facial verification implemented by iProov and Toppan Ecquaria for the Government Technology Agency of Singapore (GovTech) under the pioneering National Digital Identity (NDI) program. GovTech is the government agency driving Singapore's digital government transformation and Smart Nation initiative.

Cloud facial verification, provided by iProov, has been used to secure national digital identity. For Singapore residents, the ability to register for a bank account or engage with other organizations using the SingPass Face Verification offers a number of benefits. As well as access to a wider range of digital services, the user sees greater convenience, a simplified user experience, and increased privacy and security, as they no longer need to set up passwords or share sensitive data with every individual company. Such improvements in accessibility and online trust will lead to greater uptake of digital services, one of the aims of Singapore's Smart Nation initiative.

- Secure access to over 500 digital services offered by more than 180 government agencies and commercial entities
- Increases accessibility by encouraging Singaporeans, especially older residents with limited mobility, to use online banking and other services
- Improves inclusivity to those without smartphones by extending the service to government kiosks
- Gives private businesses, both large and small, the ability to grow their digital services without needing to build their own infrastructures and biometric database
- Grows the digital economy by encouraging uptake and use of online services, both from government and private businesses.

"Singapore's national digital identity, SingPass, enables citizens and permanent residents to transact seamlessly and securely with public and private sectors' digital services." — Quek Sin Kwok, Senior Director of National Digital Identity, GovTech Singapore

Eurostar: SmartCheck enables passengers to complete secure ticket verification and UK exit check on their mobile devices prior to travel. The biometric face verification, which uses iProov's Genuine Presence Assurance technology, is then linked to their e-ticket, with confirmation sent to the passenger. On arrival at St. Pancras International Station, passengers proceed through a dedicated SmartCheck lane. A brief face scan at the ticket gate verifies that the customer has completed the ticket check, with no sharing of paper or electronic tickets needed. A second face scan at the UK exit check allows Eurostar to verify that the passenger has completed their passport information, again replacing the need for travelers to hand over documentation.

"The brand new contactless travel technology from iProov and Eurostar is a window into the future of border control, of smoother, more seamless and convenient journeys." — Grant Shapps, Transport Secretary

Australian Taxation Office: iProov's Genuine Presence Assurance technology enables Australians to set up their myGovID national digital identity using a simple face scan on their mobile devices. This provides access to a range of services, including managing tax returns, accessing health services and applying for benefits.

For more details of iProov customers visit:
https://www.iproov.com/what-we-do/case-studies

2. Procedures for and results of data-driven and scientific validation of biometric technologies

iBeta and NIST Certification:
iBeta is accredited as a test lab by the National Voluntary Lab Accreditation Program (NVLAP Testing Lab Code 200962) to the requirements of ISO/IEC 17025:2017 (General requirements for the competence of testing and calibration laboratories). In 2011, iBeta was accredited by NIST under theNational Voluntary Laboratory Accreditation Program (NVLAP) for Biometric Testing. iBeta is the only NIST certified testing lab in existence, capable of certifying biometric solutions for liveness detection.

In addition, iBeta procedures against the ISO 30107-3 Presentation Attached Detection (PAD)standard were audited by their accrediting body and iBeta's Scope of Accreditation was increased to include conformance testing to the ISO 30107-3 standard in April 2018. iProov has achieved Level 1 and Level 2 rating in the iBeta (NIST/NVLAP) Presentation Attack Detection (PAD) certification test for GenuinePresence Assurance technology.

iBeta was not able to gain unauthorized access with the PAs yielding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAMPR) of 0%. The bona fide

False Match Rate (FMR) and False Non-Match Rate (FNMR) may be found in the final report.

iBeta GPA Level 1 Confirmation Letter
iBeta GPA Level 2 Confirmation Letter

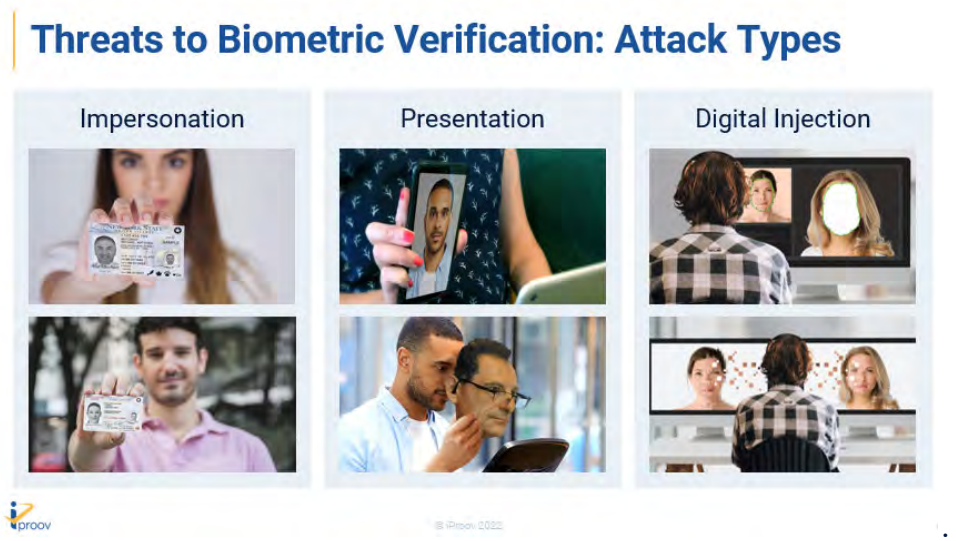
iProov also conforms with ISO/IEC 19795-1:2006 for testing biometric verification performance, audited by the UK National Physical Laboratory (NPL).

ISO/IEC 19795-1:2006 is concerned with the evaluation of biometric systems in terms of error rates and throughput rates. Metrics for the various error rates in biometric enrolment, verification and identification are unambiguously specified. Recommendations and requirements are given for the conduct of performance evaluations through the steps of planning the evaluation; collection of enrollment, verification or identification transaction data; analysis of error rates; and the reporting and presentation of results. The principles presented are generic to the range of biometric modalities, applications, and test purposes, and to both offline and online testing methodologies. These principles help avoid bias due to inappropriate data collection or analytic procedures; give better estimates of field performance for the expended effort; and clarify the limits of applicability of the test results.

Watch the OnDemand webinar: Singapore GovTech shares face verification insights: https://www.iproov.com/blog/singapore-govtech-share-face-verification-insights-on-iproov-webinar

3. Security considerations associated with a particular biometric technology

Biometric authentication can deliver great advantages to citizens, governments and organizations. In order to deliver the highest level of security, it is crucial to understand the potential attacks and the requisite defenses that need to be in place.



Biometric attacks can be segmented into three primary categories:

- **Impersonation Attacks** - Also known as imposter attacks where the wrong face or person is pretending to be someone else. The imposter is a real person, but not the **right** person or legitimate owner of the asserted identity. In modern technology this is a face matching problem, does the authenticating face match the one on the asserted legal photo ID? These are low intensity, low sophistication attacks.
- **Presentation Attacks** - These attacks can be physical static artifacts such as photos or masks, as well as digital artifacts where a recording is presented on a screen to the device camera. Presentation attacks are a very well known attack vector and continue to be used. Advancements in screens and 3D printing capabilities are progressing at pace and it's easier now to create realistic artifact attacks. Many vendors offer liveness detection solutions to mitigate known presentation attacks. The problem here is that the artifact being used is not a **real** person. Presentation attacks are low scale and pose low level risk.
- **Digital Injection Attacks** - Highly scalable attacks which can be created from digital replays or from the use of synthetic imagery which can either bypass the device camera sensors, or be injected directly into the data stream. Deepfakes, which are a type of digitally injected attack, are becoming inexpensive to create and have the potential to cause huge disruption. Digital injection attacks are far more scalable, dangerous, replicable and unpredictable and require a stronger level of security with ongoing protection against future evolving threats. The problem here to solve is to confirm that the imagery being analyzed is of the genuine user authenticating **right now**.

iProov Genuine Presence Assurance mitigates risks arising from a full range of attacks, including digital injection, and is the most secure anti-spoofing technology. An integral part of iProov Genuine Presence Assurance is the iProov Security Operation Center (iSOC) which detects biometric threats and anomalies from a range of devices and platforms. Rapidly identifying threats ensures prompt recovery and response to support the security of the solution and the protection of the customer organization and their users.

iSOC is a multi-layered, active threat management service. It combines advanced technology, with appropriate processes and experts, to provide resilience against the most sophisticated attacks. iSOC provides a level of added value that secures and reassures our customers and their end users. Find out more about iSOC click here.

iSOC is only possible because iProov takes a very different approach to providing secure biometric authentication, one which is proven, scalable and cloud-based.

Cloud-based authentication requires that matching and anti-spoofing of the biometric information is securely processed on the server. The device merely facilitates the interaction between the user and the authenticator. The user's security is not compromised by vulnerabilities of the actual device.

The iProov biometric authentication system does not store any personally identifiable information. The “face” is referred to by means of an anonymous pseudonym, which iProov receives from the relevant service provider. Therefore, the biometric is not associated with any information which might reveal the identity of the subject. Advantages of iProov’s cloud-based secure authentication:

- The methods of genuine presence detection are opaque to an attacker and cannot be reverse engineered
- They are subject to continuous change (a “moving target”), so the attacker never knows the exact method of authentication
- Attacks can be observed and analyzed and risks can be mitigated
- Inconvenience of re-binding or going through a tedious recovery process if a device is lost or changed, is removed, reducing risk and customer frustration

In addition, iProov uses a privacy firewall and strong encryption techniques to protect highly sensitive data such as face biometric to safeguard the user’s confidentiality.

4. Exhibited and potential harms of a particular biometric technology

There are a number of potential harms and biases which can impact biometric technology:

- **Ethnic/Gender/Age bias:** Attributes like age, gender, technical or cognitive ability, social or ethnic background must not become barriers to inclusion, and the system must not be allowed to operate with consistent bias. Unmonitored algorithms can erode diversity and inclusion by offering biased experiences to users of various ethnicities, genders and ages. iProov’s algorithms have been thoroughly tested by both the public and private sectors to ensure no significant level of bias. To read more about the three pronged approach iProov takes to monitor for bias read this paper.
- **Usability bias:** Usability is the fundamental business requirement of any solution, because it drives both inclusion and completion rates. There are several aspects that must be taken into account. First, it means that any solution should be user-centric and no effort such as complex instructions or actions should be expected from the user. Then it’s not equitable to demand ownership of a particular technology or device, for example restricting access only to those who have purchased a particular or high-end device. iProov has been designed as an effortless and passive experience; the user looks at the device, the device looks back and authentication is complete, typically resulting in success rates of greater than 98%.
- **Device bias**: Requiring cutting edge consumer devices excludes a vulnerable portion of society. iProov’s solutions have no need for special hardware; users can authenticate themselves on any device with a front-facing camera. This includes all personal devices - mobile phones, tablets and laptops. iProov has also been developed to work on kiosks for citizens that do not have access to a device of their own or need support. This was a key requirement in Singapore.

- **Privacy concerns**: iProov uses a privacy firewall and strong encryption techniques to protect highly sensitive data such as face biometric to safeguard the user's confidentiality

5. Exhibited and potential benefits of a particular biometric technology

As the world around us becomes more digital, cybercrime increases. It is more critical than ever that governments, financial institutions and businesses implement effective security measures.

2020 saw a significant increase in identity theft. Pandemic related stimulus programs became lucrative for individuals with negative motivations. The Federal Trade Commission saw a 2,918% increase in identity theft tied to government benefits in 2020. Analyst firm Aite Group reported losses from identity theft cases rapidly increased to US$712.4 billion in 2020, a 42% increase year-over-year.

Organizations need to establish trust and assure that the person accessing a digital service is who they claim to be. One of the areas of highest risk for any digital service is at the point of onboarding. The risk of enrolling the wrong person could incur significant financial loss, impact regulatory compliance and effect and organizations reputation.

Offering digital services raises concerns about remote identity verification, privacy and security. Implementing appropriate measures is vital in protecting legitimate online users from imposters or fraudsters.

iProov establishes the genuine presence of people asserting their identity online in low security unsupervised or semi-supervised locations such as shopping malls or travel hubs. iProov provides huge advantages in that it is:

- **Inclusive**; removes the need for any special hardware. Also replacing a device does not require the user to re-enroll
- **Passive and effortless**; without any voluntary action needed by the user
- **Reassuring**; by including an element of ceremony the user is aware that a secure authentication process is taking place
- **Secure**; widely tested including to National Grade level, users and organizations are protected from current and future threats and attacks
- **Efficient**; fast, secure and more reliable than humans at verifying identity particularly at spotting modern forms of spoof and deepfake attacks. According to a report by McKinsey, digital ID can provide a 90% potential reduction in customer onboarding costs. In Singapore, thousands of citizens use face verification to access government services at self-serve kiosks. Additionally, citizens who visit the service centers to reset their Singpass passwords have also seen a reduction in waiting time of over 10 minutes. At DMVs remotely provision a digital license or validate documents prior to an in-person visit can reduce the number of visits, wait times and burden on front office staff without

increasing back office overheads.

6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case

Biometric face authentication is still a relatively new area and as such there are, at present, no industry standards to test for digital injected attacks nor, as far as iProov can establish, are there any commercial labs which are able to provide testing for digital injection attack detection.The only option for organizations wishing to test for digital injection attacks is to use independent testing companies who usually have experience of working for government organizations. These companies are able to carry out extensive testing using a range of proven techniques. Companies which test for digital injection attacks look for verification that there is sufficient authentication and encryption protection to prevent an adversary from acquiring sensitive information through eavesdropping attempts. In addition, they also ensure that the external network security is sound and robust.

iProov is fully audited for a full range of attack scenarios:

- Tested to National Security Standards, by the US Department of Homeland Security, the UK Home Office, Australian Government and Singapore Government
- Conforms with ISO/IEC 30107-3 for presentation attack detection, tested by iBeta to Level 1 and Level 2
- Conforms with ISO/IEC 19795-1:2006 for testing biometric verification performance, audited by the UK National Physical Laboratory (NPL)
- iProov powered solutions conform to EN 319-401, certified by independent auditors including TÜV Informationstechnik GmbH and Ernst & Young for conformance to eIDAS Clause 24 1(d)
- Certified to ISO/IEC 27001:2013 Information Security Management System
- Complies with iRAP (Information Security Registered Assessor Program) and IP3 (identity proofing level three) in Australia
- Complies with GDPR (regulation (EU) 2016/679)

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Jacob Boudreau

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Jacob Boudreau
Michigan State University College of Law
Student (2L)

At the request of OSTP, I have prepared a comment on Topic 4; Exhibited and potential harms of a particular biometric technology. The main issue with the current biometric AI is that it was designed primarily by white men. Thus, the technology works best for that demographic. This will lead to concerns over the accuracy of the readings. Based on the RFI, the biometric data will be used to aid law enforcement, use for employment and student engagement, housing, and medical information. My concern is that we will be using a relatively new technology to make determinations that will have considerable impacts on people's every day life that has an unreasonable certainty for error.

First, in respect to law enforcement, I would have concerns over the issue of warrants with this technology. At what point does our biometric information count as our private property, and when would a warrant need to be issued? Would law enforcement using a third-party, or their own, software to gain access to our biometric information be an unwarranted search or seizure? I am aware of the country's hesitation to draw direct lines from the body to property (*Moore v. Regents of the University of California*), but at this point our biometric information is being treated by corporations, and now the government, like a commodity. A bit of data or information that can be bought and sold, stored for reference, or become a subject to study.

Second, I have concerns over the lack of humanity AI brings to the equation. I am a well-educated individual with a background in STEM, philosophy, and law. I am on board with using and developing technology to make life better for as many people as possible, but I have concerns with how it is being used. AI is a wonderful field and can bring so much to our society, but if it is used correctly. An AI, as much as it is developed, will always be artificial. The human

element in interactions will be lost and can never be recovered if AI is used to measure biometric data for such fundamental aspects of life – such as employment and housing. This would be using the technology for the wrong reason. After all, let's not lie to each other, this would adversely affect low-income communities more than others. Imagine being denied a job because a software interpreted you're biometric data to imply an angry or lazy disposition. Did we progress so far that we ended up back to old days of phrenology? AI denying people opportunities before they even get to talk to a person. I remember applying for a job. I had so many applications that were entirely automated messages. I never even talked to another person during the months of correspondence. Demoralizing did not even begin to describe it. I felt isolated. Like I was screaming my credentials into the void.

My third concern is notice and consent. AIs and its determinations are all made by the technology's software. The hardware is simply the means to gather the data – while there are issues here the primary concern is the determinations made on this information. The issue of notice comes into play for me because there is no way to know what the software is doing. Is the software using the correct methodology set out in the scientific literature? Or did the company adjust the code to change how the AI reads certain values? That is where my concern lies. How can the people ever be aware about the goings on within this technology? How would we know whether there is not dubious code or a hack? For this technology to be implemented in these fundamental aspects of lives, not only does this technology need to be perfectly accurate, but it also needs to be hack-proof and have some transparency to it. If one does not know what the technology is reading, how it is reading it, and for whom, does that person have informed consent?

My concern is that this technology, AI biometric determinations, is in its infancy. It should not be implemented currently unless the state can guarantee complete accuracy, security, and transparency. Since these are unobtainable at the current moment, I strongly advise against using this technology in policy making. I also have issues with using this technology for these purposes. As I said earlier, I am not against this technology for medical applications. I think there are certain fields and aspects of life where this technology is not only dubious but immoral. Those fields are the ones currently being considered (employment, housing, law enforcement). There is an entire genre of books and media warning of the application of these technologies for these purposes. This technology is best for aiding humanity by overcoming tasks we as people cannot do – well cannot do within a reasonable time. AI technology and biometrics should be used to sieve through the seemingly endless amounts of data. What would take years could only take moments with this technology. This technology is wonderful and life-changing if it is used right. Just as nuclear energy is a great source of clean energy, but, when used for the wrong purposes, nuclear weapons can lead to Armageddon. Not only is using this technology for these fundamental purposes wrong, using flawed and imperfect versions of the technology in these areas borders on willful negligence.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Jennifer K. Wagner, Dan Berger, Margaret Hu, and Sara Katsanis

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Eric Lander, PhD
Office of Science and Technology Policy (OSTP)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504
202-454-4444
BiometricRFI@ostp.eop.gov

Re: RFI Response: Biometric Technologies
86 FR 56300

Dear Dr. Lander:

We are writing in response to the OSTP's Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies published in the Federal Register on October 8, 2021 (86 FR 56300). As we write in our individual capacities, these comments are not to be attributed to our employers, professional affiliations, funding agencies, or any other person or entity. We focus our comments on the public sector and particularly on immigration-related uses of biometric technologies and we stress the importance that any policy or procedure regarding biometrics be firmly based in statutory and/or regulatory authority.

We write on our own behalf, drawing on the credentials and expertise of our group as any careful evaluation of these issues must be multidisciplinary.

- **Margaret Hu** is Professor of Law and International Affairs at Penn State Law and School of International Affairs at The Pennsylvania State University and an expert in immigration policy, national security, cybersurveillance, and civil rights;
- **Sara H. Katsanis** is Research Assistant Professor of Pediatrics at Lurie Children's Hospital and Northwestern University Feinberg School of Medicine and an expert in forensic DNA, clinical genetic testing, genetic testing oversight, and genetics policy;
- **Jennifer K. Wagner** is Assistant Professor of Law, Policy, & Engineering at The Pennsylvania State University, a licensed attorney, a member of the Pennsylvania Bar Association's Cybersecurity and Data Privacy Committee, and an expert in genetics, bioethics, and anthropology; and
- **Dan Berger** is Partner at the immigration law firm Curran, Berger & Kludt LLP in Massachusetts and an expert on immigration law.

In 2020, our group developed a comment in response to the Trump administration's NPRM Collection and Use of Biometrics by U.S. Citizenship and Immigration Services.[1] With the Biden administration now in place and you leading the re-launched OSTP, we thought it appropriate to update our comments here in the context of the ongoing, emerging uses of AI-enabled biometrics, particularly as used in immigration.

[1] Comment on the NPRM on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, submitted by Dan Berger (on behalf of Berger, Katsanis, Hu, and Wagner), October 13, 2020. Available at https://www.regulations.gov/comment/USCIS-2019-0007-5168. Docket No. USCIS-2019-0007, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services; Friday, September 11, 2020, pp.56338–56422

The RFI lays out several types of biometrics, with only a brief nod to DNA as a biometric. We see this as an unfortunate omission, given what is now known about the utility of genetic/omic information—something that we think you, Dr. Lander, know better than most scientists. However, the omission is perhaps not a surprising one; we observe current tensions and inconsistencies among different public entities' conceptualizations of DNA as a biometric (a point to which we will return in our closing remarks). Our comments herein include discussion of DNA data, facial images, and other biometrics. However, we assert that the ***context*** of biometric use is far more important than the ***type*** of biometric being used.

Our comments cover the following:

1. Our recent research survey data and findings on U.S. public perspectives on biometric data types across various contexts
2. Lessons from the 2020 proposed rule to expand biometric collection and DNA testing at USCIS
3. The future uses of biometric data toward a cybersurveillance state

1. Public perspectives on biometric data uses

Empirical data on the U.S. public's perspectives on diverse uses of biometrics in society has been lacking. We (Wagner and Katsanis) sought to address this knowledge gap and recently published two peer-reviewed journal articles.[2] We have made the full data set available open access at DOI: 10.7303/syn25618565. Useful highlights of these survey findings for OSTP include:

- Respondents were generally more comfortable than not with any of the six types of biometrics explored (fingerprint, voice sample, hand geometry, facial image, eye scan, and DNA).
- Of the respondents who were not at all or not very comfortable with biometrics, nearly one-third (28.9%) cited the main reason for this discomfort as because biometrics are a general invasion of privacy; approximately one-fifth (22.9%) indicated the main reason was because the purpose of the biometric collection or use was important to know; one-tenth (10.9%) noted the main reason was worry about government surveillance; one-twelfth (8.9%) indicated the main reason was because the policy for retaining or destroying the biometric information was important for them to know; and only 2.2% pointed to targeted advertising as the main reason for their discomfort.
- When asked about responsible uses of two *distinct* biometrics (DNA and facial imaging), a majority of respondents expressed distrust of advertisers, tech companies, retailers, and various levels of government to use either biometric. In contrast, a majority of respondents expressed *trust* in law enforcement agencies, intelligence agencies, scientists, and healthcare providers to use both types of biometrics. These majorities, however, were slim.
- Across a set of eight *social context* scenarios involving use of facial recognition technologies, only one (advertisers seeing how consumers respond to public advertising displays) drew a

[2] Katsanis SH, Claes P, Doerr M, Cook-Deegan R, Tenenbaum JD, Evans BJ, Lee MK, Anderton J, Weinberg SM, Wagner JK. A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PLoS ONE*, 2021;16(10): e025792. https://doi.org/10.1371/journal.pone.0257923; Katsanis SH, Claes P, Doerr M, Cook-Deegan R, Tenenbaum JD, Evans BJ, Lee MK, Anderton J, Weinberg SM, Wagner JK. U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics. *IEEE Transactions on Technology and Society*, DOI:10.1109/TTS.2021.3120317 (Early Access version published October18, 2021 at https://ieeexplore.ieee.org/document/9576819). See also Wagner JK. "Emerging public policy and perspectives on biometrics." Poster at the American Society of Human Genetics Annual Meeting, remote, October 2021 (showing from the same survey datasets that 49% of survey respondents reported their opinion of biometrics is less favorable now than it was five years ago; 60% indicated the COVID-19 pandemic had not changed their comfort with uses of biometrics in society; a strong majority expressed concerns about the possible misuse of their personal information generally, with 50% expressing they were very concerned and 38% expressing they were somewhat concerned; and only 31% indicated that biometric data protection and privacy laws in the U.S. are adequate).

majority opinion that such use is unacceptable. Only one scenario (law enforcement assessing security threats in public spaces) drew a majority opinion that such use is acceptable. (see **Figure 1** at the end of this letter)

- Across eight *health-related* scenarios involving use of facial recognition technologies, only two failed to elicit a majority response that the use was acceptable: healthcare providers monitoring patients' emotions or symptoms and scientists linking diverse data sources for health research. (see **Figure 1** at the end of this letter)
- Regarding relative privacy concerns in precision health research contexts, a majority of respondents (55.5%) expressed they were equally worried about the privacy of their electronic health record (EHR) data, DNA, and facial images. About one-fifth (20.1%) indicated they were most concerned about EHR data. Less than 7% indicated they were most concerned about facial images, and less than 18% indicated they were most concerned about DNA data.
- Sociodemographics had little or no effect on survey responses.

Public trust in social actors using biometrics responsibly appeared to be context-specific rather than type-dependent. Responses regarding comfort with biometrics might relate to individuals' understanding of the invasiveness of the collection rather than the ease or convenience of using the biometric. Generally, the public was split with slim majorities for each scenario analyzed, in line with the perception of ongoing distrust in how biometric data are used and managed. Given the divergent perspectives on trust in healthcare providers (who are generally trusted) and tech companies (that are generally distrusted) when using biometrics, it is apparent that biometric initiatives that involve partnerships between the two will likely generate controversy. Respondents' perspectives underscore the need for transparency and oversight. Additionally, these empirical findings suggest differential informational needs are critical to understanding public perspectives on uses of AI-enabled biometric technologies.

2. Lessons from the 2020 proposed USCIS biometric expansion

We authors collaborated in 2020 on a comment to the Notice of Proposed Rulemaking (NPRM) on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (USCIS).[3] We also collaborated on a summary of those comments published in March of 2021.[4] The NPRM expanded the definition of biometrics to authorize the collection of personal data for the purposes of vetting and tracking individuals throughout the "immigration lifecycle." The proposed changes were both complex and sweeping and, therefore, we strongly recommended that any such large-scale program result from Congressional action (not Executive branch rulemaking) and be subject to rigorous, sustained oversight. Here, we review our comments on the NPRM as they address key issues on the use of biometrics. We also note that the current Administration has not disavowed the NPRM: it is not clear if some or all of those proposals will be re-issued. Our only glimpse into the current Administration's policy on these

[3] Comment on the NPRM on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, submitted by Dan Berger (on behalf of Berger, Katsanis, Hu, and Wagner), October 13, 2020. Available at https://www.regulations.gov/comment/USCIS-2019-0007-5168. Docket No. USCIS-2019-0007, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services; Friday, September 11, 2020, pp.56338–56422

[4] Berger D, Hu M, Katsanis SH, Wagner JK. Biometric Data and Midnight Regulations. *The Regulatory Review*. March 11, 2021. Available at: https://www.theregreview.org/2021/03/11/berger-hu-katsanis-wagner-biometric-data-midnight-regulations/

issues is of concern - a recent Privacy Impact Assessment[5] (PIA) that moves toward systematizing DNA verification screening at the border without statutory or regulatory authority.[6]

In particular, the proposed rules outlined two separate processes: (1) the expanded definition and uses of biometrics and (2) the systematic implementation of DNA testing for verification of family relationships. Each of these processes are complex, and any future plans should separately address each since the legal authority and the parameters for testing (and oversight of testing) are different from that of the collection and storage of information. Moreover, we argued that the NPRM had put the cart before the horse: DHS must first clearly identify the problem for which biometrics (and reduced reliance on documents and other biographical information) is the appropriate solution.

Further, the technologies specifically proposed in the NPRM (e.g., facial recognition technology) have already been scientifically shown to be discriminatory (e.g., against women and people of color). Therefore, any new proposals should be carefully evaluated for disparate and discriminatory effects on certain populations and groups of people.

The proposal also included a dramatic expansion of the collection and storage of data on children. There is a long history of data from children being recognized as more sensitive than that of adults (e.g., medical and educational contexts). Removing the presumption of innocence for migrant children is contrary to the growing trend to protect trafficked persons from punishment for acts performed at the demand of their oppressors (traffickers). Such action would subject children to unnecessary and unjustified criminal and security-related screening. Any proposed change must be pursuant to Congressional action and subject to independent oversight informed by professionals with relevant expertise.

The NPRM also increased reliance on DNA data for verification of family units with a particular focus on parent-child relationships. We urged caution in that area to protect against separations of children from accompanying caregivers given that (1) presence of a genetic relationship does not eliminate the possibility of a parent trafficking their child; and (2) absence of a genetic parent-child relationship does not constitute evidence of trafficking.

The NPRM further outlined plans to retain relationship test results as "partial DNA profiles." We recommended that any genetic data be destroyed and only the resulting test outcome (i.e., indication of confirmation of relationship) be retained for immigration records. We also recommended that any such plan require DHS to demonstrate that the DNA testing and data retention is consistent with statutory authority.

At the time of the NPRM, rapid DNA technologies were used in lieu of relationship testing laboratories to provide DNA testing onsite in CBP/ICE stations. Rapid DNA testing allows for quick result return within hours, unlike laboratory testing, which can require families to wait, likely in detention, for weeks to receive the test results. The NPRM proposed a shift away from rapid DNA technology to mandate reliance on relationship testing laboratories accredited by the American Association of Blood Banks (AABB). The most recent Biden Administration's Privacy Impact

[5] Privacy Impact Assessment for the Operational Use of Familial DNA, DHS Reference No. DHS/CBP/PIA-071. September 10, 2021.
[6] The PIA at p.1 argues, "…Familial DNA testing is being implemented for purposes of complying with a court order" and later notes, "In January 2020, the court in Ms. L v. ICE, 3:18-cv-00428 (S.D. Cal), required DNA testing be conducted prior to any separation of an adult and child based on parentage concerns." While the PIA failed to provide a full, direct citation to the January 2020 court order, it appears to be *Ms. L. v. U.S. Immigration and Customs Enforcement.* Case No.: 18cv0428 DMS (MDD), Document 509: Order granting in part and denying in part plaintiffs' motion to enforce preliminary injunction. Filed January 13, 2020, p. 11. Available at: https://www.clearinghouse.net/chDocs/public/IM-CA-0121-0011.pdf

Assessment[7] on family verification practices decisively switched to the use of an external laboratory rather than the rapid on-site testing. This will certainly prolong detention for migrant families. We noted in our 2020 comment that relationship DNA testing for family verification should use the most appropriate technology to measure a range of relationships, not just parentage. Rapid DNA tests at this time can only be applied to parent-child and full sibling relationships, whereas relationship testing laboratories might provide broader testing for the diversity of family structures that exist on the ground. Whether through rapid DNA technologies or a laboratory, it should be noted that AABB-accreditation is insufficient oversight. AABB lacks the scope of oversight that its equivalent organizations provide for clinical (i.e., CLIA) or forensic DNA (i.e., FBI, ASCLD) testing. For example, AABB does not address how test limitations are communicated before testing nor how unusual test results or unexpected findings are handled.

A final overall response we had to the NPRM regarded privacy, which is a fundamental human right identified in the Universal Declaration of Human Rights. A proposal with international implications must extensively engage with relevant international laws and guidelines on data privacy. The proposed rule noted DHS made the decision to move "beyond only eligibility and admissibility determinations" to enable "identity management" and "enhanced vetting." These applications mark major departures from agency privacy practices that recognize the critical importance of nuance, context, and discretion under the Privacy Act of 1974 (5 USC § 552a) as applied to U.S. citizens and permanent residents. Moreover, the NPRM authorized sharing of DNA test results and biometric data "with other agencies where there are national security, public safety, fraud, or other investigative needs." There must be clear guidelines for the use and sharing of biometric data, including DNA test results.

3. Future U.S. government agency biometric expansion

For the past decade, scholars and experts have juxtaposed small data policing with big data cybersurveillance practices. The Snowden disclosures accelerated this discourse: the Squeaky Dolphin PowerPoint slide "outlines an expansionist program to bring big data together with the more traditional approaches of the social and humanistic sciences: the worlds of small data... it is all about supplementing [big] data analysis with broader sociocultural tools from anthropology, sociology, political science, biology, history, psychology, and economics."[8]

DHS now has an opportunity to revisit the Trump Administration's regulatory policies on biometrics. In the case of the proposed overall biometrics collection NPRM, the entire rulemaking was both ill-advised and rushed, as we detailed in our public comment in 2020. The NPRM provided an extraordinarily short window of 30 days for public comments, making it virtually impossible for experts to assess the proposed rule thoroughly. Indeed, each section of the proposed rule contained scientific, technical, legal, economic, and ethical issues that warranted further evaluation by experts in industry, including those in genetics, biometrics, forensics, ethics, and distinct areas of law such as immigration and data privacy, among other fields.

Understanding biometric surveillance in the context of predictive policing and national security is critical. Predictive analytics make actionable those insights gleaned from data by using algorithms, AI, and other machine-learning techniques. Extreme vetting, as it was promulgated in the prior administration, offers a useful case study. Shortly before his election, Trump announced a proposal for the "extreme vetting" of

[7] Privacy Impact Assessment for the Operational Use of Familial DNA, DHS Reference No. DHS/CBP/PIA-071. September 10, 2021.
[8] Crawford K. The Anxieties of Big Data. *The New Inquiry*. May 30, 2014. Available at: http://thenewinquiry.com/essays/the-anxieties-of-big-data/

immigrants and refugees.[9] Trump clarified that "[t]he Muslim ban is something that in some form has morphed into a[n] extreme vetting [protocol] from certain areas of the world." Extreme vetting, as it was incorporated into Executive Orders and regulatory mechanisms, purported to allow the government to predict terrorism through a combination of biometric and biographic cybersurveillance tools.

Extreme vetting—and DHS expansion of both biometric data collection and social media surveillance tools—allows the government to collect, aggregate, and analyze billions of pieces of social media data points. With approximately "2.3 billion active social media users[,]" the ubiquity and public availability of social media allows the government to monitor those who "upload hundreds of millions of photos and send 500 million tweets each day, add 300 hours of video to YouTube each minute, and create six new Facebook profiles each second."[10] Nick Rasmussen, Director of the National Counterterrorism Center, explained: "[T]he work we're doing now with our partners in the intelligence community often doesn't involve really, really sensitive intelligence. It involves looking at Twitter and/or looking at some other social media platform and trying to figure out who that individual behind that screen name, behind that handle might actually be and whether that person poses a threat . . . ."[11]

Another document released from the Snowden archives describes the preemptive philosophy of combining biometric and biographic data, presumably through AI and other data-driven tools. In a *New York Times* article by James Risen and Laura Poitras, published on June 1, 2014, titled *NSA Collecting Millions of Faces from Web Images*,[12] the authors discuss Snowden's disclosures that focus on biometric data collection. Risen and Poitras quote a 2010 NSA document that explains, "'It's not just the traditional communications we're after: It's taking a full-arsenal approach that digitally exploits the clues a target leaves behind in their regular activities on the net to compile biographic and biometric information that can help implement precision targeting.'"[13]

The long-term consequences of modern big data surveillance can be better envisioned by anticipating how and why big data vetting protocols—the combination of biometric and biographic surveillance—may be extended to the entire population. Eventually, all citizens and noncitizens may face various stages of technological vetting and algorithmic screening as part of a national security policy. Importantly, in parallel with the extreme vetting protocols mandated by the Trump administration Executive Orders, almost every immigration reform effort since 9/11 has called for biometric data collection from the entire citizenry of the United States to enhance border security efforts. Contemporary vetting and risk assessment systems integrate biometric cybersurveillance into AI and algorithmic decision-making to determine identity and associational assessments in criminal and terrorist screening contexts and to gauge

[9] Federal Register Notice, Executive Office of the President, Implementing Immediate Heightened Screening and Vetting of Applications for Visas and Other Immigration Benefits, Ensuring Enforcement of All Laws for Entry into the United States, and Increasing Transparency Among Departments and Agencies of the Federal Government and for the American People (April 3, 2017), 82 FR 16279. Available at: https://www.federalregister.gov/documents/2017/04/03/2017-06702/implementing-immediate-heightened-screening-and-vetting-of-applications-for-visas-and-other. This policy of the previous administration has not been rescinded.

[10] Handeyside H. To the Government, Your Latest Facebook Rant is Raw Intel. *ACLU*. September 26, 2016. Available at: https://www.aclu.org/blog/privacy-technology/internet-privacy/government-your-latest-facebook-rant-raw-intel

[11] "Can the high-tech hunt for terrorists stop lone wolf attacks?" *PBS NewsHour*, host Ifill B, correspondent O'Brien M. September 6, 2016. Available at: https://www.pbs.org/newshour/show/can-high-tech-hunt-terrorists-stop-lone-wolf-attacks (capturing PBS Correspondent Miles O'Brien's Interview with Nick Rasmussen, Director of the National Counterterrorism Center).

[12] Risen J, Poitras L. NSA Collecting Millions of Faces from Web Images. *New York Times*. June 1, 2014. Available at: http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html

[13] *Id.* (with Risen and Poitras quoting a 2010 NSA document)

risk. Yet, given the potential discriminatory impact of biometric surveillance, extreme vetting systems like the one promulgated by the Trump administration and extended into the current Administration might bring about disproportionate burdens on minority communities. Furthermore, the efficacies of the systems are unclear.

Governmental agencies do not treat DNA and data derived from DNA consistently as a biometric. For example, the Department of Health and Human Services downplays the genome's utility as a biometric in order to enable its extensive use as de-identified health data for research;[14] the Department of Justice tiptoes around these dual properties, relying on DNA markers useful for identification and avoiding DNA data with potential health relevance; and the Department of Homeland Security downplays the genome's utility for health insights to enable its broad interpretation of "identification" beyond DNA markers.[15] The distinct approaches among these different agencies reflect, too, the statutory authority for these agencies' collection and use of DNA as well as the potential constraints intended to prevent governmental overreach and protect individuals' rights to privacy. Further complicating matters, state biometric statutes can vary in their definitions of biometrics, sometimes—as is the case with the Illinois Biometric Information Privacy Act—excluding DNA because of its health import and corresponding applicability of health privacy laws.[16] Recognizing this tension and these incompatible conceptualizations of whether DNA is a biometric, artificial intelligence has the potential to wreak havoc on all current data governance frameworks. Furthermore, the lack of a broadly recognized right to genetic privacy along with the continued viability of the Third-Party Doctrine in 4th Amendment jurisprudence[17] leads to ongoing uncertainty and civil rights threats for individuals in the United States. All of this underscores the urgent need for both legislative action to regulate public and private collection and use of biometric data, as well as the need for an AI Bill of Rights.

In summary, we appreciate the OSTP's interest in better understanding AI-enabled biometric technology uses as well as the OSTP's ongoing efforts to develop an AI Bill of Rights.[18] We urge that expansion of biometric uses be in full recognition of the prior administration's proposals and in keeping with perspectives of the American public on the acceptability of their use. We hope that our data on perspectives and our reflections on the power of biometric data as a surveillance tool are useful to you.

If we can be of further assistance to you, please do not hesitate to contact us.

[14] Some scholars nevertheless publicly acknowledge the genome as, itself, a biometric. E.g., Ohno-Machado, L. "Making Controlled-Access Data Readily Findable and Accessible." Plenary presentation at the webinar "Streamlining Access to Controlled Data at NIH: Tackling Challenges and Identifying Opportunities," NIH Office of Data Science Strategy, remote, July 09, 2021. Available at: https://www.youtube.com/watch?v=2mH4kg7ORr4

[15] In NPRM 2020 FR 56338, DHS stated that its biometrics currently consist of, e.g., "... in certain situations, voluntary DNA testing to verify a claimed genetic relationship" and at 56414 noted, "Biometrics means the measurable biological (anatomical and physiological) or behavioral characteristics of an individual, including an individual's fingerprints, palm prints, photograph (facial image), signature, iris (iris image), voice (voice print), and/or DNA (partial DNA profile) (subject to the limitations in 8 CFR 103.16(d)(2)."

[16] 740 ILCS 14/10 definition of "Biometric identifier" excludes biological materials protected under the Genetic Information Privacy Act as well as information gathered in a health care setting.

[17] See, e.g., Maryland v. King, 569 U.S. 435, 133 S. Ct. 19581, 186 L.Ed.2d 1 (2013) (conceptualizing identification purposes as quite broad and allowing DNA identification) and Carpenter v. United States. 138 S. Ct. 2206, 2262-63; 201 L. Ed. 2d 507 (2018) (C.J. Roberts, questioning in dicta, whether the government can "secure your DNA from 23andMe without a warrant or probable cause" without running afoul of 4th Amendment right to privacy given the Third Party Doctrine.)

[18] Lander E, Nelson A. Americans Need a Bill of Rights for an AI-Powered World. *Wired*. October 08, 2021. Available at: https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/

Sincerely,

[redacted]

Jennifer K. Wagner, JD, PhD
Assistant Professor of Law, Policy, & Engineering
Pennsylvania State University
[redacted]

[redacted]

Dan H. Berger, JD
Partner, Attorney
Curran Berger & Kludt LLP
[redacted]

[redacted]

Margaret Hu, JD
Professor of Law and International Affairs
Penn State Law and School of International Affairs
Institute for Computational and Data Sciences
Pennsylvania state University
[redacted]

[redacted]

Sara H. Katsanis, MS
Research Assistant Professor
Northwestern University Feinberg School of Medicine
Ann & Robert H. Lurie Children's Hospital of Chicago
[redacted]

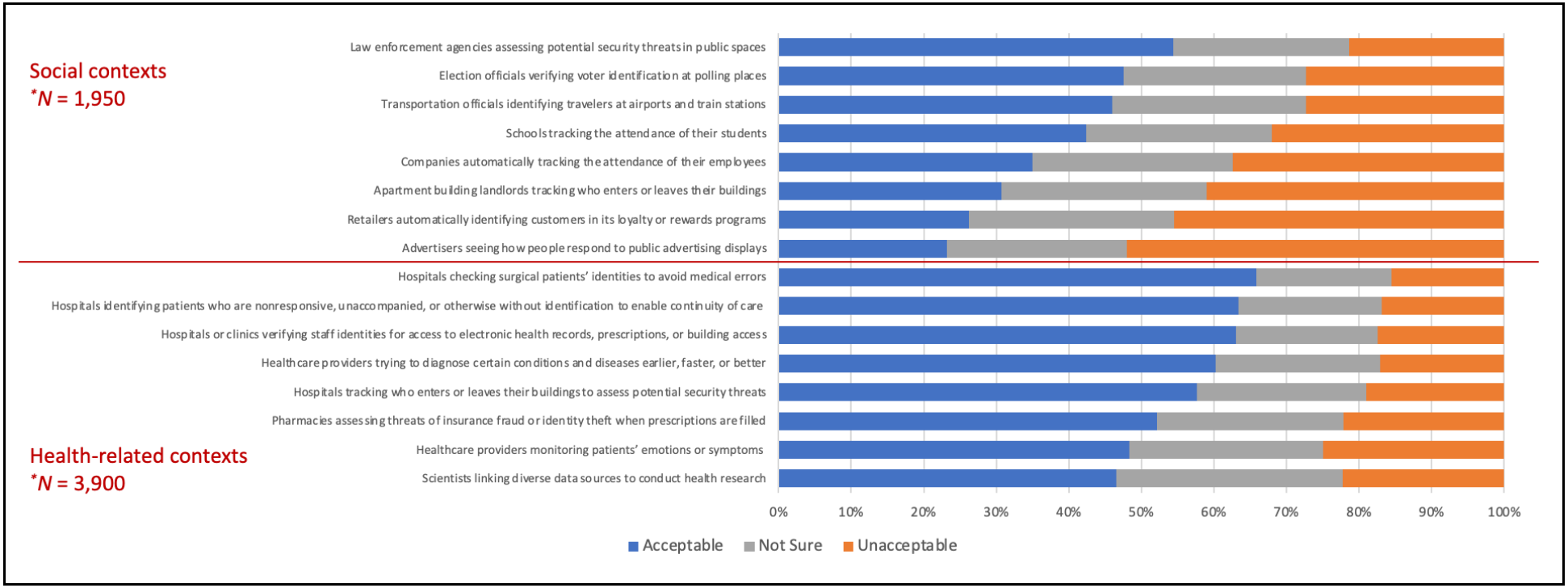


Figure 1. Data from our biometrics surveys on acceptability of biometric uses in various contexts. **N* varies within questions as the "no answer" responses were removed. Social contexts range from *N* = 1,924 - 1,950; health-related contexts range from *N* = 3,855 - 3,900. Figure adapted from Figure 2 of a prior publication.[19]

[19] Katsanis SH, Claes P, Doerr M, Cook-Deegan R, Tenenbaum JD, Evans BJ, Lee MK, Anderton J, Weinberg SM, Wagner JK. A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PLoS ONE*, 2021;16(10): e025792. https://doi.org/10.1371/journal.pone.0257923

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Jonathan Barry-Blocker

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Public Comment to RFI on Public & Private Sector Uses of Biometric Technologies

Respondent: Jonathan Barry-Blocker, Esq.
Respondent Type: Member of the Public
Respondent's Professional Roles: Law professor, civil rights advocate

I submit this Comment in my personal capacity. My professional experiences inform my analysis. I practiced law for a decade in varied roles like state prosecutor, legal services attorney, and most recently as an impact litigator in Alabama with a prominent southern civil rights organization. Currently I teach and research law at a southern public university. My academic work focuses on civil rights and trial skills. Consequently, my Comment highlights biometric technology use and potential for abuse in the Deep South.

I will focus on biometric technology in correctional settings as incarcerated citizens are some of the least protected Americans. This comment neither disputes nor critiques the efficacy of biometric technologies. Instead, I discuss the lack of oversight and regulation in correctional settings in the Deep South, particularly Alabama.

I. Use of Biometrics in Correctional Settings to Identify & Control People

Alabama has the highest incarceration rate of any democratic government. And to sidestep substantial criminal justice reform or repair its aging prisons, the state plans to construct three (3) mega prisons. The state prison system suffers from severe understaffing with a 50% vacancy rate in June 2020. By June 2021, staff attrition increased the vacancy rate to 52%. Judge Myron Thompson confronted this issue in a recent 600-page opinion where he ordered the Alabama Department of Corrections (ADOC) to [again] boost staffing levels and protect incarcerated residents from violence. The state's chronic failures precipitated the U.S. Department of Justice to file a separate suit against ADOC in 2020. But Alabama is perennially broke. It is unlikely ADOC will ever recruit sufficient people to operate the prisons, much less the mega prisons. Thus, I believe state leaders will rely heavily on biometric technologies to compensate for deficient staffing in these forthcoming facilities.

The use of biometrics in correctional settings is not new. Since 1999, some Florida jails relied on retinal scanners to track and confirm identities of incarcerated persons. In 2006 a "successful experiment" at Charleston's naval brig recommended expanding biometric use in civilian correctional facilities to better track people. By 2015, a Georgia jail installed biometric locks that confirmed correctional officers' fingerprints and heartbeats before they opened doors.

Alabama's corrections facilities use these technologies. The Calhoun county jail added facial recognition to its arsenal of fingerprint and iris scan technology in 2012. That same year, ADOC extracted fingerprints from all visitors to state prisons, ostensibly to "verify identity at the door."[1] Years later the Madison county jail relied on Clearview AI's systems to collect visual and auditory data. Most recently, the Etowah County jail in Alabama outfitted all cells and pods with fish-eye lens

[1] Alabama was the first state to demand such biometric information from people not incarcerated.

cameras and hanging microphones in order to participate in a reality television show.[2] After the show finished taping and aired, the jail did not remove the cameras and microphones. Neither residents incarcerated at the jail nor community members know whether they continue to operate. As one detainee shared with me, if the cameras and microphones still worked, the violence or inhumane conditions they recorded did not spur correctional staff to protect her and other women. And the jail has not updated its policies to account for the collection, retention, and use of this biometric information.[3]

The technologies' increased presence raise exploitative surveillance concerns. For example, consider voice prints. The Intercept reported:

> [A]uthorities are acquiring technology to extract and digitize the voices of incarcerated people into unique biometric signatures, known as voice prints. Prison authorities have quietly enrolled hundreds of thousands of incarcerated people's voice prints into large-scale biometric databases. Computer algorithms then draw on these databases to identify the voices taking part in a call and to search for other calls in which the voices of interest are detected. Some programs, like New York's, even analyze the voices of call recipients outside prisons to track which outsiders speak to multiple prisoners regularly.

The article recounts corrections departments in Florida, Texas and Arkansas use the technology. Georgia's prison system recently contracted for the technology. Even the Alachua county (Gainesville), Florida jail surveils jail calls. These technologies capture, analyze, and track all voices in a conversation. This includes non-incarcerated speakers, folks not subject to continuous government control. While all speakers may consent to having the prison/jail calls recorded, they do not consent to their voice patterns being seized, stored, and used for investigatory purposes *ad infinitum* and without limitation.

I believe Alabama, and likely other southern states, will use biometric technologies to track, manage, and investigate people housed in their prisons. These states will over rely on the technology due to chronic staffing shortages. And the state will provide scant oversight of ADOC's use of biometric technologies.

II. Dearth of Security; Deficient Stakeholder Engagement in Policymaking and Lawmaking

States too poor to build prisons do not possess resources to protect sensitive biometric information. In 2012 U.S. Supreme Court Justice Sonia Sotomayor intuited it "may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily

[2] The show – *60 Days In* – is an A&E docuseries that plants volunteers as undercover detainees at a jail. The show records their interactions with incarcerated residents, jail staff, and visitors. The volunteers are tasked with obtaining evidence of questionable or illegal activities within the jail that correctional officers or surveillance systems may miss.
[3] It is worth noting the Etowah county jail also doubles as an immigrant detention center.

disclosed to third parties."[4] Federal and state lawmakers, though, largely ignore her warning, especially in the Deep South.

In 2018, Alabama was the last state to enact a data breach notification law. A high-level cyber security professional with the city of Birmingham affirmed the state's cavalier attitude. The official conceded the city lacked adequate protection against cyberattacks stemming from years of insufficient appropriations and political disinterest.[5] Last year hackers proved him right when they breached surveillance systems at the Madison County jail in Alabama's second largest city. The jail cameras used facial recognition to track detainees and correctional staff. Hackers viewed live footage and audio of detainees and interviews between law enforcement and suspects. Now Mobile, the state's third largest city, uses Clearview AI's facial recognition technology.[6] It is unknown if the city of Mobile suffered a similar breach. Authorities never addressed or mitigated the threat to exposed citizens' privacy rights.

Disturbingly, Alabama refuses to enact consumer biometric and privacy protection measures like Illinois, Texas, California, and Virginia. Even though the state deployed biometric technologies for more than a decade in correctional settings. In late 2019 the state legislature authorized an artificial intelligence (AI) commission, the closest it has come to examining biometrics, to explore the presence and use of AI within the state. The commission's report would guide lawmakers in regulating the technologies. However as of early 2022, the commission has not issued a report. And even if it does in the future, the report would not lead to substantive lawmaking[7] or equitable laws[8] to protect Alabama citizens.

As an aside and further example, Alabama's parole agency uses two risk assessment algorithms determine parole decisions. The agency adopted these algorithms around 2016. State law requires the parole board audit these algorithms every three (3) years. Industry best practices recommend the state calibrate these algorithms to their incarcerated populations before use. Alabama flouts these laws and recommendations. I know the parole board never audited its algorithms. Nor did the parole board calibrate the risk assessment tools to the state's populations. Nevertheless, the parole board continues to use these algorithms in parole decisions. Furthermore, ADOC also uses one of these risk

[4] *See United States v. Jones*, 565 U.S. 400 (2012) (Sotomayor, J. concurring)
[5] Birmingham is Alabama's most populous city. Alabama Power and Regions Bank are headquartered there. The city is also home to the state's best (and most) hospitals and specialty medical facilities.
[6] Clearview AI has a well-documented history of violating privacy rights and exploiting biometric data. In 2021 Canada classified their biometric technology illegal after the company impermissibly collected Canadians biometric information. The country censured its national law enforcement for using the technology. Australia subsequently held the company violated national privacy laws when it covertly collected facial biometrics and incorporated them into its AI-powered identify matching service sold to law enforcement. And Britain's data privacy authority fined Clearview AI $22.6 million for failure to comply with data protection laws.
[7] Alabama had a Drone Task Force in 2014. The task force never issued a report. Instead it requested a state agency take over its tasks. The state agency seemingly abandoned the investigation. And the legislature never enacted any laws to regulate drones.
[8] The AI commission's membership is dominated by banking and business interests. A few academics and scientists are members. No consumer protection, indigency, or civil rights interests are represented in the membership.

Though the state legislature never enacted laws responsive to the drone task force, it recently proposed prohibitions on advocacy groups using drones to monitor unlawful pollution.

assessment algorithms on residents newly admitted to the state prisons. ADOC likely committed comparable regulatory violations. This is par for the course in Alabama.

Thus, the federal government should not presume states or localities in the Deep South will protect biometric information. And federal guidance or intervention is warranted given Alabama's likely reliance on these technologies in its forthcoming mega prisons.

III. The U.S. has Tenuous Governance Regimes

Unregulated biometric technologies facilitate unlawful searches and seizures in correctional settings in contravention of the Fourth Amendment of the U.S. Constitution. A "search" occurs whenever the government or a government-assisted third party intrudes upon an individual's subjective expectation of privacy. A "seizure" occurs whenever the government or a government-assisted third party captures and retains an object or information possessed by an individual. For example, voice print technologies exploit ill-defined parameters of Constitutional and privacy laws.[9] Neither federal nor southern state courts have addressed searches and seizures via these technologies in correctional settings.[10] And most southern states have few, antiquated laws to "guide" technology users.[11] Consequently, authorities and third parties must look to various Fourth Amendment decisions for guidance.[12]

For example, in *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), the U.S. Supreme Court repudiated the collection and selective drug testing of urine from pregnant [Black] women for forensic purposes. Hospital staff would test urine from women under suspicion of – but not arrested for – drug use. The hospital had a written agreement with local police, as well as supporting hospital policies, to surveil and report these pregnant women.[13] The Court ruled searching urine for drug use was outside the scope to which women consented for their urine to be collected and tested at the hospital.[14]

[9] Though the U.S. Supreme Court decision *Hudson v. Palmer*, 468 U.S. 517 (1984) held incarcerated residents have no reasonable expectation of privacy in their jail cell, the Court did not address their bodily privacy rights. "*Hudson* merely concluded that the Fourth Amendment affords no protection for the prisoner's privacy interest in his cell or his possessory interest in his effects kept there, and thus arguably has no application to searches and seizures of the person of a prisoner." *See* Wayne LaFave, *Search And Seizure: A Treatise on the Fourth Amendment (5th ed. 2018)*, § 10.9(b), p. 416.

[10] *United States v. Dionisio*, 410 U.S. 1 (1973) concerned voice exemplars collected in a grand jury investigation. The mass collection of voice files in correctional settings does not support ongoing or exigent criminal investigations.

[11] Alabama is one of the few states without strong wiretapping laws. For the past few legislative sessions, the state Attorney General sought to pass expansive surveillance measure. It would authorize law enforcement to collect, track, and analyze aural and digital communications of any person or entity with suspected ties to illicit drugs. Civil rights organizations and their allies managed to stymie the bill.
Also, most southern states refuse to enact strong privacy protection laws like Illinois' Biometric Information Privacy Act (BIPA). Virginia's new Consumer Data Protection Act is an anomaly.

[12] These decisions have limited application to correctional settings. Each decision concerns arrest or pre-trial issues. Courts have not addressed biometric regulation/rights in correctional institutions.

[13] Nearly all the surveilled women were Black and poor. Despite the common knowledge that Black people do not consume illicit substances at rates greater than other racial or ethnic groups.

[14] As an aside, Alabama is the only state with a law that criminalizes pregnant women suspected of illicit drug use. Consequently, several county jails actively – and in the case of Etowah County aggressively – surveil the bodily fluids of women arrestees and detainees. Officers and jail nursing staff will collect and conduct warrantless pregnancy and drug tests on the women's urine. These tests are done for forensic purposes solely. Unlike the South Carolina hospital in *Ferguson*, Alabama authorities largely target poor White women.

Like urine, voices are biometrics expelled from the human body. Voices should be protected from discriminatory warrantless seizure when participating speakers are not the subjects of open and active criminal investigations.

A decade later the Court seemed less sure of Fourth Amendment protections for biometrics. In *Maryland v. King*, 569 U.S. 435 (2013) the Court permitted police to obtain an arrestee's DNA (via swabbing the inside of his cheek) and run it through the FBI's DNA database. Authorities sought to identify Mr. King in other criminal matters. The Court minimized the invasion of privacy because law enforcement used minimally invasive means and did not reveal the arrestee's genetic traits.

Not a year later the Court did an about face and conferred greatest protection to cell phones, which contain substantial biometric information. In *Riley v. California*, 573 U.S. 373 (2014) the Court prohibited law enforcement from conducting warrantless searches of a cellphone's contents incident to arrest. Modern phones contain "the privacies of life" and are unlikely to contain information pertinent to immediate officer safety, destruction of evidence, or current criminal investigations. The Court foresaw warrantless searches would lead to pretextual searches and seizures of other private information, such as the trove of biometric information stored within the phone.

Four years later the Court went a step further in *Carpenter v. United States*, 585 U.S. __, 138 S.Ct. 2206 (2018). It extended Fourth Amendment protections to cell site location data generated by third-party cell phone providers. While this decision does not concern a biometric technology, it shows the Court's willingness to protect personal information from government encroachment.

Like mobile phones, recorded conversations contain voice information of more than the person under government supervision. Other parties in a recorded call can include the non-incarcerated caller, children, and non-participants to the call.[15] Analogous to the *Riley* decision, law enforcement and third-party contractors should not have unfettered authority to seize these voices from a recorded conversation.

Unfortunately, these high court decisions provide porous boundaries for government and government-assisted use of biometric information. And the opinions do not address how citizens can access biometric data seized by the government or third parties. An issue that will paramount for people incarcerated, working in, or visiting Alabama's three (3) new mega prisons.

One appellate decision from Florida touches on citizens' access to biometric data. In *Lynch v. State*, 260 So. 3d 1166 (1st DCA 2018) (per curiam) an appellate court held a defendant is not entitled to comparison photos from a facial recognition software. Mr. Lynch sought the photos as potentially exonerating evidence pursuant to discovery rights conferred by the Fourteenth Amendment of the U.S. Constitution and *Brady v. Maryland*, 373 U.S. 83 (1963). He doubted the software sufficiently determined he was the man selling drugs in police photos. The photo identification was the basis for his arrest days after the drug transaction occurred. This was an issue of first impression for the state

[15] For example, food service personnel in a drive thru or eatery, business greeters, or other folks in the same room as a caller. None of these folks consented to a recorded phone conversation. None of them should have their voices searched and seized by authorities and third parties.

and possibly the nation. Even so, the court laconically and without noticeable precedential support reasoned since Mr. Lynch "cannot show that the other photos the database returned resembled him, he cannot show that they would have supported his argument that someone in one of those photos was the culprit." The court further elided over the basis for arrest by highlighting "the jury convicted only after comparing the photo the officers too to Lynch himself and to confirmed photos of Lynch." The Florida Supreme Court denied Mr. Lynch's petition for discretionary review because the lower appellate decision did not conflict with other Florida appellate court decisions.[16]

The appellate court's decision flew in the face of relevant state and federal case law regarding *Brady* material.[17]

Mr. Lynch could not have met this contrived burden without hacking the state's files or receiving information from a mole within the police station. But the court conveniently ignored this reality. Victor Holder, Mr. Lynch's appellate attorney, highlighted how lack of regulation permitted the outcome. "Florida law enforcement agencies currently use facial recognition technology with little to no public awareness, no uniform standards governing its use, and no public oversight by the Florida Legislature."

While, no other court has relied on *Lynch* to determine a citizen's right to biometric information do not presume other states will disregard the opinion. Alabama courts consistently adopt decisions from other southern or conservative states whenever controlling precedent is absent from Alabama's common law.

IV. Conclusion

This Comment warns against relying on southern states to adequately regulate and protect biometric information. Too often these states treat emerging technologies as expediency measures. Even if the technology benefits the citizenry as well as the government, these states never enact protective laws. Alabama especially has a deplorable record of ineptly using biometric technologies. And their state lawmakers are prone to legislating emerging technologies (if at all) in an inequitable fashion. I do not believe the Alabama legislature will regulate biometric technologies once the mega prisons are constructed. Therefore, the federal government must establish clear guidelines for biometric technology use and the retention of any data.

[16] *See Lynch v. State*, No. SC19-298, 2019 Fla. LEXIS 1300, at *1 (July 19, 2019).
[17] *See Floyd v. State* 902 So. 2d 775 (Fla. 2005) (finding witness interviews that indicated an alternative perpetrator was *Brady* material; *Rogers v. State*, 782 So. 2d 373, (Fla. 2001) (finding that undisclosed police reports were "bedrock Brady materials" as they "could have been used to show that another person" committed the crime, as reflected by the many witness descriptions matching an alternate suspect."). *See also United States v. Jernigan*, 492 F.3d 1050 (9th Cir. 2007) (finding a *Brady* violation where prosecution failed to "disclose the existence of a phenotypically similar bank robber who had been robbing banks in the same area after Jernigan's incarceration); *Bradley v. Nagle*, 212 F.3d 559 (11th Cir. 2000) (discussing *Brady's* underlying policy and that even inadmissible evidence could lead to strong exculpatory evidence and therefore does not justify withholding it).

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Joseph Turow

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Annenberg School for Communication
University of Pennsylvania
3620 Walnut Street
Philadelphia, PA 19104-6220
[redacted]

Joseph Turow
Robert Lewis Shayon Professor
of Media Systems and Industries

To the Office of Science and Technology Policy:

I am responding to your Biometric RFI with the hope of furthering an important national conversation about the rise of voice profiling in marketing and its dangers for society.

As a chair professor at the University of Pennsylvania's Annenberg School for Communication, I am the author of 11 books and over 160 articles about mass media industries and systems. My most recent book is *The Voice Catchers: How Marketers Listen In to Exploit Your Feelings, Your Privacy, and Your Wallet*, which Yale University Press published in May 2021.

The book explores the rise and growth of what I call "the voice intelligence industry" and its use of voice profiling in marketing. The industry involves such tools as smart speakers, car information systems, customer service calls, and "connected-home" devices like thermostats and alarms. When you talk, their "intelligent assistants" can draw inferences about you using analytical formulas generated by artificial intelligence. *The Voice Catchers* shows how companies are working to analyze people's vocal-cord sounds and speech patterns for information about their emotions, sentiments, and personalities characteristics, all so they can better persuade people, often in real time. Soon they may be able to draw conclusions about your weight, height, age, ethnicity, and more—all characteristics that scientists believe are revealed by your voice. Marketers will be able to score you as more or less valuable, show you different products based on that valuation, give you discounts treat you better or worse than others when you want help. In other words, marketers are using voice data to model ways to discriminate between you and others in unprecedently powerful ways. And all of this is happening without adequate regulations and safeguards to help American consumers understand the risks.

Based on voluminous research including extensive interviews of 44 industry participants, *The Voice Catchers* describes this developing biometric domain, explains how it's already influencing our lives, and shows what about it needs to be stopped. The book also shows how technologies honed through voice profiling in marketing could migrate (and in some cases are already migrating) to non-marketing areas such as political campaigns, immigrant evaluation, and phone-call surveillance of incarcerated people. And it considers that voice profiling is the leading edge of a future in which marketers could use other forms of biometric surveillance in conjunction with voice. Although voice profiling can have potentially beneficial uses in medicine and proper forms of security authentication, I argue that in marketing voice profiling and other forms of biometric profiling ought to be banned. Now is the time to promote perspectives and policies to derail the voice-based world of marketing biometrics—while the industry is still being built, and before socially corrosive processes linked to it become too entrenched to change.

Following is my op-ed essay published by *The New York Times* that expands on this letter by laying out with more specificity my policy concerns about voice profiling and the voice intelligence industry. The essay, and the book, have generated lots of discussion online and elsewhere.

I much appreciate your interest in this area, and I will be happy to provide more information if asked.

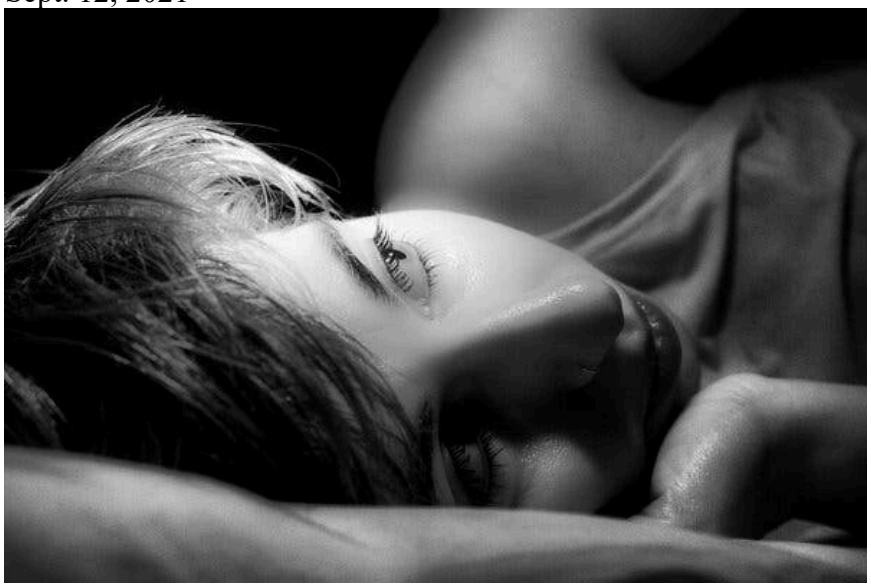
[redacted]

The New York Times
Opinion

Guest Essay

Hear That? It's Your Voice Being Taken for Profit.

Sept. 12, 2021



Credit...Devin Oktar Yalkin

• • • By Joseph Turow

Joseph Turow is a professor of media systems and industries at the University of Pennsylvania. He is the author of "The Voice Catchers: How Marketers Listen in to Exploit Your Feelings, Your Privacy, and Your Wallet."

If you've ever dialed an 800 number to ask or complain about something you bought or to make an inquiry about something you're thinking of buying, there is a decent chance you were profiled — by the arrangement of your words and the tone of your voice — without knowing it. My research suggests many customer contact centers now approach and manage callers based on what they think the person's voice or syntax reveal about the individual's emotions, sentiments and personality, often in real time.

Businesses devoted to personalized selling — including some name brand favorites — are also preparing to link what your vocal cords supposedly reveal about your emotional state to more traditional demographic, psychographic and behavioral information.

If during a call with a customer agent this biometric technology tags you as "tense," you may be offered a discount on your purchase, especially if the company's records also indicate that you're a big spender. Being identified as a certain type can also get you routed to a customer service representative whom the company believes works best with your presumed personality: maybe "logical and responsible" or "creative and playful," two such categories.

Company executives claim they are fulfilling their responsibility to make callers aware of these voice analyses by introducing the customer service interactions with an ambiguous sentence such as, "This call may be recorded for training and quality control purposes." But this legal turn of phrase is evidence of a growing threat that could turn our very voices into insidious tools for corporate profit.

It's not just call centers. Devices such as smart speakers and smartphones are now capturing both our words and the timbre of our voices.

Rohit Prasad, Amazon's chief Alexa scientist, told the online technology publication OneZero that "when she recognizes you're frustrated with her, Alexa can now try to adjust, just like you or I would do."

Soon companies may also draw conclusions about your weight, height, age, ethnicity and more — all characteristics that some scientists believe are revealed by the human voice.

Amazon and Google, the highest-profile forces in voice surveillance today, are not yet using the maximum potential of these tools, seemingly because they are worried about inflaming social fears. The technology is based on the idea that voice is biometric — a part of the body that can be used to identify and evaluate us either instantly or permanently. Businesses using this voice technology to offer us better pricing sounds great, unless you're in the camp that loses the discount. What if you end up being refused insurance or having to pay much more for it? What if

you find yourself turned away during early job screenings or have your cultural tastes prejudged as you surf the internet?

On Jan. 12, Spotify received an extraordinary patent that claims the ability to pinpoint the emotional state, gender, age, accent and “numerous other characterizations” of an individual, with the aim of recommending music based on its analysis of those factors. In May, a coalition of over 180 musicians, human rights organizations and concerned individuals sent Spotify a letter demanding that it never use or monetize the patent. Spotify claims it has “no plans” to do so, but the coalition wants a stronger disavowal.

I signed that letter but am also acutely aware that Spotify’s patent is just a tiny outcropping in the emerging voice intelligence industry. One of Google’s patents claims it can analyze the patterns of household movement via special microphones placed throughout the home and identify which resident is in which room.

Based on voice signatures, patented Google circuitry infers gender and age. A parent can program the system to turn electronic devices on or off as a way to control children’s activities. Amazon already claims that its Halo wrist band is able to identify your emotional state during your conversations with others. (The company assures device owners that it cannot use that information.) Many hotels have added Amazon or Google devices in their rooms. Construction firms are building Amazon’s Alexa and Google’s Assistant into the walls of new homes.

Major advertisers and ad agencies are already preparing for a not-too-distant future when extracting competitive value from older forms of audience data (demographics, psychographics, internet behavior) will, as one business executive told me, “start to plateau.” They too will turn to voice profiling “to create value.”

Ad executives I’ve interviewed also expressed annoyance that Amazon and Google do not allow them to analyze the words or voices of people who speak to the companies’ apps in Echo and Nest smart speakers. Some advertisers, without hard proof, worry that Amazon and Google are appropriating the voiceprints for their own use. Those concerns have led advertisers to start exploring their own ways to exploit customers’ voice signatures.

All these players recognize that we could be entering a voice-first era, where people will speak their instructions and thoughts to their digital companions rather than type them.

Because of recent major advances in natural language processing and machine learning, individuals will soon be able to speak conversationally not just to their phone assistant or smart speaker but to their dedicated bank assistant, kitchen equipment, restaurant menu, hotel room console, homework assignment or car.

In a way, much of this sounds incredibly cool — like we may finally be reaching the age of the Jetsons. These head-turning developments sound all the more exciting when some physicians and health care firms argue that a person's sounds may betray diseases such as Alzheimer's and Parkinson's. But these technologies are also worrisome because we engage a slippery slope whenever we start allowing the sounds of our voice and the syntax of our words to personalize ads and offers based on profit motives.

VICE reported that Cerence's chief technology officer told investors, "What we're looking at is sharing this data back with" automakers, then "helping them monetize it."

It could all seem like a small price to pay until you project out the use of this tech into the near future. An apparel store clerk uses an analysis of your voice to determine the likelihood of whether you can be sold certain clothing. You call a fancy restaurant for a reservation, but its voice analysis system concludes that you don't meet its definition of an acceptable diner and are refused. A school denies a student enrollment in a special course after voice analysis determines that the student was insincere about their interest in it.

How would such a future materialize? It all starts with users giving companies permission.

In our country today, only a few states have biometric privacy laws that require a company to obtain explicit consent from users. The European Union, however, demands opt-in consent, and it's likely that more states ultimately will adopt comparable laws. In its privacy policy, the social app TikTok claimed the right to collect users' voiceprints for broadly vague reasons, but as of June it also noted that only "where required by law, we will we seek any required permissions from you prior to any such collection."

These laws don't go far enough to stop voice profiling. Companies will gain customers' approval by promoting the seductive value of voice-first technologies and exploiting people's habit-forming tendencies and by stopping short of explaining how voice analysis will actually work.

Many people don't tend to think of nice-sounding humanoids as threatening or discriminatory, but they can be both. We're in a new world of biometrics, and we need to be aware of the dangers it can bring — even to the point of outlawing its use in marketing.

Joseph Turow is a professor of media systems and industries at the University of Pennsylvania. He is the author of "The Voice Catchers: How Marketers Listen in to Exploit Your Feelings, Your Privacy, and Your Wallet."

https://www.nytimes.com/2021/09/12/opinion/voice-surveillance-alexa.html#:~:text=12%2C%202021-,Joseph%20Turow%20is%20a%20professor%20of%20media%20systems%20and%20industries,of%20letters%20to%20the%20editor.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Joy Buolamwini

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Dr. Joy Buolamwini
Cambridge, MA
[redacted]

26 January 2022

Office of Science and Technology Policy
Executive Office of the President of the United States
Eisenhower Executive Office Building
1650 Pennsylvania Ave.
Washington, DC 20504

Re: Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, FR Doc. 2021–21975

Addressing Topics 2, 4, and 6(h)

In response to the Office of Science and Technology Policy's Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies, I, Dr. Joy Buolamwini, submit this comment to call attention to the increased adoption of biased and discriminatory biometric technologies without sufficient study and scrutiny, including for functions within the federal government which impact the lives of every American. The absence of effective public consideration prior to the adoption of such technologies has profound and disparate impacts. And as illustrated most recently by the behavior of a leading government contractor in the facial recognition industry,[1] the present state of affairs allows companies to make broad and unchecked claims to address concerns of bias, while in fact dismissing and distorting the science that informs these concerns.

In my scholarship, I have produced several peer-reviewed MIT studies demonstrating how commercial facial analysis systems exhibit, gender and skin type bias.[2] A landmark government report in the field,[3] has shown bias in facial recognition algorithms based on age, race, and gender.

---

[1] Tonya Riley, *ID.me CEO Backtracks on Claims Company Doesn't Use Powerful Facial Recognition Tech*, CyberScoop (Jan. 26, 2022), https://www.cyberscoop.com/id-me-ceo-backtracks-on-claims-company-doesnt-use-powerful-facial-recognition-tech/.

[2] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research 77 (2018); http://gendershades.org. Joy Buolamwini & Inioluwa Deborah Raji, *Actionable Auditing: Investigating the Impact of Publicly Naming Biasing Performance Results of Commercial AI Products*, 2019 Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society 429. https://dl.acm.org/doi/10.1145/3306618.3314244.

[3] *See generally* Patrick J. Grother, Mei L. Ngan, and Kayee K. Hanaoka, *Face Recognition Vendor Test Part 3: Demographic Effects*, NIST Interagency/Internal Report 8280 (Dec. 19, 2019), https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects.

This Office has requested comments on the "exhibited and potential harms" of biometric technologies, and in particular "[h]arms due to questions about validity of the science used in the system" and "harms due to disparities in effectiveness of the system for different demographic groups."[4] As noted in the literature cited above, there is a clear propensity for these biased AI systems failing disproportionately burdening women and BIPOC persons. The real-world impact on marginalized communities will likely get worse because of the unchecked proliferation of facial recognition technologies generally. These technologies are being deployed at an unprecedented rate across state and federal agencies. They are imposed on the public without sufficient public scrutiny, debate, or oversight, causing harm to the populous generally.

For example, a growing number of state and federal bodies have contracted with the company ID.me to verify the identity of persons seeking government benefits or services. ID.me primarily does this through facial recognition technology, but very little is publicly known about how this company's algorithms behave, or whether it suffers from the same bias as the other vendors analyzed in the literature above. And far from being transparent, ID.me has chosen instead to publish a whitepaper[5] that reveals little to the government or the public about the technology it employs. To show the shortcomings of this paper, I have attached an annotated version of this report to this comment, where I note numerous places where the report obfuscates technical terminology, misleads readers around the nature of these concerns, and summarily dismisses "university studies," including peer-reviewed research I conducted while at MIT, ostensibly in order to assure the public that it takes claims of bias seriously.[6]

The primary claim in the paper was that many of the concerns proven out by the literature only apply to what the paper calls "one to many" ("1:many") facial recognition technologies, and their technology is a "one to one" ("1:1") technology. This a mischaracterization of the literature. As the National Institute of Standards and Technology said in a 2019 study of this issue, "[f]or one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. False positives might present a security concern to the system owner, as they may allow access to impostors."[7]

---

[4] Off. of Sci. & Tech. Pol'y, *Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies*, 86 Fed. Reg. 56300, 56301 (Oct. 8, 2021).
[5] ID.me, Promoting Access, Equity, and Inclusion With AI and Digital Identity (2022), https://insights.id.me/wp-content/uploads/2022/01/IDme-Anti-Bias-Whitepaper.pdf.
[6] See Exhibit A, attached.
[7] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

And even under this strained dichotomy, ID.me now admits that it uses 1:many matching as a part of its service.[8]

And yet despite this lack of serious engagement with leading technical literature on bias in a range of facial recognition technologies, the IRS has announced that it will require use of ID.me for all access to online accounts. This places all Americans at the mercy of unverified and under-scrutinized algorithms, from a field whose algorithms are already known to have biased properties. The Office of Science and Technology Policy should advise against the adoption of these harmful and biased technologies and call for the dedication of more resources to develop standards for ensuring adequate transparency, public scrutiny, and oversight before procurement of facial recognition and other biometric technologies.

I thank this Office for its consideration of this comment, and I welcome any further discussion on these matters. If you have questions, please do not hesitate to contact me at [redacted].

Sincerely,
Dr. Joy Buolamwini

Ph.D. Media Arts and Sciences, Massachusetts Institute of Technology (2022)
MS. Media Arts and Sciences, Massachusetts Institute of Technology (2017)
MSc. Learning ad` Technology, University of Oxford, Distinction (2014)
B.S. C.. puter Science, Georgia Institute of Technology, Highest Honors (2012)

Dr. Joy Buolamwini is a computer scientist and poet of code who uses art and research to illuminate the social implications of artificial intelligence. She founded the Algorithmic Justice League in 2016 to create a world with more equitable and accountable technology. Her TED Featured Talk on algorithmic bias has over 1.4 million views. Her MIT thesis methodology uncovered large skin type and gender bias in AI services from companies like Microsoft, IBM, and Amazon. In 2020, these companies stepped back from selling facial recognition technology to law enforcement. In addition to advising elected officials during US congressional hearings, she serves on the Global Tech Panel to advise world leaders and executives on reducing AI harms. She is the spokesperson for Olay's #DecodeTheBias campaign appearing in September *Vogue* and on Good Morning America to raise awareness about the need for algorithmic justice.

[8] Riley, *supra* note 1.

Dr. Buolamwini's journey is depicted in the critically-acclaimed documentary *Coded Bias*, which sheds light on threats AI poses to civil rights and democracy. She has written op-eds on the impact of AI for publications like *TIME Magazine* and *New York Times*. Her spoken word visual audit "AI, Ain't I A Woman?" which shows AI failures on the faces of iconic women like Serena Williams, Oprah Winfrey, and Michelle Obama, has been part of exhibitions ranging from Ars Electronica to The Cooper Gallery at Harvard Square. A Rhodes Scholar and Fulbright Fellow, Dr. Buolamwini has been named to notable lists including *Forbes'* 30 under 30, *Ebony* 100 Powerlist, *Bloomberg*50, *Time* Next 100, *Fortune Magazine* named her "the conscience of the AI revolution." She is the first Black researcher to grace the cover of *Fast Company*, appearing in the 2020 "Most Creative People" issue. She holds graduate degrees from Oxford University and MIT; and a bachelor's degree from the Georgia Institute of Technology. A former pole vaulter, she still holds sentimental Olympic aspirations.

Exhibit A

ID.~~me~~ no

Promoting ~~Access, Equity, and Inclusion~~ cherry-picking omission With AI and Digital Identity

Dr. Joy Buolamwini | Annotations

We must make sure that the federal government does not adopt vendors who omit important and relevant findings concerning the technologies they sell or the harms they risk. ID.me's failure to cite the research they critique prevents others from drawing their own conclusions about the technical precision of that research which undermines the company's trustworthiness. More importantly, ID.me uses the experiences of people with disabilities to justify the adoption of biometric technologies, which masks the harms that such technologies pose to marginalized communities.

Executive Summary

As the COVID-19 pandemic accelerated the transition to digital and the rapid at-scale adoption of evolving technologies, questions emerged about equitable access to government benefits and services. Two such technologies under scrutiny are facial recognition and face match for remote identity verification.

The Difference Between Facial Recognition and Face Match

Facial recognition is a precise technical term used by organizations such as the National Institute of Standards and Technology (NIST). There are two distinct types of facial recognition: 1:many and 1:1, and they are frequently conflated. Media reports and even university studies often fail to distinguish between them correctly. For ease of understanding in this paper, we will refer to them as 1:many facial recognition and 1:1 face match. Simply put, 1:1 face match is equivalent to an airport agent comparing your face to the photo on your government ID card. 1:many facial recognition is equivalent to giving your picture to the same agent, putting him on stage at a rock concert, and asking him to pick your face out of the crowd. With millions of possible matches, the challenge of finding the right face increases measurably.

	1:Many Facial Recognition	1:1 Face Match
Compares your face only to the photo on your government ID	✗	✓
Is included in the National Institute of Standards and Technology Identity Assurance Level 2 (NIST IAL2)	✗	✓
Widely adopted by tens of millions of Americans using Android and iPhones	✗	✓

ID.me does not use 1:many facial recognition.

Face Match Benefits Include Equity and Justice for Identity Verification

Research shows that the most equity-enhancing way to use those technologies for remote identity verification combines best-in-breed algorithms with human-in-the-loop relief valves. That research includes detailed testing by NIST, independent assessments of facial-recognition and face-match vendors, and tests of our own orchestration platform.

Face match also helps bring justice for those who have been exploited. The paper details a case involving a caregiver attempting to steal the identities of people with disabilities to file for Pandemic Unemployment Insurance. Due to adherence to NIST IAL2, the caregiver was escalated to a Trusted Referee, who perceived the fraud and alerted the state.

Facial recognition technologies as defined by the Federal Trade Commission include a set of technologies that process imaging data to perform a range of tasks on human faces, including detecting a face, identifying a unique individual, and estimating demographic attributes.

https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf

Using people with disabilities to justify the proliferation of biometric technology before there is sufficient public scrutiny, debate, and oversight in determining its adoption is not equitable or just.

Key Takeaways

Four key takeaways are covered in detail in this paper:

- ✔ **Facial recognition and face match are frequently misunderstood** – Media reports and even university studies often fail to use precise terminology, leading to confusion among readers

  Which peer-reviewed university studies fail to use precise terminology? Which readers are confused?

- ✔ **Leading algorithms perform more equitably** – The best facial-recognition algorithms perform more equitably across demographic groups for 1:1 face match, such as an application in which a user is attempting to verify identity

  More equitable as compared to what? How do all algorithms perform overall?

- ✔ **Human reviewers and in-person verification control for any potential bias** – Peer-reviewed scientific studies show the best face-match results are achieved by fusing computer-based and human-driven facial recognition

  Meanwhile...

- ✔ **There are significant benefits to artificial intelligence (AI) and 1:1 face match that can be captured when implemented correctly** – AI and 1:1 face match can stop identity theft at scale, help state workforce agencies process legitimate claims faster, deter fraud, recover accounts easier, and bring justice for those who have been exploited

There are significant risks and harms that arise from AI and 1:1 face verification that can deny individuals access to government benefits, undue scrutiny, time wasted seeking to clear name of erroneous fraudulent or other criminal accusations, and more.

According to the National Institute of Standards and Technology (NIST):

"For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians.

The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. False positives might present a security concern to the system owner, as they may allow access to impostors."

https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

Robert Williams was falsely arrested even with the use of human reviewers who looked at face matches produced from a facial recognition product used by police. ID.me attempts to use "face match" to distance themselves from facial identification. Yet face matches are used in facial identification processes that include humans-in-the-loop that have failed. Mr. Williams was detained for close to 30 hours after being arrested in front of his two young daughters based on decisions informed by erroneous face matches.

https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/

ID.me

Yes, facial recognition is frequently misunderstood and definitions are used by some vendors to evade accountability and scrutiny.

After stating facial recognition has two distinct types (1:1 verification and 1:many identification), ID.me then uses facial recognition to only mean identification.

As a term of art, face matches are used in both verification and identification processes.

ID.me fails to use the precise technical definition of 1:1 facial recognition while claiming others conflate technical terminology. This shows the imprecise nature of terminology used by some vendors, even ones verified by the United States government.

For more information on a range of facial recognition technologies, visit primer.ajl.org.

Introduction

As services and transactions increasingly move online and the economy becomes ever more digital, we have an enduring obligation to ensure everyone has the opportunity to participate. ID.me makes that real with our "No Identity Left Behind" initiative, a fundamental commitment to equity and access. Equity is why we do what we do. This paper shares insights on the application of AI and facial recognition in identity proofing at NIST SP 800-63-3 IAL2. IAL2 is the federal standard that defines required and suggested controls for authenticating consumers for high-risk services. Examples include:

- **Authenticating individuals for access to taxpayer services**
- **Enabling individuals to apply for unemployment benefits**
- **Empowering consumers to access health care records in the public and private sectors**

Equity with respect to AI and facial recognition can be difficult to parse because there are many different applications of the technology and scrutiny on how law enforcement, in particular, uses it. Still, it is crucial to unpack how AI affects individuals from various communities and demographics as they attempt to access vital government programs. Given that AI and facial recognition can automate many workflows – enabling faster service delivery – the empirical data and truth must win over false perception.

Findings from a 2019 NIST report on facial recognition are important for policymakers because those findings relate to NIST SP 800-63-3 IAL2. Understanding how the leading facial recognition algorithms affect equity and access in the context of NIST 800-63-3 can help policymakers understand if IAL2 requirements are equitable. That is vital to ensure optimal policies for equity and access and so the public understands the controls that are used.

Understanding how all 189 facial recognition algorithms evaluated in the 2019 NIST report perform gives policymakers a comprehensive view about the overall state of play, not just the algorithms that support marketing materials. Omitting key findings from the NIST report can undermine the perceived trustworthiness of ID.me to both policymakers and the general public.

The best available research and data on those topics paint a clear and hopeful picture:

- **The leading algorithms show extremely high accuracy across all demographics in IAL2 flows**

  Yet it appears leading algorithms may have played a role in false arrests? How can that be?
- **ID.me internal tests across 15,468 images show no detectable bias tied to skin type**

  Third-party validations of these findings are needed as well as a full phenotypic and demographic breakdown of findings.
- **Mitigating controls – such as human reviewers and in-person verification – control for any potential bias**

  And yet human reviewers have nonetheless been tied to wrongful arrests. Potential bias? Why not talk about the bias recorded in the 2019 NIST Report?

ID.me

"No identity left behind"

or

"No face left alone?"

The ideal cases shared by vendors often do not address what can go wrong.

Using ID.me could risk:

(i) Individuals being denied speedy access to taxpayer services,

(ii) Individuals being denied the ability to apply for unemployment benefits unencumbered, and

(iii) Individuals denied access to health care records in the public and private sectors.

The ID.me NIST IAL2 solution uses leading algorithms as validated by NIST and NIST-accredited laboratory testing. ID.me also employs two sets of human reviewers to check the technology's decision when AI denies access in the self-serve flow. That hybrid approach enables the leading algorithms, which are more accurate and less biased than trained humans,[1] to streamline access while mitigating any risk of bias.

The remainder of this paper goes beyond the headlines, unpacks the science, and explains:

- ✓ **An overview of the 2019 NIST Face Recognition Vendor Test (FRVT)**
- ✓ **The difference between 1:1 face match and 1:many facial recognition and why it matters**
- ✓ **The critical difference between a false positive and a false negative**
- ✓ **Confusion about facial recognition and pass rates by gender**
- ✓ **NIST's findings on the highest-quality algorithms**
- ✓ **How ID.me uses those findings and Trusted Referees to enhance equity in identity verification**

The remainder of this paper also:

- ✗ **Omits findings from the 2019 NIST FRVT Report that show substantial evidence of demographic effects on the basis of age, gender, and race.**
- ✗ **Omits citations to sources that would allow the veracity of claims that "MIT research" conflates technical terminology to be externally assessed.**
- ✗ **Omits the 2020 Association for Computing Machinery ACM statement on the present state of facial recognition technology. The ACM is the the world's largest educational and scientific computing society. It provides the computing field's premier Digital Library and serves its members and the computing profession with leading-edge publications, conferences, and career resources.**

1 Crumpler, William, How accurate are Facial Recognition Systems - and Why Does It Matter?, Center for Strategic & International Studies https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter

688

ID.me

June 30, 2020

"The ACM U.S. Technology Policy Committee (USTPC) has assessed the present state of facial recognition (FR) technology as applied by government and the private sector.

The Committee concludes that, when rigorously evaluated, the technology too often produces results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems.

The consequences of such bias, USTPC notes, frequently can and do extend well beyond inconvenience to profound injury, particularly to the lives, livelihoods and fundamental rights of individuals in specific demographic groups, including some of the most vulnerable populations in our society. Such bias and its effects are scientifically and socially unacceptable.

For both technical and ethical reasons – pending the adoption of appropriately comprehensive law and regulation to govern its use, oversee its application, and mitigate potential harm – USTPC urges an immediate suspension of the current and future private and governmental use of FR technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights."

https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf

ID.me fails to provide even one citation for the claim university studies often fail to use precise terminology.

Studies Dr. Buolamwini has led relating to gender classification delineate that future work is needed on facial verification 1:1 matching and facial identification 1:many matching. NIST answered that call and reports demographic effects on the basis on age, race, and gender.

The titles of her studies specify the types of models evaluated

2017 MIT Masters Thesis:

"Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers"

https://www.media.mit.edu/publications/full-gender-shades-thesis-17/

2018 Peer-Reviewed Paper:

"Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification"

https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

2019 Award Winning Peer-Reviewed Paper:

"Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products"

https://dl.acm.org/doi/10.1145/3306618.3314244

An Overview of the 2019 NIST FRVT

In 2019, NIST conducted a study of more than 189 commercial algorithms from 99 developers to quantify the accuracy of facial-recognition algorithms for different demographic groups. Notably, many of those algorithms were immature and submitted by universities for research purposes. Test results from those algorithms should not be conflated with the performance of leading algorithms or algorithms actually used by IAL2 vendors.[2]

The results were based on a dataset of more than 18 million images of 8.5 million individuals. Key findings include[3]:

- **Algorithms perform differently:** The results show a wide range in accuracy across developers. The best performers produce "many fewer errors" than less-mature algorithms. Mature algorithms can therefore be expected to have smaller demographic differentials.
- **Demographic effect is vanishingly small:** False negatives – when a legitimate person's selfie fails to match a reference photo of his or her face – occur at extremely low rates across demographic groups. That is particularly important because a false-negative error would deny a legitimate person access.
- **Leading algorithms perform more equitably:** The best facial-recognition algorithms perform more equitably across demographic groups for 1:1 face match in scenarios when a valid user is attempting to pass. False-negative errors, which block valid people, are usually remedied on a second attempt.
- **Confusion about bias abounds:** Media reports and even university studies often fail to use precise terminology and, as a result, negatively skew the public discourse. For example, studies on gender, which related to face-classification algorithms, were falsely conflated with facial recognition, which looks for similarity.

What does that mean to organizations seeking to leverage those technologies to provide secure, equitable services? In short, they should understand how performance varies across types of algorithms (for example, 1:1 vs. 1:many), they should adopt only the highest-performing algorithms, and they should take action to mitigate known and potential performance limitations and errors. The sections that follow provide insights into how to take those actions to increase access, equity, and inclusion in digital identity.

2 IAL2 vendors should disclose the specific algorithms they are using to certifying bodies so they can be evaluated for equity and inclusion.

3 Grother, Patrick; Ngan, Mei; and Hanaoka, Kayee. Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects, 2019, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

IMPORTANT NIST REFERENCE ON FALSE POSITIVES

https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

ID.me

Also from the 2019 NIST FVRT are less favorable observations.

"For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. False positives might present a security concern to the system owner, as they may allow access to impostors."

"Among U.S.-developed algorithms, there were similar high rates of false positives in one-to-one matching for Asians, African Americans and native groups (which include Native American, American Indian, Alaskan Indian and Pacific Islanders). The American Indian demographic had the highest rates of false positives."

"For one-to-many matching, the team saw higher rates of false positives for African American females. Differentials in false positives in one-to-many matching are particularly important because the consequences could include false accusations. (In this case, the test did not use the entire set of photos, but only one FBI database containing 1.6 million domestic mugshots.)"

https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

The Difference Between 1:1 Face Match and 1:Many Facial Recognition and Why It Matters

Let's clarify why there are more errors tied to more complex use cases. 1:1 face match is equivalent to an airport agent comparing your face to the photo on your government ID card. 1:many facial recognition is equivalent to giving your picture to the same agent, putting him on stage at a rock concert, and asking him to pick your face out of the crowd. With millions of possible matches, the challenge of finding the right face increases measurably.[4] Face match tied to NIST IAL2 deals specifically with 1:1 matching. The goal is to avoid a false negative so legitimate people are able to gain access. An additional goal is to avoid a false positive so an identity thief is unable to claim a different person's identity. That is a simplistic use case in the context of advanced technology.

1:Many Facial Recognition

1:1 Face Match

With more than 129 million Android smartphones and 113 million iPhones in use in the U.S.,1:1 face match is already widely adopted by tens of millions of Americans. It has been proven at scale. *False negatives* occur when the technology fails to match the same person from the FaceID enrollment photo to the image captured during a specific attempt to unlock the phone. Apple and Android manufacturers allow for additional attempts and then prompt the user for a PIN if repeated attempts fail. While that content isn't covered by the 2019 NIST report directly, it provides a helpful frame to interpret the results of the study and how leading companies introduce additional controls to provide access pathways in the event AI doesn't perform as intended.

4 NIST benchmarks FPIR for 1M+ databases at 0.001, which is much higher than 1e-6 for 1:1,. but still excellent for many use cases.

The Difference Between False Positives and False Negatives

False-positive errors occur when two faces look similar but do not belong to the same person. Those errors are often embarrassing when humans make them in social interactions, such as mistaking a stranger for a friend. A false-negative scenario might involve failing to recognize an old friend you went to school with years ago.

False positives are much more common in 1:many facial-recognition scenarios. They are far less common in 1:1 face matching. After all, what are the odds that a person who steals your wallet looks just like you?

False Negative – Algorithm Fails to Match Two Images of the Same Person's Face

False Positive – Algorithm Incorrectly Matches Two Faces That Aren't the Same Person

When verifying identity for government benefits, false negatives would be associated with denying access to a person who is the same as in the government ID photo. The NIST report shows that false-negative errors are vanishingly small across demographic groups. To the extent false-negative errors occur across all algorithms, false-negative errors are actually lower in darker skin tones for 1:1 matching under certain conditions. Keep in mind, false negatives can often be remedied by trying a second time, as NIST notes.

The errors related to false positives are most relevant for fraud and unauthorized access. Those errors would not relate to legitimate people getting blocked from their rightful benefits, but rather to a criminal gaining unauthorized access. The NIST report notes "false positive differentials are much larger than those related to false negatives and exist broadly, across many, but not all, algorithms tested." While that is relevant for 1:many anti-fraud scenarios, **the false-negative rate is the key metric in 1:1 identity verification as it deals with blocking a valid person.**

If the concern is fraud, false-positive rates for 1:1 identity verification also matter. A false positive match could enable someone else to claim your benefits. NIST's Patrick Grother explicitly talks about the implications of false positives for one-to-one matching as seen in the quotes on the right panel. Why is ID.me dismissing false-positive rates, where NIST has shown high rates of false positives for Asians and African Americans as compared to Caucasians? According to the NIST report US algorithms had the highest false-positive rates on the Americans Indian demographic.

Seperately, what constitutes darker skin tones? The NIST study did not use phenotypic skin type analysis but instead demographic racial categories. Skin types and their related skin tones are not stable across racial categories. See Section 7.3.3 and 7.3.4 of Dr. Buolamwini's 2017 MIT Master's Thesis.

ID.me

Why are False Positive Metrics from NIST Omitted?

As noted above, according to the National Institute of Standards and Technology (NIST):

"For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. False positives might present a security concern to the system owner, as they may allow access to impostors."

"Among U.S.-developed algorithms, there were similar high rates of false positives in one-to-one matching for Asians, African Americans and native groups (which include Native American, American Indian, Alaskan Indian and Pacific Islanders). The American Indian demographic had the highest rates of false positives."

"For one-to-many matching, the team saw higher rates of false positives for African American females. Differentials in false positives in one-to-many matching are particularly important because the consequences could include false accusations. (In this case, the test did not use the entire set of photos, but only one FBI database containing 1.6 million domestic mugshots.)"

https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

The NIST report highlights three additional findings related to error rates:

- **False negatives** are often remedied by the user attempting a second time
- **False-negative rates** are extremely low across demographic groups
- **False-negative errors** tend to be algorithm specific

ID.me appears to be conflating the phenotypic attribute of skin tone with the demographic attribute of race.

The Difference Between Face Classification and Facial Recognition and How They Perform Across Genders

The 2019 NIST report addressed confusion in the market about facial-recognition versus facial-classification algorithms as they relate to pass rates across genders. The excerpt from the NIST report that highlights the confusion, and how it affects perceptions of bias, follows with bolding added for emphasis by ID.me:

"Over the last two years there has been expanded coverage of face recognition in the popular press. In some part this is due to the expanded capability of the algorithms, a larger number of applications, lowered barriers to algorithm development, and, not least, reports that the technology is somehow biased. This latter aspect is based on Georgetown and two reports by MIT. The Georgetown work noted prior studies articulated sources of bias, and described the potential impacts particularly in a policing context, and discussed policy and regulatory implications. **The MIT work did not study face recognition, instead it looked at how well publicly accessible cloud-based estimation algorithms can determine gender from a single image. The studies have been widely cited as evidence that face recognition is biased.**

This stems from a confusion in terminology: Face classification algorithms, of the kind MIT reported on, accept one face image sample and produce an estimate of age, or sex, or some other property of the subject. **Face recognition algorithms, on the other hand, operate as differential operators:** They compare identity information in features vectors extracted from two face image samples and produce a measure of similarity between the two, which can be used to answer the question 'same person or not?'. Face algorithms, both one-to-one identity verification and one-to-many search algorithms, are built on this differential comparison."[5]

For a more comprehensive explanation of the terminology in question, visit primer.ajl.org

5 Grother, Patrick; Ngan, Mei; and Hanaoka, Kayee. Introduction, page 14. Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects, 2019, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

ID.me

The MIT work referenced by NIST includes the 2017 Buolamwini Thesis and the 2019 Raji and Buolamwini peer-reviewed paper. Neither study claims to evaluate face recognition. How news media covers academic research is not always reflective of how authors of academic studies frame or understand their work.

As stated in the 2017 MIT Thesis page 96: "This thesis focused on the diversity of benchmark datasets and the performance of gender classification algorithms in regard to gender and skin type. Future work is needed to advance scholarship on dataset representation and intersectional evaluation of algorithms not limited to gender classification."

https://www.media.mit.edu/publications/full-gender-shades-thesis-17/

As stated in the 2019 peer-reviewed paper page 5:

"Given a clear understanding of the Gender Shades study procedure and follow up audit metrics, we are able to reflect on corporate reactions in the context of these results, and evaluate the progress made by this audit in influencing corporate action to address concerns around classification bias."

https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf

ID.me (correctly) points out the gender classification differs from facial verification. This is important because the metrics like error rates that measure performance for gender classification and and false-non-match rate for facial verification differ. Observations of gender classification metrics raised concerns about facial recognition metrics. The 2019 NIST report shows those concerns were warranted.

The NIST report goes on to compare false-negative rates of the 52 most accurate recognition and matching algorithms to the classification algorithms in the MIT study: The best algorithms "almost always gives (sic) false-non-match rate (FNMR) below 1%. These error rates are far better than the gender-classification error rates that spawned widespread coverage of bias in face recognition. In that study, two algorithms assigned the wrong gender to black females almost 35% of the time. The recognition error rates here, even from middling algorithms, are an order of magnitude lower. Thus, to the extent there are demographic differentials, they are much smaller than those that (correctly) motivated criticisms of the 2017-era gender classification algorithms."[6]

The NIST authors chose to compare their results with the 2017 MIT Thesis instead of the more up-to-date 2019 peer-reviewed paper that they also cite. The 2019 paper recorded an error rate near 35% for Amazon Rekognition's gender classification feature as it related to darker-skinned females. It is unclear why the NIST report does not reference the more recent study though it cites that study in the motivation section of the paper.

If we use the 2017 MIT Thesis as a reference, error rates are simply calculated as the percentage of subjects in a category assigned a label that does not match the ground truth annotations provided for a given image. As such, errors would include false positives and false negatives. Why does this matter? Well, when we look at false positive rates relating to one-to-one matching, the NIST report overview had the following to say:

"For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians."

"The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. False positives might present a security concern to the system owner, as they may allow access to impostors."

The omission of such key findings from the NIST report in this "anti-bias" white paper is extremely concerning, especially because this white paper purports to help policymakers better understand a complex range of facial recognition technologies.

For a more comprehensive explanation of different facial recognition technologies and associated metrics, visit primer.ajl.org.

693

ID.me

Here, there is a conflation of skin type and race. The Gender Shades studies did not evaluate race but instead evaluated skin type using the Fitzpatrick Skin Phenotype classification system. The findings have implications for race, yet if the argument is the need for precision when speaking about research studies, conflating a phenotypic attribute with a demographic attribute creates confusion for some readers.

Performance metrics used for gender classification and those used for facial recognition are different.

As ID.me notes above, the tasks of gender classification and facial verification are indeed different and so are the performance metrics used to evaluate them.

6 Idib. Page 54.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Joy Mack

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

RFI Response: Biometric Technologies

I am Joy Mack. I am responding to your Request as a citizen; member of the public. 01/15/2022

1. I desire to share my experience, my suffering; about the nefarious use of artificial intelligence, biometric, Facial Recognition Technologies (herein after FRT), and other technology type systems.

2. I am a victim of extra judicial punishment; on a type of black list Watch List and Kill List.

{I inadvertently exposed misconduct at the [redacted] County Courthouse. A ruse or scheme that they do all the time did not go as planned. To shield the misconduct; and to keep the public from knowledge of how they operate; I have been placed in a retaliatory take down program, of trauma based conditioning, discrediting and stigma.}

3. Because I am being denied information, hearings; due process rights; for the First, Fourth, Fifth, and Fourteenth Amendment violations directed against me - in these clandestine operations; it is from this perspective that I hope your office can best served the public.

4. Although my limited statement reference a fraction of what is happening to me; millions of unwitting Americans throughout the United States endure the same suffering.

5. My personal experience is that the Biometric Technologies are weaponized and used as systems of oppression. In fact; that is why it is so difficult to guard or protect against it.

6. Hitler and his Collaborators used types of systems without today's technology; and destroyed the lives of millions in the process.

7. The basis, studies of algorithms technologies should be exposed as Systems of Surveillance even if not specifically used in law enforcement.

8. Through the use of artificial Intelligence / biometric technologies; I suffer continuing and ongoing harassment, retaliation and surveillance. These clandestine system of operations / technologies;

has created a platform which encourages emotional, financial, physical devastation without ever touching the person.

9. The Office of Science and Technology should first look within the federal, state, and local agencies for abuse and misuse.

10. The governments collection of personal information about the everyday John or Jane Doe; allows 'it' to know more about the person than they know about themselves?

11. Further; these agencies weaponized my personal information; place people like me into their research apparatus to test their technologies without my knowledge or consent, and without exposing the suffering it cause.

12. At this writing; when I think of things like the use of google maps; that is good. Yes, there are others. But; it is difficult for me to think of positive application on my life; because of the continuing and ongoing warfare directed against me in the use these technologies.

MY VIEW: (as to what has happened to me)

13. The algorithm systems is a connection to or a tie into the drag net collection of personal data, metadata etc.; weaponized with intent to assault the psyche, frustrate, cause fear, intimidate, ridicule, control behaviors chill speech.

14. Algorithms systems are capable and intended to neutralize the population. Algorithms set up triggers and people exposed to these triggers are clueless the triggers exist. They can incite to cause harm to others or even to themselves.

15. Back in the 1990's; the Miami Dade County was experiencing high rate of assaults and other crimes against tourist. What they found was that the rental vehicles had a certain numbering system on the Vehicle Plate which made tourist easy targets. Upon information and belief; the State of Florida / Miami Dade County/ changed this system of identifying rental vehicles so to assist to make tourist safe.

16. Well for the years of my surveillance; a similar type system is being used to punish me. I hear similar complaints from others throughout the United States.

17. I have noticed a numbering pattern to the vehicles that track and harass me no matter where I am on this earth;

18. I notice the computer internet pass when I go to the public libraries. The only way this can take place is with algorithms which will be implemented and used to track every person in the United States.

19. Algorithms used in these clandestine operations strips people of Fundamental Rights and thereby denies rights people don't even know are affected.

20. Algorithms Systems force arbitrary capricious applications, creates discriminatory intent, invades privacy, can be and is being used as a system of extra judicial punishment including psychological warfare and can and will be used to ostracize (blacklist) others; further it creates a bigger divide in a nation which boast diversity.

21. Even with an alleged Bill Of Rights; there is no check list or process with the authority to stop it/shut down systemic use.

22. A person cannot attribute what is happening to them via algorithms.

In fact; in Congressional Hearings held within the past two years; the Federal Bureau Of Investigations alleged that safeguards are in place and alleged these systems are not being abused. **That's untrue**.

23. Of course you would not recognize what is happening to me. You are not familiar with the people I know. In fact when the nefarious use of FRT first started happening to me years ago; I was flabbergasted.

24. I would be at some location and here comes a person who looks like someone I know or someone in my family. But these situations were intended and presented as orchestrations to cause fear, intimidate, ridicule, control my behavior, and chill my speech.

25. It was not until years and years later that I became aware of the technology and I then realized how they were abusing FRT. Such use is shocking, unconsciousable and the idea to use the technology in this manner against people is beyond the imagination; of any person who respects the rights of others. There should be penalties for nefarious use of technologies.

26. I created a website placing a 'few' of the pictures that I could retrieve; in my effort to show algorithm systems / Facial Recognition Technology being used against me.

I only show one or two instances in my website but the pattern of conduct directed against me and the system of algorithms used is what gives it – its power and thus make it debilitating. These patterns of conduct are continuing and ongoing.
See my Gallery in: [redacted]

27. And if a person make any effort to complain on the nefarious us of Facial Recognition Technology; they risk being called delusional, placed in handcuffs and taken away. This is the evil side of the **FRT** that has not been exposed and no one is talking about.

28. Back in the 1990's; the Miami Dade County was experiencing high rate of assaults and other crimes against tourist. What they found was that the rental vehicles had a certain numbering system on the Vehicle Plate which made tourist easy targets and upon information and belief; the State of Florida / Miami Dade County/ changed this system of identifying rental vehicles.

29. Well for all the years and years of surveillance; a similar type system is being used to punish me. Numbers unique to my life has been weaponized and replayed over and over and over in my daily liberties.

30. There is no system in place for redress of these technologies. I would be amazed to see efforts to address such issues which will include federal, state, and local agencies.

31. It is my hope that in you efforts to find alleged **iterative safeguards** against anticipated and unanticipated misuse or harms; I pray that you will consider First, Fourth, Fifth, and Fourteenth Amendment Constitutional and privacy rights provisions in your efforts.

RE: ***RFI Response: Biometric Technologies***

Joy Mack
[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Karen Bureau

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Cc: [redacted]
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Thursday, November 18, 2021 5:20:25 PM

I am writing today to bring your attention to the harmful use of GPS/BIOMETRICs in Electronic Visit Verification in Medicaid based in home health care visits. As a person with a disability who will be negatively affected by EVV, I am advocating for the banning of GPS/biometric data gathering being used as a way to penalize people with disabilities who require assistance with Activities of daily living.

Karen Bureau

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Lamont Gholston

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI; [redacted]
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Saturday, January 15, 2022 4:06:42 PM

Dental biometric techniques are reliable sources of human identification. These hard tissue landmarks and array of hard tissues are under genetic control. This method of tissue mapping captures the curvilinear 'footprint' of the dentoalveolar complex. The human dental arch form has a demonstrated descriptive and taxonomic value (Sanin, 1970; Biggerstaff, 1972; Pepe,1975; Lavelle, 1978; Felton, 1987; Gholston, 1990; Ferrario, 1993,1994).
Dental biometrics differ from the procedures of forensic dentistry and the attempted tooth contour mapping of
Jain (2009).

When fully developed, and implemented, these dental biometric procedures could assist the work of the
military, the State Department and Homeland Security in confirming individual identities. The shape of the human dental arch is as unique as fingerprints. This dental biometric technique requires no x-rays or blood.

Warmest regards,

Lamont Gholston, DMD, MPH, MSD
Jan. 15, 2022
[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Lawyers' Committee for Civil Rights Under Law

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

[redacted]

January 15, 2022

Dr. Eric S. Lander, Science Advisor and Director
Office of Science and Technology Policy, Executive Office of the President
1650 Pennsylvania Avenue
Washington, DC 20504
BiometricRFI@ostp.eop.gov

RE: RESPONSE TO RFI ON BIOMETRIC TECHNOLOGIES

Dear Director Lander,

The Lawyers' Committee for Civil Rights Under Law (LCCRUL) is pleased to submit these comments in response to the White House Office of Science and Technology Policy (OSTP) request for information on "Public and Private Sector Uses of Biometric Technologies."[1] The LCCRUL is a nonpartisan, nonprofit organization whose mission is to secure equal justice for all through the rule of law, targeting in particular the inequities confronting Black Americans and other racial and ethnic minorities. The LCCRUL was formed in 1963 at the request of President John F. Kennedy to mobilize the private bar to combat racial discrimination and the resulting inequality of opportunity – work that continues to be vital today.

Thank you for the opportunity to build the record on the use of these technologies and how they fit into national policymaking on AI and equity.[2] As you and Deputy Director Nelson recently wrote while announcing this project, "[W]e need a 'bill of rights' to guard against the powerful technologies we have created" which may include "the federal government refusing to buy software or technology products that fail to respect these rights [and] requiring federal contractors to use technologies that adhere to this 'bill of rights.'"[3]

We write to provide guidance on the application of Title VI of the Civil Rights Act of 1964 to the use of biometric technologies by federal agencies and the recipients of federal funds. Title VI prohibits the use of federal funds for programs and activities that discriminate on the basis of race or national origin.[4] Consequently, the federal government and recipients of federal funds are prohibited from using technologies that either intentionally discriminate or produce discriminatory disparate impacts.[5] Many biometric and algorithmic technologies, such as facial recognition, have been shown to result in, or have the potential to result in, such discrimination.

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56300-02 (Oct. 8, 2021).
[2] The White House, *Join the Effort to Create a Bill of Rights for an Automated Society* (Nov. 10, 2021), https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.
[3] Eric Lander and Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED (Oct. 8, 2021), https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.
[4] 42 U.S.C. § 2000d.
[5] *See* U.S. DEP'T OF JUSTICE, CIVIL RIGHTS DIV., TITLE VI LEGAL MANUAL, SECTION VII: PROVING DISCRIMINATION – DISPARATE IMPACT, https://www.justice.gov/crt/fcs/T6Manual (2021). (hereinafter Title VI Legal Manual).

[redacted]

Moreover, even if a tool is facially neutral that does not mean it is incapable of harm. No matter how complex biometric and algorithmic technologies are, they are just tools in the hands of those who wield them. When a technology is used to make a discriminatory system more efficient, that is a discriminatory use of the technology because it increases the quantity or quality of harm. Federal law requires that these technologies be used only in a nondiscriminatory manner.

We urge OSTP to incorporate the federal government's legal obligations under Title VI as it develops policy recommendations for biometric and algorithmic technologies.

Below, we discuss (I) the legal requirements of Title VI, and (II) examples of some technologies whose use may violate Title VI, such as facial recognition and behavioral recognition.

I. Title VI prohibits federal dollars from funding programs that either intentionally discriminate or have a disparate impact on protected classes.

Title VI states, "No person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving [f]ederal financial assistance."[6] This prohibition on discrimination applies to both intentional discrimination and practices that result in unfair disparate impacts. Every federal agency is obligated to ensure that their programs—and recipients of their funding—comply with Title VI.[7]

The Department of Justice (DOJ) has assembled a comprehensive manual for agency guidance on Title VI. This manual explains the legal principles behind federal agency Title VI enforcement as well as legal criteria agencies should use to determine Title VI compliance with agency action.[8] Such guidance assists federal agencies with ensuring that they enforce rules to (A) prohibit intentional discrimination and (B) withhold funding from programs that result in intentional discrimination or a disparate impact.

A. Title VI prohibits intentional discrimination and practices that result in unfair disparate impacts.

Title VI outright bans federal funding for discriminatory programs, including those that are intentionally discriminatory as well as those that create discriminatory disparate impacts. When determining if a program is intentionally discriminatory, the Supreme Court has indicated that one must show that an entity adopted a policy "because of" not merely "in spite of" its adverse effects upon an identifiable group.[9] In determining disparate impact, "Title VI regulations prohibit practices having a discriminatory effect on protected groups, even if the actions or

[6] Civil Rights Act of 1964 § 601, 42 U.S.C. § 2000d (1964).
[7] 42 U.S.C. § 2000d-1.
[8] *See* TITLE VI LEGAL MANUAL, *supra* note 3.
[9] *Id.* (quoting *Personnel Adm'r of Mass. v. Feeney*, 442 U.S. 256, 279 (1979)).

practices are not intentionally discriminatory."[10] Unlike intentional discrimination, a disparate impact results where a particular program may not have been designed with a discriminatory purpose, but has a disproportionate adverse effect on protected groups.[11] The DOJ notes that establishing adverse effect for a disparate impact claim is generally a "low bar" given the wide range of harms, such as "physical, economic, social, cultural, and psychological" harms.[12]

Disparate impact analyses proceed in three steps.[13] A *prima facie* disparate impact claim requires demonstrating that a facially neutral policy is discriminatory in practice. Upon such a showing, the burden shifts to the funding recipient to provide a "substantial legitimate justification" for the policy or practice. If the recipient can provide this, the practice may still be unlawful if an "equally effective alternative practice" would yield less discriminatory results or if the recipient's "legitimate practices are a pretext for discrimination."[14]

B. Agencies must ensure programs they finance comply with Title VI, including by withholding funds from discriminatory programs.

Disparate impact guidelines prohibit the subsidizing of policies or practices that are facially neutral but discriminatory in practice.[15] Title VI requires federal agencies to promulgate regulations and take appropriate actions—including withholding funds—to ensure compliance with Title VI's prohibition of discrimination.[16] Agencies have a duty to investigate and monitor funding recipients even without an official complaint.[17] Under guidance from the Attorney General, agencies must "ensure that…disparate impact provisions in [agency] regulations are fully utilized."[18] Indeed, as the Supreme Court has indicated, private lawsuits are not permitted under Title VI, and thus federal agencies are the only means of enforcing this cornerstone of the Civil Rights Act. To date, 26 federal agencies have published Title VI regulations. Agencies should "initiate affirmative compliance reviews" to guarantee that agency funding violates neither the intentional nor the disparate impact standards of Title VI.[19]

Per these guidelines, for instance, state and local law enforcement agencies may not use federal funding in any racially discriminatory manner. The DOJ has a wide array of enforcement tools to ensure compliance, such as lengthy cooperation agreements with local police departments deemed to be in violation of Title VI, subjecting such departments to court-orders, or even

[10] *Id.* (citing (citing *Guardians Ass'n v. Civil Serv. Comm'n*, 463 U.S. 582, 643 (1983) (Steven, J., dissenting) (citing *Lau v. Nichols*, 414 U.S. at 568, 571 (Stewart, J., concurring) and *Fullilove v. Klutznick*, 448 U.S. 448, 479 (1980) (opinion of Burger, C.J.)); *Alexander v. Choate*, 469 U.S. 287, 293 (1985)).
[11] *Ricci v. DeStefano*, 557 U.S. 557, 577 (2009).
[10] Title VI Legal Manual, *supra* note 3, at Section VII.
[13] *Ga. State Conference of Branches of NAACP v. State of Georgia*, 775 F.2d 1403, 1417 (11th Cir. 1985) (disparate impact standard from Title VII is "instructive" for Title VI). *See Albemarle Paper Co. v. Moody*, 422 U.S. 405, 425 (1975); *see McDonnell Douglas Corp. v. Green*, 411 U.S. 792, 802-03 (1973) (describing the three-step disparate impact analysis in the analogous Title VII context).
[14] *Id.*
[15] *Id.*
[16] 42 U.S.C. § 2000d-2.
[17] Title VI Legal Manual, *supra* note 3, at Section VII(D). Agencies have a "clear mandate" to collect relevant demographic data from recipients of federal assistance to monitor or evaluate compliance. *Id*.
[18] Title VI Legal Manual, *supra* note 3, at Section VII.
[19] *Id.*

withholding funding.[20] In September 2021, the DOJ launched a comprehensive review of all law enforcement departments currently receiving federal dollars to ensure Title VI compliance.[21]

One example of a successful Title VI challenge includes a 2013 Ninth Circuit finding that the Maricopa County Sheriff's Office engaged in intentional discrimination when it permitted officers to expressly take race into account in determining which individuals it should detain.[22] In another example, a Florida case found a Title VI violation where a racially neutral formula was used to distribute aid to elderly residents, but the result was a disparate impact.[23] The court found that certain "[m]inority elderly [residents] have a disproportionate tendency to reside with…extended family." [24] As a result, a greater number of minority residents were excluded from aid while non-minority residents that more commonly lived alone did receive aid. The funding formula skewed federal assistance away from racial minorities in need of help, a statistical effect the Court held to violate the disparate impact requirement.[25]

As the federal government consider policies for the use of biometric and algorithmic technologies by federal agencies or recipients of federal funds, Title VI obligates them to ensure that these technologies and how they are used do not produce unlawful racial discrimination.

II. Biometric technologies carry significant risk of bias and disparate impact.

Biometric technologies are a subset of algorithmic technologies, which operate by analyzing large sets of data, identifying correlations and patterns within the data, and then extrapolating from those patterns to make decisions, predictions, or matches.[26] When the source data for an algorithm comes from societal sources that are a product of historic and ongoing systemic inequalities—such as our criminal justice system, housing markets and urban development produced by redlining and segregation, or longtime disparities in access to jobs, education, lending, or healthcare—the algorithm will discover the pattern.[27] The algorithm will not know that one set of patterns is acceptable to use and that another set of patterns is unacceptable. Absent careful design and intervention, the algorithm will see patterns of discrimination in society and reproduce them, because that is how the algorithm (or artificial intelligence) works.[28] Researchers have noted that such technologies "present a veneer of social control or risk

[20] Katie Benner, *Justice Dept. to Review Enforcement of Civil Rights Protections in Grants*, N.Y. Times (Sep 16, 2021).
[21] *Id.*
[22] *Melendres v. Arpaio*, 989 F.Supp.2d 822, 827 (9th Cir. 2013).
[23] *Meek v. Martinez*, 724 F. Supp. 888, 899 (11th Cir. 1987).
[24] *Id*.
[25] *Id.*
[26] Nicol Turner Lee, Paul Resnick, & Genie Barton, *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harm,* BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.
[27] *See, e.g., Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F. 4th 330, 348 (4th Cir. 2021) (en banc) (Gregory, C.J. concurring) ("Many measures of resource distribution and public well-being now track the same geographic pattern [from past redlining]: investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates; and the list goes on.").
[28] *See Confronting Bias: BSA's Framework to Build Trust in AI,* BUSINESS SOFTWARE ALLIANCE (June 8, 2021), https://ai.bsa.org/wp-content/uploads/2021/06/2021bsaaibias.pdf.

[redacted]

mitigation," while in reality they "tend to reproduce, maintain, and naturalize structural inequalities…and allow policymakers to avoid necessary structural reforms."[29]

Biometric and algorithmic technologies can directly or indirectly result in discrimination through their design or the datasets used to train their algorithms. "Biometric information" is an umbrella term for "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[30] Biometric technologies, in turn, capture and analyze such information.[31] Biometric technologies are used in various ways, each of which carries risk of discrimination. Some systems are used to identify or verify identity of an individual, such as facial recognition. Others are used to make decisions about whether an individual will receive an opportunity, such as eligibility determinations for jobs or healthcare.[32]

As explained below, the reliability and risk of bias in biometric technology varies greatly depending on the design of the technology and the biometric marker being analyzed. One significant factor in determining reliability and risk of bias is the representativeness of the data set, including how the data was collected and how it is used. For example, criminal DNA databases are over-representative of Black people,[33] while medical research DNA databases are over-representative of white people.[34]

[29] Stefanie Coyle & Rashida Richardson, *Bottom-Up Biometric Regulation: A Community's Response to Using Face Surveillance in Schools,* in AI NOW INSTITUTE, REGULATING BIOMETRICS: GLOBAL APPROACHES AND OPEN QUESTIONS 104 (Amba Kak ed., Sep. 1, 2020). *See also* Erin Simpson & Adam Conner, *How To Regulate Tech: A Technology Policy Framework for Online Services*, CENTER FOR AMERICAN PROGRESS (Nov. 16, 2021), https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/ ("Use of digital technologies—including…biometric technology, and more—have introduced new vectors to continue the deeply rooted historical exploitation of and discrimination against protected classes."); Yeshimabeit Miller & Amy Traub, *Data Capitalism + Algorithmic Racism,* DEMOS, https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf ("Baked into the mathematical formulas of the algorithm, represented by lines of code, are legacies of racist public policy and discrimination dating back to the foundation of this country, codified through existing data sets as if they were digital artifacts of the past.").

[30] Illinois' Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2008); *see also* California's California Consumer Privacy Act, defining the same term as "an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity." Cal. Civ. Code §1798.140 (West 2019).

[31] *See Biometric Standards Program and Resource Center,* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (last updated June 4, 2020), https://www.nist.gov/programs-projects/biometric-standards-program-and-resource-center.

[32] *See generally* P. Jonathan Phillips, Et Al., *An Introduction to Evaluating Biometric Systems* 56, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2000), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151436.

[33] Erin Murphy and Jun H. Tong, *The Racial Composition of Forensic* DNA *Databases*, California Law Review (Dec. 2020), *available at* https://www.californialawreview.org/print/racial-composition-forensic-dna-databases/#clr-toc-heading-1.

[34] Vicky Stein, *Genetic research has a white bias, and it may be hurting everyone's health*, PBS NewsHour (updated on Mar. 22, 2019), https://www.pbs.org/newshour/science/genetic-research-has-a-white-bias-and-it-may-be-hurting-everyones-health.

[redacted]

To better consider the risk of disparate impact, we focus here upon two commonly used biometric technologies: (A) biometric identification technology (primarily facial recognition technology), and (B) behavioral recognition technology.

A. Biometric Identification Technology, such as facial recognition technology (FRT), discriminates on the basis of race and gender.

Biometric identification technology involves measuring biological characteristics to identify or verify the identity of individuals. FRT is the most common technology and it typically is used to compare "identity information in features vectors extract from two face image samples and produce a measure of similarity between the two."[35]

Empirical research demonstrates that FRT presents a significant risk of bias and disparate impact on protected groups by producing inaccurate and skewed outputs. Of all biometric technologies, FRT in particular has received the most criticism for its demonstrated racial and gender bias and its subsequent impact on individuals and communities of color due to its frequent use by law enforcement.[36] Indeed, the data is so alarming that three of the largest purveyors of FRT recently scaled back their operations because of these concerns: IBM and Microsoft both stopped selling FRT products to police departments out of concern that "such technology could be used by the police to violate 'basic human rights and freedoms,'"[37] as did Amazon.[38] And these concerns have already prompted at least seven states and almost two dozen cities to limit the use of FRT by government entities, such as law enforcement, schools, and campus security.[39]

1. Even when facially neutral, FRT is discriminatory in practice.

Several major studies have analyzed commercially available and "state-of-the-art" FRT algorithms and found overwhelming evidence of bias that runs across lines of race, gender, and skin color. One 2018 study, for instance, "measured the accuracy of three commercial gender

[35] PATRICK GROTHER ET. AL, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 14 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[36] We understand that there are additional technologies, including iris scanning technologies, but we focus on FRT in our discussion as it is one of the more commonly-used biometric technologies.

[37] Bobby Allyn, *IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance,* NPR (June 9, 2020), https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance; Olivia Solon, *Microsoft won't sell facial recognition to police without federal regulation,* NBC NEWS (June 11, 2020), https://www.nbcnews.com/tech/internet/microsoft-won-t-sell-facial-recognition-police-without-federal-regulation-n1230286. *See also,* Kashmir Hill & Ryan Mac, *Facebook Plans to Shut Down Its Facial Recognition System,* N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html (describing Facebook's decision to turn off facial recognition tools but keep the data).

[38] Jeffrey Dastin, *Amazon extends moratorium on police use of facial recognition software,* REUTERS (May 18, 2021), https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

[39] Associated Press, *States Push Back Against Use of Facial Recognition by Police,* U.S. NEWS (May 5, 2021), https://www.usnews.com/news/politics/articles/2021-05-05/states-push-back-against-use-of-facial-recognition-by-police. The City of San Francisco prohibited the practice in 2019, followed by California's statewide three-year moratorium on police use of FRT derived from body cameras. And other states have responded with bans of varying intensity: New York, for example, currently has a two-year moratorium on the use of FRT in schools, while Virginia requires all local law enforcement and campus-based security to get the approval from the state legislature before FRT can be utilized. Additional limits and requirements are currently being considered in about twenty states.

[redacted]

classification algorithms" and found that all three systems are more accurate on "male faces than female faces" and "lighter faces than darker faces," while performing "worst on darker female faces."[40] The authors of the study noted that despite "darker females [constituting] 21.3% of the [benchmark], they constitute 61.0% to 72.4% of the classification error."[41] A 2019 study from the National Institute of Standards and Technology (NIST) found similar results when it discovered that "a majority of facial-recognition systems exhibit bias," finding that they "falsely identified African-American and Asian faces 10 times to 100 times more than Caucasian faces."[42] These and other studies demonstrate FRT is discriminatory.[43] Research also shows that humans are very bad at identifying unfamiliar faces, which can compound discrimination from FRT if the algorithms require humans to check and verify the accuracy of their results.[44]

2. Law enforcement agencies use FRT in a discriminatory manner with disproportionate adverse effect on protected groups.

FRT has a well-documented history of compounding previously existing racial disparities, particularly when used in the law enforcement sector. Studies show, "[i]n at least three cases that are publicly known police have relied on erroneous face recognition identifications to make wrongful arrests of Black men,"[45] leading to multiple lawsuits against the police departments that made the arrests.[46] Critically for Title VI analysis, we are not aware of *any* false arrests based on a FRT mismatch of non-Black individuals.[47] Black Americans are more likely to be stopped, arrested and incarcerated for minor crimes, and therefore have more mugshots in the police databases. This creates what some call a "feed-forward loop" making Black Americans disproportionately "subject to future [FRT] surveillance."[48] In Detroit, a 2016 program saw

[40] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classificationi,* 81 Proc. of Machine Learning Res. 1, 12 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[41] *Id.* at 10.
[42] *Grother et. al, supra,* FN 30.
[43] This detection bias is well-documented in several peer-reviewed studies. *See generally, id.*; Brenan F. Klare et. al, 7 IEEE TRANSACTIONS ON INFO. FORENSICS AND SECURITY 1789 (2012) ("performances of all three commercial algorithms [studied] were consistent in that they all exhibited lower recognition accuracies on the following cohorts: females, Blacks, and younger subjects"); Cynthia M. Cook et. al., Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems, 1 IEEE TRANSACTIONS ON BIOMETRIC BEHAV. AND IDENTITY 32 (2019) ("our analyses show that demographic factors influenced both the speed and accuracy of all eleven commercial biometric systems evaluated.").
[44] *See, e.g.,* Alice Towler et. al., *Can face identification ability be trained? Evidence for two routes to expertise,* PSYARXIV (Aug. 26, 2020), https://psyarxiv.com/g7qfd/ (noting that "many uses of face recognition software have actually increased the need for human processing" but that "[p]rofessional staff who use this technology in their daily work are extremely prone to error, identifying the wrong face from the array on 40% of trials").
[45] *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, New America: Open Technology Institute (June 3, 2021), https://www.newamerica.org/oti/briefs/civil-rights-concerns-regarding-law-enforcement-use-of-face-recognition-technology/.
[46] Complaint, *Robert Julian-Borchak Williams v. City of Detroit*, No. 2:21-cv-10827 (E.D. Mich. Apr. 13, 2021), ECF No. 1; Complaint and Demand for Trial By Jury, *Nijer Parks v. John E. McCormack*, Case No. L-003672-20 (N.J. Nov. 25, 2020).
[47] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,* N.Y. TIMES (last updated Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
[48] Alex Najibi, *Racial Discrimination in Face Recognition Technology,* Harvard University: Blog: Science Policy (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/?web=1&wdLOR=c495F80EB-3312-4EC4-8695-0AB4D028987B.

police install high-definition cameras throughout the city. While most Michigan residents were found in the system, police unevenly distributed the cameras resulting in higher surveillance in predominantly Black areas and little surveillance in predominantly White or Asian ones.[49]

Law enforcement has also utilized biometric scans to selectively chill protected First Amendment protest activity. Six federal agencies used FRT to identify protestors after George Floyd's May 2020 murder.[50] Baltimore Police used the same technology in 2015 during protests over Freddie Gray's death in police custody.[51] Given Black Americans' overrepresentation in preexisting police databases, police use of FRT to surveil protestors carries with it both a disparate impact in terms of Black protestors' likelihood of arrest and also in its ability to deter constitutionally protected activity. Such surveillance also builds on a long history of law-enforcement efforts to "target[] groups that the government deem[s] subversive."[52] The Fourth Circuit recently held *en banc* that Baltimore activists would likely prevail on their constitutional challenge to the city's aerial surveillance program.[53] Whereas mass surveillance presents risks to everyone, the court found, its impact is felt primarily by "'those least empowered to object.' Because those communities are over-surveilled, they tend to be over-policed, resulting in inflated arrest rates and increased exposure to incidents of police violence."[54]

As demonstrated here, the use of FRT by law enforcement and other state actors has a disparate impact on protected groups due to both the technology itself and its deployment in a manner that makes existing discriminatory systems more efficient and therefore more discriminatory.

B. Behavioral Recognition Technology carries significant risk of bias and disparate impact on protected groups, and lacks a reliable scientific foundation.

Beyond FRT researchers that study facial geometry, some scientists are also attempting to judge behaviors in an "objective" fashion. We touch upon this concerning area briefly given that it is growing in popularity but not in reliability. Behavioral biometrics technology seeks to identify or

[49] *Id.*

[50] Radhamely De Leon, *Six Federal Agencies Used Facial Recognition On George Floyd Protestors*, VICE (June 30, 2021), https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors. In another high-profile incident, NYPD surveilled a racial justice protest, recorded an attendee "speaking loudly into a megaphone," and attempted to arrest him in his apartment shortly thereafter by sending dozens of officers in riot gear. Amnesty International, *Ban dangerous facial recognition technology that amplifies racist policing* AMNESTY INTERNATIONAL (Jan. 26, 2021), https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

[51] Kevin Rector & Alison Knezevich, *Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest,* THE BALTIMORE SUN (Oct. 11, 2016), https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

[52] Sahil Singhvi, *Police Infiltration of Protests Undermines the First Amendment*, BRENNAN CENTER FOR JUSTICE (Aug. 4, 2020), https://www.brennancenter.org/our-work/analysis-opinion/police-infiltration-protests-undermines-first-amendment.

[53] *Leaders of a Beautiful Struggle v. Baltimore Police Dep't.*, 2 F.4th 330 (4th Cir. 2021) (en banc).

[54] *Id.* at 347 (quoting Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance,* THE CENTURY FOUNDATION (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/?agreed=1.). The opinion noted further that "liberty from governmental intrusion can be taken for granted in some neighborhoods,while others "experience the Fourth Amendment as a system of surveillance, social control, and violence." *Id.*at 348. (quoting Devon W. Carbado, F*rom Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence*, 105 CAL. L. REV. 125 (2017)).

[redacted]

make qualitative assessments about individuals based on human behavior. It works by observing *how* someone performs a certain action, rather than by scrutinizing a discrete biological characteristic.[55] Examples include analysis of an individual's gait, keystrokes, facial expressions, and voice. Such biometrics depend on artificial intelligence to "identify and model those features of each [individual's] behavior that are most unique."[56] For example, software might analyze an individual's unique typing rhythm, speed, or cadence, or their speed and step patterns to create a unique profile for that individual for the purposes of future identification.

1. Behavioral biometrics often rests on ill-derived scientific findings.

Many applications of behavioral biometrics have been labeled "pseudo-science" and "a license to discriminate," to the extent they are "not rooted in scientific fact."[57] One study of existing technology that aimed to discern people's internal emotional states concluded that "there is insufficient evidence to support" the "common view that humans around the world reliably express and recognize certain emotions in specific configurations of facial movements."[58] As the study firmly noted, its findings showed conclusively that facial expressions "are not 'fingerprints' or diagnostic displays that reliably and specifically signal particular emotional states."[59] In particular, these technologies pose a high risk of discrimination against people with disabilities, such as a person who has suffered partial facial paralysis.

And yet, the market for emotion recognition biometric software is worth billions.[60] The increased demand for such services is particularly worrisome, as such technologies are increasingly deployed in high-stakes situations: from a recruiter's review of a job applicant, to a "jury's cultural misunderstanding about what a foreign defendant's facial expressions mean," to a "'smart body' camera falsely telling a police officer that someone is hostile and full of anger."[61]

2. Many algorithms used to assess human behavior have been shown to be discriminatory in practice.

Analyses of behavioral biometrics have found repeatedly that certain algorithms perform differently across various demographic subgroups. In 2011, researchers documented the repeated inability of car-based voice recognition systems to accurately detect the speech of women and individuals with thicker accents, which indicates a propensity for discrimination on the basis of

[55] International Biometrics and Identity Association*, Behavioral Biometrics,* 3 (May 1, 2017), https://www.ibia.org/download/datasets/3839/Behavioral%20Biometrics%20white%20paper.pdf.
[56] *Id.* at 4.
[57] Drew Harwell, *HireVue's AI face-scanning algorithm increasingly decides whether you deserve the job*, The Washington Post (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.
[58] Lisa Feldman Barrett et. al, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 PSYCHOL. SCI. IN THE PUB. INT. 1, 46 (2019).
[59] *Id.*
[60] Jay Stanley, *Experts Say 'Emotion Recognition' Lacks Scientific Foundation*, American Civil Liberties Union (Jul. 18, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/experts-say-emotion-recognition-lacks-scientific.
[61] *Id.*

[redacted]

national origin.[62] A 2017 study of YouTube's automatic captioning software found the same, and suggested that the overrepresentation of Caucasian, male speakers in the algorithm's training dataset may be to blame.[63]

Some prominent companies using biometric-based behavioral data are starting to limit the ways biometrics are used to screen job applicants. For example, HireVue recently announced its decision to stop using facial monitoring in its candidate recruitment software.[64] After auditing its technology, HireVue found little correlation between monitoring facial expressions and candidate success,[65] leading many to worry that the technology would simply "replicate systemic biases that are ingrained in the environment in which they are designed."[66] The audit suggested HireVue investigate the risk of bias against protected groups and candidates with accents.

The underlying science and studies support the conclusion that use of behavioral biometrics is discriminatory, which has legal consequences, pursuant to Title VI, for its use by federal agencies and recipients of federal funds.

III. Conclusion

Title VI of the Civil Rights Act of 1964 strictly prohibits the federal government and recipients of federal funds from engaging in activities that result in discrimination based on race or national origin. Many biometric and algorithmic technologies produce just such results. Consequently, Title VI forbids the use of these technologies unless and until mechanisms are developed to prevent the discriminatory outcomes.

This is not a situation where a problem exists without a statute to address it. Current federal law controls this situation and must be executed correctly and thoroughly. We urge OSTP to take account of the federal government's legal obligations under Title VI as it addresses biometric and algorithmic technologies and crafts policy recommendations for agencies.

Thank you for the opportunity to provide comment on this important topic. For additional questions, please contact [redacted].

[62] Graeme McMillan, *It's Not You, It's It: Voice Recognition Doesn't Recognize Women*, TIME.com (June 01, 2011) https://techland.time.com/2011/06/01/its-not-you-its-it-voice-recognition-doesnt-recognize-women/.
[63] Rachael Tatman, *Gender and Dialect Bias in YouTube's Automatic Captions* (Apr. 4, 2017), *available at* http://www.ethicsinnlp.org/workshop/pdf/EthNLP06.pdf.
[64] Lindsey Zuloaga, *Industry Leadership: New Audit Results and Decision on Visual Analysis*, HireVue (Jan. 11, 2021), https://www.hirevue.com/blog/hiring/industry-leadership-new-audit-results-and-decision-on-visual-analysis. In 2019, a formal complaint was lodged against HireVue with the Federal Trade Commission, alleging the software was "biased, unprovable, and not replicable," this constituting "unfair and deceptive trade practices." Harwell, *supra,* fn. 51.
[65] Zuloaga, *supra,* fn. 58.
[66] Roy Maurer, *HireVue Discontinues Facial Analysis Screening*, SHRM.org (Feb. 3, 2021), https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/hirevue-discontinues-facial-analysis-screening.aspx.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Lisa Feldman Barrett

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Inferring Emotions From Physical Signals

Lisa Feldman Barrett, Ph.D.
University Distinguished Professor
Director, Interdisciplinary Affective Science Laboratory
Northeastern University and Massachusetts General Hospital/Harvard Medical School

Executive Summary

You cannot detect a person's emotional state (i.e., angry, sad, fearful, remorseful, etc.) from patterns of facial signals, physiological signals, or neural signals, according to peer-reviewed scientific articles. Scowling in anger, smiling in happiness, frowning in sadness, - all these are stereotypes of emotional expressions. They reflect common beliefs about emotional "expressions," beliefs held by people who live in western countries, but these beliefs don't correspond to how people actually express emotion in real life. And these stereotypes don't generalize to cultures that are very different from ours. Any technology that claims to read emotion in physical movements, physiological signals, or neural signals is misrepresenting what it can do, according to the best available, peer-reviewed scientific evidence. Inferring a person's mood or affect (e.g., sleepiness during driving) via such signals may hold more promise.

Background

Research in psychological science, computer science, neuroscience, and physiology attempt to identify emotional states in humans and non-human animals by measuring signals in behavior (e.g., facial muscle movements, postural changes, vocalizations, word use, etc.), signals in the brain (e.g., brain imaging patterns) and signals in peripheral physiology (e.g., autonomic nervous system changes in heart rate, skin conductance, etc.). These efforts are referred to as **emotion inference** (the term used in this document), emotion perception, emotion detection, or more commonly, emotion recognition. Machine learning (ML) algorithms are trained to detect patterns for the purpose of inferring the presence of emotional states, such as anger, happiness, sadness, and fear. ML is a powerful family of techniques that allow scientists to program and train a computer model on one set of observations, identify data patterns, and assess how well these patterns generalize to a new set of observations. In emotion inference efforts, human raters view a sample of signals (e.g., photographs or videos of people making facial movements) and label them with emotion words; this becomes the ML training set. Once a pattern is identified for each emotional state, it is used to diagnose the presence of that state in a new sample of signals.

Emotion inference can be distinguished from **affect inference** which uses similar data and ML approaches to infer the presence of affective states such as pleasure, boredom, sleepiness,

arousal, distress and interest. Methods to infer emotion and affect are collectively referred to as **affective computing** or **emotion artificial intelligence** (a.k.a. "emotion AI").

The global market for emotion and affect inference products is projected to double by 2024 to reach $56 billion.[1] Efforts to infer affect and emotion can be found in every commercial, educational, medical, and governmental sector (summarized in Table 1). Large companies have established R&D projects and made major acquisitions in emotion AI including Apple[2], Amazon,[3] IBM,[4] Google,[5] Facebook,[6] and Microsoft.[7] Several of these companies have released software platforms for others to attempt to build emotion AI products. Major car companies have significant emotion and affect inference efforts to infer driver inattentiveness and/or sleepiness and to estimate levels of frustration and joy.[8] Many startups are also building new recording methods and inference models for specific use cases.[9]

Emotion AI Applications[10]

Business & Industry	**Health Care & Education**	**Consumer and Entertainment**	**Government, Police, Military, Legal**
Marketing & Advertising ● Targeted advertising ● Customer purchase monitoring[11] ● Smart billboards **Customer Service** ● Chatbots ● Customer experience monitoring **Human Resources** ● Job interviews and hiring decisions ● Productivity monitoring ● Team functioning **Safety & Quality Control** ● Factory monitoring ● Vehicle safety features (e.g., monitoring driver	**Diagnostics** **Patient Monitoring** ● Symptoms monitoring[15],[16] ● Suicide prevention **Treatment** ● Mental health chatbots ● Wellness apps **Schools** ● Learning, attention, distraction & motivation[17],[18],	**Consumer Apps** ● Personal wellness apps ● Dating apps **Entertainment** ● Gaming & AR/VR ● Companion robots ● Adult entertainment	**Police** ● Parole monitoring ● Crowd control & protest monitoring ● Threat assessment **Courts & Criminal Justice** ● Sentencing ● Parole board decisions **Security Screening & Counterterrorism** ● Behavioral profiles ● Lie detection ● Interrogation **Elections & Political Campaigns** ● Political ads

[1] https://findbiometrics.com/biometrics-news-marketsandmarkets-projects-emotion-recognition-market-double-next-four-years-020508/
[2] https://9to5mac.com/2016/01/07/apple-emotient/
[3] https://www.wired.com/story/amazon-detect-fear-face-you-scared/
[4] https://www.washingtonpost.com/business/2019/07/31/emotion-detection-ai-is-billion-industry-new-research-says-it-cant-do-what-it-claims/
[5] https://www.techradar.com/news/internet/cloud-services/you-can-now-try-google-s-emotion-detecting-image-api-for-yourself-1315249
[6] https://techcrunch.com/2016/11/16/facial-gesture-controls/
[7] https://blogs.microsoft.com/ai/happy-sad-angry-this-microsoft-tool-recognizes-emotions-in-pictures/
[8] https://singularityhub.com/2020/07/29/what-if-cars-could-read-and-react-to-your-emotions-soon-they-will/
[9] https://resource.affectlab.io/top-10-emotional-artificial-intelligence-startups-that-have-created-a-global-disruption/
[10] Modified with permission; Fridman, J., Winterberg, S. (2021). Responsibly assessing and investing in affective computing technologies *IEEE Transactions on Affective Computing,* submitted.
[11] https://thecounter.org/walgreens-kroger-testing-cameras-that-guess-shoppers-age-gender/
[15] https://www.empatica.com/blog/embrace2-receives-fda-clearance-for-children-ages-6-and-up-edce647ef610.html
[16] https://winterlightlabs.com/news/isctm-2020-news-update
[17] https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/
[18] https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france

attention, sleepiness & distraction) [12],[13],[14] • Air traffic control safety (e.g., monitoring controller attention, sleepiness & distraction)	[19]		• Crowd monitoring[20] **Governance and Regulation** • Monitoring citizens[21]

Assessment

To date, peer-reviewed scientific articles indicate that patterns of facial signals, physiological signals, or neural signals have limited reliability, specificity, and generalizability to infer the presence of a particular emotional state (e.g., [22,23,24,25]). (Most ML technology in industry is proprietary and without access to the code, it is difficult to assess their function.) Here is a brief summary of notable peer-reviewed findings:

- An interdisciplinary team of senior scientists, commissioned by the Association for Psychological Science, reviewed over 1,000 peer-reviewed scientific papers and came to a consensus view: the common assumption "that a person's emotional state can be readily inferred from his or her facial movements" has no scientific support.[22] For example, it has been assumed that scowling is the universal facial expression of anger. Yet studies consistently show that humans who live in urban culture settings scowl only about 30% of the time when angry, which is considered low reliability. The other 70% of the time, they express anger in other meaningful and context-specific ways (frowning, crying, smiling, etc.). People also scowl to express other states, including confusion, concentration, humor at a bad joke, stomach upset, etc., so scowling has low specificity as a marker of anger. Scowling is not a universal expression of anger; it is a Western stereotype. No stereotypical facial expression (smiling in happiness, frowning in sadness, etc.) is a reliable, specific, and generalizable predictor of emotional state. Therefore, it is inaccurate to refer to facial

[12] https://www.fastcompany.com/90368804/emotion-sensing-cars-promise-to-make-our-roads-much-safer
[13] https://blog.affectiva.com/affectiva-automotive-ai-building-emotionally-aware-cars-with-in-cabin-sensing
[14] Eyben, F., Wöllmer, M., Poitschke, T., Schuller, B., Blaschke, C., Färber, B., & Nguyen-Thien, N. (2010). Emotion on the road—necessity, acceptance, and feasibility of affective computing in the car. *Advances in human-computer interaction*, *2010*.
[19] https://syncedreview.com/2020/01/16/emotioncues-ai-knows-whether-students-are-paying-attention/
[20] https://www.wsj.com/articles/trumps-rallies-arent-just-part-of-his-campaign-they-are-the-campaign-11571753199?mod=searchresults&page=1&pos=1
[21] https://www.ft.com/content/68155560-fbd1-11e9-a354-36acbbb0d9b6
[22] Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A., & Pollak, S. (2019). Emotional expressions reconsidered: Challenges to inferring emotion in human facial movements. *Psychological Science in the Public Interest*, 20, 1-68; Le Mau, T., Hoemann, K., Lyons, S.H., Fugate, J. M. B., Brown, E. N., Gendron, M., & Barrett, L. F.* (2021). Professional actors demonstrate variability, not stereotypical expressions, when portraying emotional states in photographs. *Nature Communications*, 12, https://doi.org/10.1038/s41467-021-25352-6
[23] Azari, B., Westlin, C., Satpute, A.B. *et al.* Comparing supervised and unsupervised approaches to emotion categorization in the human brain, body, and subjective experience. *Sci Rep* 10, 20284 (2020). https://doi.org/10.1038/s41598-020-77117-8
[24] Siegel, E. H., Sands, M. K., Van den Noortgate, W., Condon, P., Chang, Y., Dy, J., *Quigley, K. S., & *Barrett, L. F. (2018). Emotion fingerprints or emotion populations? A meta-analytic investigation of autonomic features of emotion categories. *Psychological Bulletin, 144*(4), 343-393.
[25] Gendron, M., Crivelli, C., & Barrett, L. F. (2018). Universality reconsidered: Diversity in meaning making of facial expressions. *Current Directions in Psychological Science*, 27, 211-219; Gendron, M., Hoemann, K., Crittenden, A. N., Mangola, S. M., Ruark, G., & Barrett, L.F. (2020). Emotion perception in Hadza hunter-gatherers. *Scientific Reports*, 10 3867. https://doi.org/10.1038/s41598-020-60257-2.

movements, such as a scowl, as "anger expressions" or even "emotional expressions." Such terms confuse a movement with its (possible) emotional meaning. Many reports, both peer-reviewed and from industry, claim that emotion AI technology can accurately detect emotions. This is not the case. Under optimal conditions, such technology can detect facial *movements*, but the emotional *meanings* of these movements is incorrectly assumed rather than tested.

- A similar pattern of findings exists for measures of the autonomic nervous system and brain. In an individual study, certain patterns of signals might distinguish one emotion from another, but these patterns are not reliable (do not replicate) across different statistical methods and studies.[23,24]
- Facial movements, vocalizations, and gestures have significant cultural differences.[25]
- Using emotion stereotypes to infer emotions also increases the likelihood of racial bias from emotion AI technology.[26]
- Even humans do not "recognize" or "detect" emotions in one another. Rather, people make educated guesses based on context, including the immediate situation, the state of their own bodies, their own past learning history, and their cultural learning. This means that in machine learning, third-party labels that are applied to training data are inferences, not objective "readings." When "emotion AI" algorithms are evaluated for their ability to predict with consistency relative to human inferences, high values do not reflect the objective accuracy or validity of the algorithm to detect an emotional state.

Monitoring techniques involving many different signals (more than just two or three), known as multimodal monitoring, may hold more promise for emotion inference, provided ML algorithms model and predict patterns *within a given individual* over time (e.g., [27]), search for *multiple patterns* for each emotion category (e.g., [28]), and then examine whether any of the patterns predict across individuals and situations. Robust and generalizable inferences will require many signals collected simultaneously for the same person across many contexts, with their active and willing participation. Algorithms for affective inferences in certain circumstances, e.g., sleepiness during driving, may hold more promise, in part because the training data can be labeled objectively (e.g., did the person fall asleep or not).

[26] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765

[27] Hoemann, K., Khan, Z., Feldman, M.J. *et al.* Context-aware experience sampling reveals the scale of variation in affective experience. *Sci Rep* 10, 12459 (2020). https://doi.org/10.1038/s41598-020-69180-y

[28] Khalaf, A., Nabian, M., Fan, M., Yin, Y., Wormwood, J., Siegel, E., Quigley, K. S., Barrett, L, F., Akcakaya, M., Chou, C-A., & Ostadabbas, S. (2020). Analysis of multimodal physiological signals within and between individuals to predict psychological challenge vs. threat. *Expert Systems with Applications*, 140, https://doi.org/10.1016/j.eswa.2019.112890.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Madeline Owens

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

[redacted]

Cleaning Up Garbage in Facial Recognition Technology

Madeline Owens, University of Pittsburgh

Comment submitted in response to White House Request for Information (RFI) on Biometrics

November 21, 2021

Abstract

"Garbage in, garbage out" is a computer science phrase referring to the problem of poor-quality inputs leading to poor-quality outputs. Charles Babbage first expressed the idea behind the phrase in his autobiography about his experiences as a mathematician in Victorian England. Although not directly connected, his idea is key to understanding contemporary debates regarding facial recognition technology (FRT), including the data auditing of FRT algorithms. This comment explores the term GIGO; considers its application to FRT; and proposes best practices to address the issue, including establishing minimum photo quality and editing standards, annual algorithmic audits, and allowing governments and companies to purchase only the most sophisticated software trained on representative data. The comment's critical approach foregrounds analysis of the connection between evidence and identification tools built on computer algorithms. Independent research was conducted as part of an undergraduate course in communication at the University of Pittsburgh. Younger generations are surveillance natives; therefore, when we believe a technology crosses the line, the potential negative impacts of that technology must be severe.

History of GIGO

According to the *Oxford English Dictionary*, the first known printed usage of the phrase "garbage in, garbage out" dates to 1957 ("garbage"). At the time, high-speed computers had to be manually programmed, and data typically was inputted using punch cards or tape. In the article "Applying New Electronic Computers to Traffic and Highway Problems" for *Traffic Quarterly*, Dr. Ernst E. Blanche uses the acronym "GIGO" for the phrase "garbage in, garbage out," which "emphasizes that the results are no better than the data given to the computer" (411). The concept, however, is much older and dates to Victorian England.

Compared to mainland Europe, mathematical innovation in Great Britain had stagnated from 1750 to 1830 due to the island's isolated geographical location, war with France, and distrust of new ideas in the field (Flood et al. 2). Queen Victoria assumed power in 1837 and presided over a social, economic, scientific, and technological Golden Era for Britain. In his autobiography *Life from the Passages of a Philosopher*, Charles Babbage retells his development of the Difference Engine Number One, the first prototype for an automated calculator. Seeking to reduce the mental labor and frequency of error in calculations, the object of the Difference Engine was to "calculate and print a *series* of results formed according to given laws," called "tables" (Babbage 38). In 1823, seeing a potential use for nautical calculations, the government agreed to finance the development of a large-scale Difference Engine and granted Babbage 1,500 pounds from the Civil Contingencies fund (Babbage 52). Between 1823 and 1842, the government spent over 17,000 pounds on Babbage (Babbage 68). During his progress checks with the government, Babbage had been asked by two members of the House of Lords and the House of Commons respectively, "'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out'" (qtd. in Babbage 50)? Babbage dismissed the

question as a misunderstanding of the machine's design. However, given the state of calculators at the time, the representatives' confusion was warranted.

At the time, slide rulers and printed mathematical tables were primarily used for calculations (Flood et al. 243-244). These devices were "mechanical," meaning that "useful operation relied on the continuous informed intervention of the operator" (Flood et al. 245); essentially, if the operator made a mistake, the output would be inaccurate. Babbage's Difference Engine, which operated by steam, was the first *automated* calculator, meaning "it embodied mathematical or computational rule in mechanism" (Flood et al. 250). The calculator was programmed ahead of time, and the operator, having nothing to do with the input, only needed to pull a lever.

Perhaps the question that the members of Parliament posed to Babbage seemed inane and ignorant—they did not understand the concept of automated calculation. However, their concerns have returned full force today with the increasing use of facial recognition technology. FRT does, in fact, require the informed intervention of the operator, specifically relating to probe photo editing. Low quality or overly edited probe photos will lead to garbage outputs. In addition, improperly trained algorithms will inevitably produce garbage, no matter the quality of the input.

FRT and Data Audits

There are two broad categories of FRT: one-to-one identification and one-to-many identification. One-to-one identification is when a person's identity is verified from a photo of them, such as when a smartphone matches a photograph on file with a user's face to unlock the phone (Castelvecchi). One-to-many identification is when a person's photograph is matched to

multiple photos contained in a database (Castelvecchi). There is also a third related category of FRT—demographic and behavioral classification. Clare Garvie specifically examines the second category. According to her, police departments often feed “celebrity lookalike” images, police sketches, poor quality images, and substantially edited photos into facial recognition algorithms ("Garbage In”). These practices reduce the accuracy of the algorithm—feeding a computer bad information (“garbage”) leads to inaccurate results (more “garbage”). According to a recent National Institute of Standards and Technology report, there have been huge gains in accuracy since 2013, although “only the most accurate [algorithms] excel on poor quality images and those collected long after the initial enrollment sample” (Grother et al. 6). However, what happens when the input is good, but the data on which the algorithm has been trained is garbage?

Facial recognition relies on datasets that train algorithms to produce certain outputs when certain data is inputted (Lee et al.). Essentially, algorithms are trained through supervised learning, a process in which mated and non-mated pairs of photos are shown to a computer and the computer must find the shortest route to matching the mated photos (“Personal communication”). For example, researchers in one study trained a computer algorithm to distinguish between photos of dogs and wolves. The algorithm succeeded, but researchers soon learned that the algorithm was sorting the wolf photos together not by physical features but by detecting snow in the images; as a result, the study was a failure (“Personal communication”). How the computer comes to its conclusions is a “black box”; even developers are oftentimes unsure of the computer’s methods (“Personal communication”). This becomes especially problematic if the pairs of photos come from unrepresentative or incomplete datasets; bias can easily be codified into an algorithm (Lee et al.).

In tax audits, algorithms review whether filers pay their fair share. Algorithm audits assess how well machines are doing their jobs. These latter audits can be conducted in two ways: first, by examining the algorithm's code and data and, second, by interviewing company stakeholders about the perceived impact of the algorithm (Ng). In the Gender Shades study, a group of MIT researchers, using the first method, found that one technology company's gender classification system had a 97% accuracy rate (Hardesty). However, this number was based on a dataset that was 77% male and over 83% white, and the algorithm's accuracy rate dropped substantially for women with darker skin (Hardesty). Although the Gender Shades study focused on gender classification algorithms, many facial recognition algorithms are trained in much the same way. Some scholars promote regular audits, arguing that they produce insightful information and encourage companies to reexamine bias in their algorithms. However, algorithmic audits also create a set of ethical concerns.

A recent controversy is HireVue's use of a facial recognition algorithm in assessing video interviews of candidates for hire. HireVue turned to a third-party auditing company, O'Neil Risk Consulting & Algorithmic Auditing (ORCAA), which consulted Hirevue stakeholders and found no evidence of bias in company procedures (Ng). However, HireVue has come under fire for using this audit as a public relations stunt. ORCAA's audit targeted a specific section of the company's procedures and did not evaluate the algorithm or data, yet HireVue proclaimed the audit's success (Ng). Are data audits truly useful, or are they simply ways for companies to gain positive publicity? In addition, Raji and colleagues warn against overreliance on algorithmic audits, finding several ethical concerns. One such concern is that expanding the dataset for facial recognition technology requires the increased surveillance of minority communities, creating issues of privacy and consent (Raji et al. 4-5).

Recommendations and Conclusion

Ideally, due to the “garbage in, garbage out” problem in FRT, I would recommend against the use of facial recognition technology in all fields. However, I realize that this is unrealistic, as use of FRT is likely to increase in the future. Instead, I propose three best practices. First, as Garvie recommends, governments and companies using facial recognition must establish minimum photo standards for probe photos (“Garbage In”). Organizations such as the International Organization for Standardization and other scholars in the academic community are developing specific image quality thresholds for an algorithm to accurately make a match (“Personal communication”). On a related note, certain photo edits should be prohibited. As Garvie argues, adjusting an image for lighting and coloring is minimally problematic, but substantial edits such as copying and pasting other people’s facial features onto a probe photo should be unacceptable ("Garbage In”).

Second, companies should have annual data audits of the technical type. Audits should thoroughly test the algorithm’s data and code and seek to highlight biases present in the underlying datasets. Finally, I recommend that governments and companies be allowed to purchase only the most accurate algorithms available that have been trained on representative data. Due to the disparity in accuracy rates between various algorithms, governments and companies should only purchase those that can match faces with a high degree of accuracy across all demographics. Raji and colleagues’ concerns about infringing on the privacy rights of minorities are real. However, instead of fighting the losing battle against FRT, we should work to make algorithms equally accurate for non-white males. Further, datasets that target minorities should be sequestered and constrained to auditing purposes only; in addition, such datasets should only contain images of people who can explicitly opt in and opt out of inclusion. By

taking these steps, we can minimize the likelihood of the “garbage in, garbage out” problem in FRT.

In conclusion, the phrase “garbage in, garbage out” originated in a 1957 *Traffic Quarterly* article, but the idea behind it dates to Victorian mathematician Charles Babbage’s Difference Engine. “Garbage in, garbage out” may not have been a problem for Babbage, but it is an increasingly large one today with the frequent use of biased facial recognition technology. Only with proper safeguards can the issue be properly managed.

Works Cited

Babbage, Charles. *Passages from the Life of a Philosopher*. United States, New York University Press, 1989.

Blanche, Ernest E. “Applying New Electronic Computers To Traffic and Highway Problems.” *Traffic Quarterly*, vol. 11, no. 3, 1957, pp. 406–416, babel.hathitrust.org/cgi/pt?id=uc1.$b3472&view=1up&seq=432.

Castelvecchi, Davide. “Is Facial Recognition Too Biased to Be Let Loose?” *Nature News*, Nature Publishing Group, 18 Nov. 2020, www.nature.com/articles/d41586-020-03186-4.

Flood, Raymond, et al. *Mathematics in Victorian Britain*. Oxford University Press, 2011.

"garbage, n. (6.a.) and adj." *OED Online*, Oxford University Press, Sept. 2021, www.oed.com/view/Entry/76687. Accessed 30 Oct. 2021.

Garvie, Clare. “Garbage In. Garbage Out: Face Recognition on Flawed Data.” *Georgetown Law Center on Privacy and Technology*, 16 May 2019, www.flawedfacedata.com/.

Garvie, Clare. Personal communication. 19 Nov. 2021.

Grother et al. “Face Recognition Vendor Test (FRVT): Part 2: Identification.” *NIST.gov*, 28 Oct. 2021, pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

Hardesty, Larry. “Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems.” *MIT News | Massachusetts Institute of Technology*, 11 Feb. 2018, news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

Lee, Nicol Turner, et al. “Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms.” *Brookings*, Brookings, 25 Oct. 2019, www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Ng, Alfred. “Can Auditing Eliminate Bias from Algorithms? – the Markup.” *The Markup*, 23 Feb. 2021, themarkup.org/ask-the-markup/2021/02/23/can-auditing-eliminate-bias-from-algorithms.

Raji, Inioluwa Deborah, et al. “Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing.” *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, doi.org/10.1145/3375627.3375820.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Marsha Tudor

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Wednesday, December 8, 2021 8:22:23 AM

Dear Committee,

Thank you for seeking input.

I have many concerns about AI and will detail them before Jan 15th. But wanted to begin with a comment about my personal experience yesterday.

I was seeking to pay my IRS estimated Taxes for 2021. I went to the site where I had paid in the past. There is a new process called ID.me; it collects additional information BEFORE you are allowed to pay. Included among the requests was a "selfie." I am outraged that the IRS is now collecting that kind of biometric information - especially without an "opt-out" option.

Facial recognition is highly controversial and needs to have a compelling reason for any such data gathering. I believe implementing a procedure like this without the type of research your group is doing could lead to serious civil rights infringements.

Thank you for the work you are doing!
Marsha Tudor

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Microsoft Corporation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Microsoft

January 15, 2022

Dr Eric Lander, The President's Science Advisor and Director of OSTP
Dr Alondra Nelson, OSTP Deputy Director for Science & Society
Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500
Via email to: BiometricRFI@ostp.gov

Dear Dr Lander and Dr Nelson,

Microsoft Response to OSTP Request for Information on Public and Private Sector Uses of Biometric Technologies [Document Number: 2021-21975]

Microsoft appreciates the opportunity to provide feedback in response to the Office of Science and Technology Policy's *Request for Information on Public and Private Sector Uses of Biometric Technologies* as part of its initiative to develop a Bill of Rights for an Automated Society. We share OSTP's view that AI and other data-driven technologies must serve society equitably and respect the enduring values of American democracy. Through policy, process, and technological measures, we need to harness the beneficial uses of AI technologies and mitigate their potential misuse and harms. OSTP's Bill of Rights initiative is a timely and important contribution to the discussion of what effective guardrails ought to look like, and we look forward to sharing our knowledge and experiences in support of the initiative.

Facial Recognition Technology: An Instructive Case Study

Since 2018, Microsoft has engaged in an expansive program of work to better understand the sociotechnical implications of facial recognition technology, and to design and enact effective safeguards to harness its benefits and guard against its potential risks. This work has been conducted in partnership with experts inside and outside of the company, and has included the development of legislative proposals[1] as well as the internal adoption and implementation of Facial Recognition Principles.[2] We have found the work to be instructive not just for ensuring the safe and rights-respecting use of facial recognition technology, but for our responsible AI program more generally.[3] Below, we set out some key insights in the spirit of sharing our lessons learned and helping inform OSTP's initiative.

[1] Brad Smith, *Facial Recognition: It's Time for Action*, Microsoft (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.
[2] Microsoft, Six Principles for Developing and Deploying Facial Recognition Technology, https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf.
[3] We describe key elements of our governance program below; *see also* Natasha Crampton, *The Building Blocks of Microsoft's Responsible AI Program*, Microsoft (Jan. 19, 2021), https://blogs.microsoft.com/on-the-issues/2021/01/19/microsoft-responsible-ai-program/.

Centering on use cases and calibrating risk and mitigations

Facial recognition systems can create risks that are sociotechnical in nature—they arise at the intersection of technology and society and are highly sensitive to the context of use. Specifically, three categories of risk often rise to the top of discussions about facial recognition systems: risks of bias and discrimination, the potential for new intrusions on privacy, and possible threats to democratic freedoms and human rights. When and how those potential risks materialize, who they may impact, and how evenly they are distributed is highly dependent on the use case for the technology. For example, using facial recognition technology to unlock a device has very different implications than using it for ongoing surveillance in a law enforcement context. As a result, we appreciate and endorse OSTP's commitment to an assessment of use cases that is finely tuned and granular.

Beyond the specific use case for an AI system, it is important to study other factors that influence its overall risk profile. AI systems vary widely in their degree of automation, the readiness of the technology for the application, and the complexity of the deployment environment.[4] Therefore, Microsoft believes that any regulatory framework or principles should take a risk-based approach. We encourage OSTP to draw upon the work led by NIST to define an AI Risk Management Framework.[5] We support NIST's commitment to adopt an approach that is flexible, outcomes-based, and designed to secure positive influences of AI systems while minimizing their potential negative impacts.[6]

Conducting impact assessments

Impact assessments can play an important role in identifying and mitigating the sociotechnical risks of specific AI deployments. At Microsoft, completing an impact assessment is the first step in our Responsible AI by Design process. Assessments are conducted by multi-disciplinary teams, which include product managers, data scientists, designers, and product counsel, and with the benefit of input from user research. By interrogating a system's purpose, stakeholders, intended uses, deployment geographies, and failure modes, among other things, assessment teams gain a deeper understanding of the impact of their AI systems and how to design effective mitigations for potential harms. Further, Microsoft uses the outcomes of individual assessments to inform other product cycles: many common mitigations and effective strategies have been incorporated into our Responsible AI Standard as standard product development requirements for AI systems. These standard procedures include a structured process to identify, measure, and mitigate potential fairness-related harms of AI systems,[7] and requirements to establish feedback channels and ongoing evaluation procedures.

[4] For example, the Partnership on AI has produced a helpful paper explaining how different types of facial recognition systems work. This paper was the result of a series of workshops on facial recognition systems convened by PAI between September 2019 and January 2020. It brought together Partner organizations and communities developing, engaging with, and affected by these systems. Partnership on AI, Understanding Facial Recognition Systems (2020), http://partnershiponai.org/wp-content/uploads/2021/08/Understanding-Facial-Recognition-Paper_final.pdf.

[5] NIST, *AI Risk Management Framework*, https://www.nist.gov/itl/ai-risk-management-framework.

[6] Response of Microsoft Corporation to NIST RFI on an Artificial Intelligence Risk Management Framework (Sept. 15, 2021), https://www.nist.gov/system/files/documents/2021/09/16/ai-rmf-rfi-0088.pdf.

[7] We focus on three types of fairness harms: quality of service, allocation harms, and representational harms.

Facilitating the responsible use of facial recognition technology

In addition to proactive harm mitigation, we encourage our teams to engage in systems-level thinking about the technology they are developing. This thinking keeps people at the center of AI systems and highlights additional steps necessary to facilitate responsible deployments by our customers.

Microsoft makes its facial recognition technology available through cloud-based application program interfaces (APIs) that can be called by our customers. In this model, our facial recognition API, Face API, is a building block that our customers use to create a facial recognition system. A facial recognition system includes the technology as well as the people who will use it, the people who will be subject to it, and the environment in which it is deployed. To be fit for purpose, the facial recognition system must be both a valid solution to the problem it is intended to solve and a system that warrants trust by individuals and society.

Compared to more traditional forms of software development, creating an AI system that is fit for purpose requires greater knowledge transfer between developers of the technology and deployers of the system. This is because decisions about how to deploy a system, including the societal context in which it is used, have a significant impact on any potential risks the system may generate. As such, it is important that deployers have the information needed to make responsible deployment decisions and identify and address any potential risks. Through our facial recognition work, we have developed effective mechanisms and channels for information transfer between developer and deployer. In particular, our Face API Transparency Note communicates—in understandable language aimed at non-technical audiences—how Face API works, the choices deployers can make that influence accuracy, and the importance of thinking about the whole system during deployment. [8] The Note also clearly explains the importance of keeping a human in the loop for deployments of Face API. This type of stakeholder communication is an important practice to secure the responsible deployment of the technology.

Developers must go beyond creating technologies that meet needs and social expectations and ensure that AI systems are tested to ensure their deployments take into consideration safety concerns, as well as concerns of individual rights and those around democratic norms. Microsoft believes that it is incumbent on developers to not just undertake their own testing prior to releasing technology, but also to facilitate testing by independent third parties and participate in established benchmark testing programs such as NIST's Ongoing Face Recognition Vendor Test. While there are some respects in which NIST's tests would benefit from modernization and refinement, benchmark testing is important to enable comparisons across vendors and develop an understanding of the state-of-the-art of the technology. However, as with all testing, benchmark tests only indicate how the technology will work in conditions that reflect the benchmark data, and there will always be limits on the number of conditions that benchmark testing programs can model. This then leads to the critical need for operational testing, by which we mean testing by deploying entities in the context in which the system will be used and with the people who will interact with the system. Microsoft provides guidance on specific considerations for conducting operational testing in the "Plan for an evaluation phase" section of our Face API Transparency Note. This includes information about the importance of collecting ground truth

[8] Microsoft AI, Transparency Note: Azure Cognitive Services: Face API (2019), https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20(March%202019).pdf.

evaluation data, considering factors such as sensor position and lighting, and seeking feedback from the people who are operating the system and those who are impacted by the system.

Common uses of facial recognition technology

Customers use Microsoft's facial recognition technology in a wide range of applications. Set out below are some common uses of facial recognition technology that we believe can be deployed with known, effective safeguards like those that Microsoft has implemented through its Facial Recognition Principles. We also believe that these safeguards can be included in new regulations and laws, further described in the next section.

- **Facial Verification to Access Secured Devices and Services**. Face API is frequently used to verify a person's identity to grant them access to secured devices and services, for example by matching a selfie against another photo on file to prove identity and enable a product or service. National Australia Bank, for example, has experimented with using Microsoft's facial verification technology to allow customers to withdraw money from an automated teller machine without using a bank card.[9]

- **Touchless Access Control.** Face API is often used to enable enhanced touchless access experiences. With appropriately trained human supervision, facial recognition can help individuals complete check-in processes at airports, stadiums, theme parks, and other high-traffic areas. In addition to speeding up the process and reducing the burden of producing a physical method of authentication, facial recognition technology minimizes the risks posed to hygiene and security from the loss or theft of physical methods of authentication such as credit cards or tickets.

- **Personalization.** Face API can be used to enable ambient personalization and enrich experiences on shared devices. For example, where meaningful explicit consent experiences are implemented, devices that know an individual, such as home computers and work kiosks, can recognize those individuals and provide personalized services, such as hands-free interaction or directions to a meeting. These deployments also assist individuals with dyslexia and other disabilities for whom character input requirements (i.e., passwords) may be burdensome.

- **Enable Accessibility.** Microsoft projects, such as Seeing AI[10] and Project Tokyo,[11] use facial recognition technology to provide more immersive social experiences for people who are blind or low vision.

[9] Microsoft News, *NAB and Microsoft Leverage AI Technology to Build Card-Less ATM Concept* (Oct. 23, 2018), https://news.microsoft.com/en-au/2018/10/23/nab-and-microsoft-leverage-ai-technology-to-build-card-less-atm-concept/.
[10] Microsoft, *Seeing AI*, https://www.microsoft.com/en-us/ai/seeing-ai.
[11] Microsoft, *Project Tokyo*, https://www.microsoft.com/en-us/research/project/project-tokyo/; John Roach, *Using AI, People Who Are Blind Are Able to Find Familiar Faces In a Room*, Microsoft (Jan. 28, 2020), https://news.microsoft.com/innovation-stories/project-tokyo/.

- **Digital Access and Cybersecurity.** According to a recent Government Accountability Office report, sixteen U.S. federal agencies rely on facial recognition technology for digital access or cybersecurity. Uses range from unlocking devices with facial recognition to identity verification of individuals using government websites.[12] These authentication tools are important assets to prevent cybercrime and other malicious actions taken on digital devices.

- **Law Enforcement.** Law enforcement agencies use facial recognition technology for a range of use cases, including identification of victims of crime, missing persons, and other investigative efforts. While Microsoft believes that certain use cases can support the public interest if guided by appropriate legislative guardrails like those outlined in the section below, we also recognize that the United States has a strong need for a whole-of-society conversation about how the police should—and should not—use facial recognition technology. In 2020, as the nation's attention turned to issues at the intersection of racial equity and policing, Microsoft affirmed our policy position that we will not sell facial recognition to police departments in the United States until a strong law, grounded in human rights, has been enacted. It is our hope that this position will help create space for the much-needed societal conversation about the use of advanced technologies, such as facial recognition, in policing.

New Laws Are Needed, and Effective Safeguards Have Been Identified

While Microsoft will continue to uphold our Facial Recognition Principles and exercise restraint in decisions about the design, development, and deployment of our technology, we remain convinced that regulation of facial recognition technology is essential and time sensitive. In particular, we need strong laws grounded in human rights to provide people with protection under the law and avoid a commercial race to the bottom. Our position on regulation is informed by our internal work developing company-wide Facial Recognition Principles, implementing those principles through our internal governance program, and our external engagement with customers, partners, civil society organizations, academics, and policymakers. We believe there are specific, effective safeguards that can be adopted now to establish the right guardrails for the beneficial use of the technology. For facial recognition systems deployed by government agencies, these safeguards include:

- Upfront transparency and accountability measures, such as a requirement for government agencies to adopt a publicly available facial recognition policy in advance of system implementation and to consult impacted communities on a regular basis before and after adoption.
- Requirements to only use technology that is testable by independent third parties (e.g., via an API) and subject to benchmark and operational testing on a regular basis.
- Requirements to train employees using facial recognition systems and carry out meaningful human review of decisions that impact legal rights or have similarly significant impacts on individuals.

[12] U.S. Gov't Accountability Off., Facial Recognition Technology: Current and Planned Uses by Federal Agencies (2021), https://www.gao.gov/assets/gao-21-526.pdf.

- Due process protections and record-keeping requirements, including pre-trial disclosure of the use of facial recognition technology to criminal defendants, and statutory reporting obligations akin to those imposed in the Wiretap Act.
- Restrictions on certain use cases, including:
    - A prohibition on the use of facial recognition technology for indiscriminate, mass surveillance.
    - Restrictions on the use of facial recognition to engage in targeted ongoing surveillance of specific individuals. Such use should only occur when it would provide evidence of a serious criminal offense, and when either a search warrant has been obtained or there are exigent circumstances (i.e., immediate danger of death or serious physical injury to any person).
    - A prohibition on the use of facial recognition in a manner that could discriminate based on protected characteristics, chill First Amendment activities, or otherwise infringe on human or constitutional rights.

Many of these protections have been adopted in Washington State's facial recognition law,[13] which is the first law of its kind to enact specific legal guardrails on the use of facial recognition technology by government agencies. Like most initial forays into a new legal field, the Washington law can be improved upon and will evolve with experience in the future; however, it remains an important initial articulation of safeguards that should attend government use of facial recognition technology.

Additional regulatory safeguards for commercial use cases should include:

- Requirements for commercial facial recognition service providers to:
    - build technology that is testable by independent third parties (e.g., via an API) and to implement mitigation plans in the event that independent testing reveals material unfair performance differences across demographic groups;
    - provide documentation that explains the capabilities and limitations of the technology in terms that deploying organizations and consumers can understand, and that enables deploying organizations to conduct operational testing; and
    - contractually prohibit the use of their services to unlawfully discriminate.
- Requirements for organizations deploying facial recognition technology to:
    - ensure testing in operational conditions and implementation of reasonable guidance from developers to ensure best quality results;
    - provide conspicuous and accessible notice of all uses of facial recognition technology;
    - secure explicit consent for all persistent tracking, identification, or verification tasks except in narrow security scenarios that conform to strict limits.
- Restrictions on private sector disclosures to law enforcement agencies of face templates or other personal data derived from facial recognition technology, unless such disclosure is with the consent of the individual concerned, required by law, or necessary to respond to an emergency involving danger of death or serious physical injury to any person.

[13] Wash. Rev. Code § 43.386; *see* Brad Smith, *Finally, Progress on Regulating Facial Recognition* (Mar. 31, 2020), https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/.

In addition to the safeguards set out above, the responsible deployment of facial recognition systems in commercial settings would be strengthened in important ways by the protections afforded by a comprehensive federal privacy law.

Governance as a Strong Foundation for Building AI Systems that Warrant Trust

Microsoft believes that a strong internal governance program is necessary to enact principled commitments to responsible AI and support the ongoing evolution of policies and practices that is necessary in this complex, fast-moving domain. Our approach is research-led, governed by policy, and supported by engineering systems and tools. It embraces the "hub-and-spoke" model that has worked successfully to integrate privacy, security, and accessibility into our products and services.

Our "hub" includes: the Aether Committee, whose working groups leverage top scientific and engineering talent to provide subject-matter expertise on the state-of-the-art and emerging trends regarding the enactment of Microsoft's AI principles; the Office of Responsible AI, which sets our policies and governance processes; and our Responsible AI Strategy in Engineering (RAISE) group, which enables our engineering groups to implement our responsible AI processes through systems and tools. The three groups work together to set a consistent bar for responsible AI across the company and they empower our "spokes" to drive initiatives and be accountable for them.

The spokes of our governance include our Responsible AI Champs community. The Champs are appointed by company leadership and sit in engineering and sales teams across the company. They raise awareness about Microsoft's approach to responsible AI and the tools and processes available, they spot issues and help teams assess ethical and societal considerations, and they cultivate a culture of responsible innovation in their teams.

To enact our principled commitment to responsible AI, we have developed our Responsible AI Standard, an internal set of product development rules that sets out how we enact our AI principles and that is underpinned by Microsoft's corporate policy. Now in its second version, the Responsible AI Standard recognizes the need to actively guide a process of Responsible AI by Design, including through practices such as impact assessments and fairness testing. We are engaged in the process of systematically rolling out the Responsible AI Standard across the company and building the set of implementation methods that teams can draw upon, including tools, patterns, and practices crowdsourced from within and outside the company and refined through a maturity process.

We have also established a process for ongoing review and oversight of high-impact cases and rising issues and questions, since we recognize that high-impact cases warrant additional oversight, and it is impossible to reduce all the complex sociotechnical considerations into an exhaustive set of pre-defined rules. Our Sensitive Uses process requires that use cases that meet our review criteria are reported to our Office of Responsible AI for triage and review, which includes a deliberation when there is no existing precedent to draw upon. Since July 2019, we've processed over two hundred use case reviews, including an uptick in reviews since March 2020 as more Microsoft teams and customers sought to use AI technologies amid applications and opportunities with harnessing data and AI methods to mitigate challenges with Covid-19.

We have also been engaged in work to build out the "paved road" for responsible AI at Microsoft – the set of tools, patterns and practices that help our engineering teams easily integrate responsible AI requirements into their everyday development practices. Although tooling – particularly in its most technical sense – is not capable of the deep, human-centered thinking work that needs to be undertaken while conceiving AI systems, we think it is important to develop repeatable tools, patterns, and practices where possible so the creative thought of our engineering teams can be directed toward the most novel and unique challenges, not reinventing the wheel. Integrated systems and tools also help drive consistency and ensure that responsible AI is part of the everyday way in which our engineering teams work. Our AI development platform, AzureML, serves as the foundation for this paved road, so that our customers will also benefit from our development of engineering systems and tools. Our Responsible AI Dashboard is our most recent release: it's a single pane of glass that brings together several mature responsible AI tools in the areas of machine learning interpretability, unfairness assessment and mitigation, error analysis, causal inference, and counterfactual analysis. This helps developers undertake holistic assessment and debugging of models and is the product of deep research-to-practice collaborations between our Aether community and engineering teams over several years.

Key Considerations for Effective AI Policymaking

Microsoft believes that policymaking for AI generally and facial recognition technology specifically must be approached with a deep understanding of the technology and its use cases as well as a clear understanding of the problems regulation seeks to solve. Answering these questions will require broad input from stakeholders who develop, deploy, or are impacted by AI systems. OSTP has begun this discussion thoughtfully in the current RFI and its other consultation initiatives. In addition, AI regulation will need to fit into existing laws and regulatory schemes: gaps and areas for improvement should be identified before proceeding. To this end, Microsoft endorses a review of the adequacy of existing civil rights enforcement authorities as recommended by the BSA | The Software Alliance in its RFI response of January 13, 2022. Finally, we believe that government, industry, civil society organizations, and other stakeholders must be agile when working to secure rights-respecting outcomes in a complex, fast-moving domain; this will likely require an incremental approach to policymaking.

Conclusion

Microsoft appreciates the opportunity to contribute its learnings from its facial recognition and governance efforts and welcomes further dialogue on these topics as OSTP progresses its Bill of Rights initiative. We stand ready to assist OSTP in shaping the guardrails to ensure that AI and other data-driven technologies serve society equitably and respect the enduring values of American democracy.

Sincerely,

Natasha Crampton
Chief Responsible AI Officer
Microsoft Corporation

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

MITRE Corporation

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

About MITRE

The MITRE Corporation is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers, participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program. Working across federal, state, and local governments—as well as industry and academia—gives MITRE a unique vantage point. MITRE works in the public interest to discover new possibilities, create unexpected opportunities, and lead by pioneering together for public good to bring innovative ideas into existence in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

MITRE does not produce or sell biometric technologies, nor competes to operate systems, but does have a long history of providing data- and evidence-driven support to federal agencies in the areas of biometric research, development, testing, and evaluation; system prototyping and design; acquisition guidance; and operational policies. We focus on providing accurate, unbiased, information and guidance without attempting to influence decisions to any particular outcome. MITRE also occasionally performs independent research on priority biometric issues that lack private sector motivation or ability. MITRE's Duane Blackburn also previously worked at the Office of Science and Technology Policy (OSTP) for eight years, across two administrations, where one of his duties was coordinating interagency activities on biometric technologies.

Introduction and Overarching Recommendations

Biometric technology is a powerful tool that can be used to achieve many positive outcomes or could also lead to harms if used incorrectly—this has led to much debate within the policy community. Biometrics are also incredibly complex and nuanced, which has led to a staggering volume of mis- and disinformation from those seeking to influence the policy community. Effective biometrics policies and regulations must be based on data, evidence, and experience. Yet, many of the nation's policy actions and proposals on biometric technologies have been driven by advocate messaging (both for and against) or inaccurate analyses that mistakenly conflate biometrics with other technologies, fail to differentiate between algorithms and systems, or fail to recognize the breadth and depth of existing technical and operational analyses, evidence-based policies, and national and international standards and best practices. Within this response, MITRE provides unbiased recommendations and insights on biometric technology and policy considerations so that OSTP has an accurate, unbiased, foundation on which to review Request for Information (RFI) responses and determine their subsequent actions. MITRE stands ready and willing to assist and advise going forward, as OSTP deems appropriate.

OSTP and the National Science and Technology Council (NSTC) have a long and distinguished history leading federal and national efforts on biometric technology. The NSTC Subcommittee on Biometrics and Identity Management (BIdM) led efforts far beyond the NSTC norm of coordinating research and development activities by also tackling other important issues such as terminology, standards development, privacy practices, public education, and public-private

collaboration.[1] Even though this Subcommittee expired approximately ten years ago, its interagency members continue to gather throughout the year to exchange information and provide mutual mentoring, to host the government's annual identity conference, and to collaborate on special projects. Going forward, MITRE strongly recommends that OSTP leverage these prior and ongoing activities, existing policies, and experienced interagency personnel within their biometrics efforts.

Overarching Recommendation #1: Follow NSTC policy and international vocabulary standards. This RFI's definition of biometrics does not align with existing NSTC policy or international standards, which will create confusion, complicate policy analyses, and likely lead to incorrect policy decisions.[2] It intermingles (identity) biometrics with inference of emotion/intent and in a couple of occasions also folds in the biological and medical community's use of the word "biometrics" (to generically describe any biological-based data). Those are three different categories of technologies/issues that have different backgrounds, uses, and operational considerations and should have distinct policy analyses. To ensure clarity and to promote proper analysis, all references to biometrics in this MITRE response are limited to identity matters and discussion of other topics will specifically state so without using that term.

Policy matters for biometric technologies was also a focus for OSTP in the years following the 9/11 terrorist attacks. Complicating factors at that time were insufficient knowledge about these then-new technologies and inconsistent use of terms, which led to conflating different technologies and risks. NSTC BIdM attacked this problem, in part, by developing a *Glossary* document, and an aspect of its approval by parent NSTC Committees included direction to federal entities to consistently align with these definitions within their future activities and materials.[3,4] For the most part, federal agencies have done so for the past fifteen years, and the NSTC's *Glossary* document later served as a reference input in the development and updates of international biometric vocabulary standards.[5]

Overarching Recommendation #2: Ensure policy decisions are evidence- and science-based. MITRE strongly recommends that OSTP's biometric activities be based on reasoned analysis of data and evidence, as intended by the *Foundations of Evidence-Based Policymaking Act of 2018* (P.L. 115-435) and called for in the NSTC's *Protecting the Integrity of Government Science*.[6,7]

Much of the national conversation today *against* biometrics resembles the conversations *for* them twenty years ago: driven not by data and evidence but rather on misguided assumptions of their capabilities and Hollywood-inspired visions of operational systems that use them. A large

[1] Blackburn, Duane and Garris, Michael. A National Science and Technology Council for the 21st Century. 2021. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-2388-national-science-technology-council.pdf.

[2] ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37: Biometrics. 2017. ISO, https://www.iso.org/standard/66693.html. Last accessed January 8, 2022.

[3] This Glossary is available within the Subcommittee's compendium document Biometrics "Foundation Documents" at https://apps.dtic.mil/sti/pdfs/ADA505048.pdf, page 24.

[4] At the time this Subcommittee reported to both the NSTC Committee on Technology and the NSTC Committee on Homeland and National Security. The Subcommittee was shortly thereafter rechartered as the Subcommittee on Biometrics and Identity Management, reporting solely to the NSTC Committee on Technology.

[5] ISO/IEC 2017.

[6] Foundations for Evidence-Based Policymaking Act of 2018. 2018. United States Congress, https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf.

[7] Protecting the Integrity of Government Science. 2022. The White House, https://www.whitehouse.gov/wp-content/uploads/2022/01/01-22-Protecting_the_Integrity_of_Government_Science.pdf.

portion of current policy analyses and news articles on this topic are not accurate, rendering subsequent recommendations or actions based on them to be flawed. Unfortunately, it appears that some of the discussion and questions in this RFI have been influenced by these faulty analyses. "When bad information becomes as prevalent, persuasive, and persistent as good information, it creates a chain reaction of harm."[8]

Biometric technologies and the systems that use them are very complex and nuanced, making it difficult for well-meaning but inexperienced entities to develop accurate analyses. There are also several entities that appear to be much more driven to *influence* audiences (both for and against biometrics) rather than to *inform* them in an accurate and non-biased manner.[9] While this has disappointingly become commonplace for many debatable topics within the current national environment, these works are in many cases driving the modern policy dialogue on biometrics. Reasoned analysis and policy decisions, based on data and evidence, prevailed twenty years ago. It must similarly prevail today as well.

Overarching Recommendation #3: Biometric policy decisions need to be specifically focused and nuanced. There are multiple biometric modalities (face, finger, and iris recognition being those predominantly used by federal agencies, with rapid DNA growing) and several existing and potential use cases—with all having unique technical, operational, and policy considerations. Analyses or policy decisions that are proper for one modality and one use-case are most likely inaccurate for others. OSTP's future work must therefore be specifically focused to be accurate. Relatedly, policy analysis on attribute and cognitive or emotional state inference technologies will be decidedly different than for biometrics, and the same holds true for biological and medical data. There will be some overlap of concerns, and maybe even a few aligned best practices, but wholesale conflation of the different capabilities must be avoided.

Questions Posed in the RFI

2. Procedures for and results of data-driven and scientific validation of biometric technologies...

Biometric technologies have a long history of being subjected to scientific evaluation and held to high academic rigor.[10,11] There are several active academic conferences and journals dedicated to the development and testing of biometric systems. [12,13] Biometric examiners can also achieve

[8] Commission on Information Disorder Final Report. 2021. Aspen Institute, https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf.

[9] D. Blackburn, Two National Academies Recs for NIST Have Value for Wider R&D Community. 2021. https://www.linkedin.com/pulse/two-national-academies-recs-nist-have-value-wider-rd-duane-blackburn/. Last accessed December 7, 2021.

[10] Overview of the NIST Face Recognition Vendor Test, from 1994 to present. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt Last accessed December 22, 2021.

[11] For instance, the IEEE Biometrics Council, https://ieee-biometrics.org. Last accessed December 22, 2021.

[12] For instance, the IEEE Biometrics: Theory, Applications, and Systems conference. Last accessed January 6, 2022.

[13] For instance, the IEEE Transactions on Information Forensics and Security routinely accepts biometrics papers. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206 Last accessed January 6, 2022.

professional certification.[14,] One can even earn accredited academic engineering degrees in biometrics.[15]

Properly designed and implemented evaluations have played significant roles in the further development of multiple biometric modalities and in planning their use in federal (and other) operations. The two largest current issues in biometric evaluations are below:

- A community-wide lack of explaining evaluations to non-expert audiences so that the results and their relevancies are generally understandable. This results in external entities picking up the slack to explain the findings, even if they do not have the knowledge, insights, or desire to do so accurately.
- An increasing number of biometric evaluations (usually performed by entities advocating for or against the technology) that do not follow international biometric evaluation standards and/or fail to meet minimum statistical significance requirements, yet nonetheless are embraced and promoted in news articles or policy analyses and recommendations as providing "scientific evidence" about biometric technology.[16]

The NSTC BIdM previously produced a paper, *Biometric Testing and Statistics*, to explain key concepts, procedures, and metrics to the public.[17] More recently, the FedID document *Biometric Face Recognition: References for Policymakers* similarly provides introductory and intermediate overviews of testing and evaluating biometric technologies specifically for legislators and policymakers.[18] The NSTC BIdM also drove U.S. engagement with the international community to develop and refine international standards for biometric testing, which includes principles and frameworks, methodologies for the three types of performance evaluations, modality-specific testing, and quantifying performance variation across some demographic groups.[19] MITRE strongly recommends that OSTP, and others interested in this topic, study these papers and standards. Summaries of key takeaways are described below.

Biometric Evaluation Axiom: Different types of evaluations provide different insights. *Corollary: Improperly taken "insights" are usually inaccurate.*

Biometric algorithms and other system components, as well as human-system interaction, must be extensively tested to identify necessary future research, to inform decisions while planning operational systems, and to monitor operational performance. The international biometrics community has long coalesced around three types of evaluations, with each serving a different purpose. It is critical for policymakers to understand the differences among the three and how to properly consider their results.

[14] For instance, the Latent Print Certification from the International Association for Identification, https://theiai.org/latent_requirements.php, Last accessed December 22, 2021.

[15] For instance, West Virginia University Biometric System Engineering: https://admissions.wvu.edu/academics/majors/biometric-systems-engineering.

[16] ISO/IEC 19795-1:2021, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. 2021. International Organization for Standardization, https://www.iso.org/standard/73515.html. Last accessed December 7, 2021.

[17] This document is available within the Subcommittee's compendium document Biometrics "Foundation Documents" at https://apps.dtic.mil/sti/pdfs/ADA505048.pdf, page 149.

[18] Biometric Face Recognition: References for Policymakers. 2020. FedID, https://www.mitre.org/sites/default/files/publications/biometric-face-recognition-references-for-policymakers.pdf.

[19] Standards by ISO/IEC JTC 1/SC 37. 2021. ISO, https://www.iso.org/committee/313770/x/catalogue/. Last accessed December 21, 2021.

- Technology Evaluations assess the abilities of biometric recognition algorithms only; they do not evaluate other components that are necessary in operational systems. They typically involve massive numbers of subjects in standard data sets so that performance variation across different algorithms can be measured and compared. Results from these evaluations are used to identify areas that require additional research or as a first step in selecting an algorithm for operational use. Highlighting any result from a technology evaluation and claiming that to be the expected outcome within an operational system will almost always be incorrect.
  - The National Institute of Standards and Technology's (NIST) biometric technology evaluations are considered the gold standard of biometric technology evaluations.
  - Testing organizations must carefully consider the makeup of test data to ensure it can provide accurate and useful evaluation results. Reproducibility requires datasets that are publicly available and/or available via data sharing agreements. Results from evaluations that use vendor or advocate datasets that are not openly shared are suspect.
- Scenario Evaluations enable initial assessments of how a full biometric system (which includes a biometric recognition algorithm as one of several of its components) will perform in a *specific* use case. A mock-up of the anticipated operational environment is created, and humans are used as live subjects throughout the evaluations. Scenario evaluations involving multiple different systems would have the same environment and subjects, but they would receive their own input data from the live subjects.
  - Results from scenario evaluations offer a good understanding of how an individual system will operate in the real world for that one specific use case and population, thus providing potential operators input on selecting systems and establishing operational procedures. Different systems will likely have different results for the same use case and results for one system will vary from one use case or population to another; assumptions that other systems will perform the same as the tested system, or that the tested system will perform similarly in different use cases, will usually be inaccurate. The DHS-sponsored Maryland Test Facility's Biometric Technology Rallies are examples of scenario evaluations.[20]
- Operational Evaluations are evaluations of a specific system in a specific use case while it is in use. They do not usually measure accuracy directly (though it can sometimes be feasible), but rather analyze other factors such as cost, workflow impact and user experience. Results from operational evaluations are typically used to enhance procedures within the operational system. Annual reports on usage and timing from the major biometrics systems are examples of operational evaluations that are performed continually. U.S. Customs and Border Protection has performed several operational evaluations, for example.[21]

[20] Biometric Technology Rally. 2021. Department of Homeland Security, https://www.dhs.gov/science-and-technology/biometric-technology-rally. Last accessed December 13, 2021.

[21] M. Mason. Biometric Breakthrough - How CBP is Meeting its Mandate and Keeping America Safe. 2021. U.S. Customs and Border Protection, https://www.cbp.gov/frontline/cbp-biometric-testing. Last accessed December 13, 2021.

Biometric Evaluation Axiom: Evaluations must meet statistical significance requirements and be sufficiently documented to be repeatable. *Corollary: Evaluations that do not meet these requirements should be ignored.*

Properly measuring the accuracy of a biometric recognition algorithm or system in a nonbiased and statistically significant manner is complicated, time-consuming, and costly. Parameters that may at first seem inconsequential can have significant ramifications, leading to incorrect results. National and international standards for biometric performance testing and reporting should be followed with any deviation from the standard being documented in detail. The reliability of results from evaluations that do not follow these standards are highly suspect.

Evaluation protocols must be precisely designed to ensure accurate and nonbiased results. One major consideration is the makeup of the test database, which must be studiously developed to produce accurate evaluation results. (A dishonest evaluator can produce whatever result desired by improperly modifying the makeup of the database and system parameters.) Evaluations must also be thoroughly documented so that external entities can repeat the evaluation and receive statistically similar results. There have unfortunately been a few widely-referenced evaluations that failed these requirements—anyone with biometric knowledge could easily tweak their parameters in ways that nonexperts wouldn't see to produce wildly better or worse outcomes.

All evaluations, including those of biometric technologies, must follow common statistical significance requirements. Otherwise, the results may not be trustworthy. For biometric evaluations, the fidelity of the accuracy measures depends on the numbers of individuals used and comparisons made. Evaluations with higher numbers of individuals and comparisons will provide more precise results. Evaluations with only a few dozen individuals or comparisons often have high error variances, making their measurements (and any analyses based on them) suspect. Biometric modalities used in major federal government systems (such as fingerprint, face, iris, or DNA) now have such low error rates that evaluations must have massive numbers of test subjects and comparisons to reach statistical significance.

Biometric Evaluation Axiom: Evaluation metrics will vary based on the type of evaluation (technology, scenario, and operational) AND the operating mode of the biometric. *Corollary: The metrics for each are not interchangeable, and trends seen in one metric do not always hold for others.*

Biometric systems function in one of three different modes, as discussed below:

Verification, where there is a 1:1 comparison of the live subject to their claimed identity in the system. A conceptual example is when a foreign national enters the United States, his or her face may be compared against a visa photo to verify that the traveler is indeed who he or she claims to be in their travel document.

- There are a few different acceptable metrics for verification (based on evaluator's preference), though all are mathematically linked and can be derived from one another.
- Any test reporting a true match rate must also report a corresponding false match rate (or false accept and false reject rates). It is trivial to adjust system parameters to produce a desired outcome for only one rate but doing so also usually causes the corresponding rate to fall into unacceptable ranges. Any statement that only lists one such metric, without its corresponding metric, is completely useless information.

Closed-set identification (1:many), where all potential subjects are known to be in the database and the system works to properly find them. A conceptual example is checking identities within a confined facility such as a correctional institution. An issue for awareness is that while this is the easiest evaluation to perform (and does provide useful insights), there are relatively few operational activities that function in this mode.

- In some closed-set applications, systems are setup without a threshold setting so systems will return the 'best' candidate, regardless of how confident the system is in this match.

Open-set identification (1:many), where the system attempts to see if a subject is in the database. Conceptual examples include checking for duplicate drivers' licenses or to identify a criminal suspect. An issue for awareness is that this is the most complex mode to evaluate, as it contains considerations and issues found while evaluating both verification and closed-set identification.

- Note that there is no "biometric surveillance" function, despite how often it is discussed in policy advocacy materials. Widespread surveillance is a use-case, much more discussed in theory than found in actual operation, which leverages multiple interconnected biometric systems performing open-set identification functions.

Acceptable accuracy metrics for each function are different, and measured accuracy trends within one function do not necessarily show up similarly for the other two functions. This is both a statistical issue as well as one of terminology, with non-experts incorrectly conflating statistical metric nomenclature across the functions. The previously mentioned NSTC BIdM and FedID documents explain proper metrics for each in detail.

3. Security considerations associated with a particular biometric technology…

The IT security implications of the collection, storage, and utilization of biometrics data have been well understood by the community for many years. MITRE is therefore instead predominantly focusing on the new risks associated with genomics data at the intersection with modern medical practice in answering this question.

In general, the deployment of computational artificial intelligence has highlighted deficiencies in consideration of the ethical applications of the technologies utilizing them. In many cases, fundamental principles of the ethical treatment of persons were not considered, which was originally described as the principles of "respect for persons" and "do no harm" in the Belmont Report.[22] MITRE recommends the implementation of a holistic ethics assurance approach that prevents the violation of ethical rights and requires the development of a lifecycle ethical analysis process to achieve equitable and actionable ethics within AI applications.

In recent years, various technologies have expanded the depth and breadth of analyses that can be applied to personal information, presenting means to collect and extract more useful information while diminishing the anonymity and privacy that once existed within the data. The expansion of technologies for evaluating identity, ancestry, and health come with the downstream concerns of the equitable and protected collection, storage, and transmission of this data. Differential privacy considerations and tradeoffs should be reviewed with each technological advance to ensure balance of information privacy and information utility. The

[22] The Belmont Report. 1979, Department of Health, Education, and Welfare, https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf.

utility of genomic information with current technologies could pose potential for longitudinal privacy leakage as new technologies come online and leverage the data in unanticipated ways. An example is the identification of individuals thorough the genetic markers of related individuals, extending to multiple generations of relatives beyond the originating genome.

The development of mechanisms and technologies to safeguard these types of sensitive information must be considered and preemptively developed in parallel to the emerging technologies, assuring the protection of the rights and privacy of individuals. Expansion of technologies to leverage advances in genomics and molecular biology have opened the use of these data for identification of individuals and provides an example of exposure risk for personally identifiable information (PII). The collection of genomics data for precision medicine techniques provides a risk for the use of these data in a changed context. The same genomics data collected for medical applications such as cancer detection and characterization contain identifiable genomic markers of identity. While these data are expanding in popularity and utility in the commercial and healthcare spaces for determining ancestry and evaluating health risks, the individual is often required to weigh those benefits of precision medicine against the risks of forfeiting their privacy; moreover, the individual may not even be aware of these privacy risks.

The security of digital genomic data poses a long-term sensitivity for the information contained within it. Unlike most types of PII, the genome of an individual is relatively immutable, remains uniquely identifiable over the lifespan of the individual, and maintains sensitivity beyond the individual due to intrinsic linkages to relatives and offspring via heredity. Innovative applications for protecting these data largely remain at the academic level and are not yet realized for implementation by commercial entities, the healthcare industry, non-profit organizations, and government agencies.

Within biometric technologies, new advances in contactless fingerprint technologies allow faster and higher-throughput collection but also removes the human operator. This in turn makes operational security more difficult. The *Biometric Presentation Attack Detection Framework* has been developed as a general framework for detecting attack mechanisms for biometric technologies such as spoofing.[23] Additionally, several of the top performing face recognition algorithms have been developed by foreign entities, raising national security concerns.

4. Exhibited and potential harms of a particular biometric technology…

Oversimplified analyses. Many harms often discussed in biometric policy analyses have been based on inaccurate projections. A common example is taking a result from a technology evaluation of an algorithm and assuming the same error rates will occur in an operational system. It is important to realize that biometric systems are *emergent* systems, "where the system's behavior is a consequence of the interactions and relationships amongst its components, rather than the independent behavior of individual elements. Evaluating an operational system's performance thus requires an end-to-end (full system) analysis."[24] Measured algorithm traits from a technology evaluation don't necessarily show up in operational systems (due to actions taken

[23] ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework. 2016. ISO, https://www.iso.org/standard/53227.html. Accessed January 7, 2022.

[24] Biometric Face Recognition…, FedID 2020.

from other system components), and if they do, their impact will vary by use case and the algorithms (and other system components) selected.

Bias. One of the most-discussed concerns within policy analyses of biometrics is bias, with nomenclature issues again creating significant confusion. Technical/evaluation bias, operational bias, and prejudicial bias are different things but they are often incorrectly intermingled, which creates misinformation that significantly muddles public debate. For example: a knowledgeable individual could use a biometric algorithm with significant demographic technical/evaluation biases and develop systems that lack prejudicial bias. The same individual could also use an algorithm without measurable demographic technical/evaluation biases and develop a system with significant prejudicial bias. The two biases are not the same, even though they are commonly (and inaccurately) discussed as such in advocacy materials. This issue has been especially profound within third-party analyses of NIST's *Face Recognition Vendor Test Part 3: Demographic Effects* technology evaluation results, leading to inaccurate discussions about the report's results and what they mean for operational systems and policy considerations.[25] Additional discussion on the differences across these types of biases can be found in the MITRE document *When and How Should we "Trust the Science?"*[26] This incorrect conflation of bias terminology is not unique to biometrics, as many artificial intelligence discussions encounter similar issues, for example. MITRE recommends developing explanatory reference material and specific guidance on how to minimize all three forms of bias in biometric (and other) systems and related decision-making processes.

Privacy. The First Amendment includes free speech and free association protections, and the Fourth Amendment protects persons from unreasonable search and seizure. Critics claim biometric systems have the potential to violate First Amendment and Fourth Amendment constitutional protections because they may be used to improperly conduct surveillance activities on law-abiding persons. Legal, privacy, and civil liberties subject matter experts should advise executives, project managers, and developers, about potential risks and how to comply with constitutional, statutory, and regulatory requirements. By providing guidance through the entire project lifecycle, the risk of violating constitutional protections, privacy rights, and civil liberties can be substantially minimized. For additional discussion of privacy considerations of biometrics, please review the NSTC document, *Privacy & Biometrics: Building a Conceptual Foundation*.[27]

6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case…

MITRE is not aware of existing stakeholder engagement best practices that are specific to biometric system design. The Organisation for Economic Co-operation and Development (OECD) recently released a report with numerous issue-agnostic models to consider for policy

[25] P. Grother, M. Ngan and K. Hanaoka. Face Recognition Vendor Test Part 3: Demographic Effects. 2019. National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8280. Last accessed November 23, 2021.

[26] D. Blackburn. "When and How Should We 'Trust the Science'?". 2021. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-1187-when-and-how-should-we-trust-the-science_0.pdf.

[27] Privacy & Biometrics: Building a Conceptual Foundation. 2006. National Science and Technology Council, https://www.hsdl.org/?view&did=463913.

and public officials to engage with citizens to shape best practices for utilization.[28] MITRE's observation of OSTP's public "listening sessions" supporting this RFI is that the sessions were beneficial in understanding concerns and emotions surrounding these technologies but were lacking accurate and nuanced insights necessary for proper policymaking.

Biometric data is PII and should be collected, stored, and shared in accordance with federal, department, and agency-specific privacy policies and procedures. Biometric specific nuances should be further discussed and will often need to be specific to individual modalities and use cases to be beneficial. Existing reference material to build from include the NSTC's Privacy and Biometrics document, International Biometrics + Identity Association (IBIA) Ethics document, Biometrics Institute's Ethical Principles, and existing international biometric standards from ISO/IEC.[29,30,31]

One of the activities within the NSTC BIdM was to establish a formal interagency process to collectively analyze national and international standards and to select those that will be used in federal biometric systems and processes. As part of this work, the NSTC issued the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* (which was later further reinforced by *National Security Presidential Directive 59*) and created the *Registry of US Recommended Biometric Standards*. [32,33,34] Upon expiration of the Subcommittee, the NSTC delegated the responsibility of maintaining the registry to NIST.

Court admissibility of biometric information in courts is dependent on meeting Daubert standard (*Daubert v. Merrell Dow Pharmaceuticals, Inc*., 509 U.S. 579).[35] The Daubert ruling established basic criteria for courts determining whether methodologies are valid to the court (pp. 592-595). MITRE recommends that the OSTP reach out to the Department of Justice, Federal Bureau of Investigation, as they frequently deploy the Daubert standard for court proceedings and have training programs for expert witnesses.

MITRE notes that the use cases and associated usability of biometrics with individuals having disabilities remains a growing and needed area of research to enable the development of mitigation and inclusion strategies.[36]

[28] Chwalisz, Claudia. Eight Ways to Institutionalize Deliberative Democracy. 2021. OECD, https://doi.org/10.1787/4fcf1da5-en. Last accessed December 21, 2021.

[29] Ethics. 2021. IBIA, https://www.ibia.org/policy-advocacy/ethics. Last accessed December 21, 2021.

[30] Ethical Principles for Biometrics. 2019. Biometrics Institute, https://www.biometricsinstitute.org/ethical-principles-for-biometrics/. Last accessed December 21, 2021.

[31] Standards by ISO/IEC… ISO, 2021.

[32] NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards. 2007. White House Office of Science and Technology Policy, https://www.nist.gov/system/files/documents/2017/04/12/nstc_policy_bio_standards.pdf.

[33]Directive on Biometrics for Identification and Screening to Enhance National Security. https://www.govinfo.gov/content/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf. Last Accessed January 07, 2022.

[34] More info available at https://www.nist.gov/itl/iad/image-group/support-registry-us-recommended-biometric-standards. Last accessed January 9, 2022.

[35] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). https://supreme.justia.com/cases/federal/us/509/579/. Last Accessed January 07, 2022.

[36] Brink, R and Scollan, R. Usability of Biometric Authentication Methods for Citizens with Disabilities. 2019. MITRE, https://www.mitre.org/sites/default/files/publications/pr19-1396-usability-biometrics-for-disabilities.pdf.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

National Association for the Advancement of Colored People Legal Defense and Educational Fund

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

New York Office
40 Rector Street, 5th Floor
New York, NY 10006-1738

Washington, D.C. Office
700 14th Street, NW, Suite 600
Washington, D.C. 20005

www.naacpldf.org

LDF
DEFEND EDUCATE EMPOWER

January 15, 2022

Submitted via electronic mail (BiometricRFI@ostp.eop.gov)

RE: OSTP RFI on Public and Private Sector Uses of Biometric Technologies

On behalf of the NAACP Legal Defense & Educational Fund, Inc. ("LDF"), we offer the following comments in response to the Office of Science and Technology Policy's ("OSTP") Notice of Request for Information ("RFI") on Public and Private Sector uses of Biometric Technologies.[1] This comment responds to the RFI by addressing the exhibited and potential harms of biometric technologies used for individual identification and the inference of emotion, disposition, character, or intent, and its racial ramifications.

Founded by Thurgood Marshall in 1940, LDF is the nation's first and premier civil rights legal organization devoted to racial justice. Since its founding, LDF has worked at the national, state, and local levels to pursue racial justice and eliminate structural barriers for Black people in America in the areas of criminal justice, economic justice, education, and political participation.[2] In each of these areas, emerging technologies, including artificial intelligence ("AI") can be used in ways which threatened the rights, freedoms, and dignity of Black people and other marginalized communities. In collaboration with advocates, activists, and attorneys, LDF has challenged the use of technology, including biometric technologies and automation, in a racially discriminatory manner[3] and has also developed principles and guardrails to protect against their discriminatory use.[4] With this experience, we submit this comment in response to the RFI.

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56,300 (Oct. 8, 2021) https://www.govinfo.gov/content/pkg/FR-2021-10-08/pdf/2021-21975.pdf.
[2] About Us, NAACP LEGAL DEF. & EDUC. FUND, https://www.naacpldf.org/about-us/.
[3] *See e.g.*, NAACP Legal Def. & Educ. Fund, SEPT 10, 2021 Comments on NIST Special Publication 1270 "A Proposal for Identifying and Managing Bias in Artificial Intelligence" letter, https://www.naacpldf.org/wp-content/uploads/2021-09-10-LDF-Comments-in-Response-to-NIST-Special-Publication-1270-Identifying-and-Managing-AI-Bias-.pdf; LDF Sends Letter Expressing Concerns Over NYPD's Compliance with the P.O.S.T. Act (February 24, 2021), https://www.naacpldf.org/news/ldf-sends-letter-expressing-concerns-over-nypds-compliance-with-the-post-act/; Press Release, NAACP Legal Def. & Educ. Fund, Civil Rights Groups Call for Strong Guardrails in Hiring Assessment Technologies (July 29, 2020) https://www.naacpldf.org/press-release/civil-rights-groups-call-for-strong-guardrails-in-hiring-assessment-technologies/; Letter from LDF, AI Blindspot, et al. to Fed. Banking Reg. Agencies, (July 1, 2021), https://nationalfairhousing.org/wp-content/uploads/2021/07/Federal-Banking-Regulator-RFI-re-AI_Advocate-Letter_FINAL_2021-07-01.pdf; Letter from Megan Haberle, Sr. Pol'y Couns., NAACP Legal Def. & Educ. Fund, to Kathleen M. Pennington, Acting Assoc. Gen. Couns. for Fair Hous., (Aug. 23, 2021), https://www.regulations.gov/comment/HUD-2021-0033-0215; Testimony of Janai Nelson before the NYC Automated Decision Systems Task Force (April 30, 2019), https://www1.nyc.gov/assets/adstaskforce/downloads/pdf/ADS-Public-Forum-Comments-NAACP-LDF.pdf.
[4] *Principles*, Civil Rights Privacy and Technology Table, https://www.civilrightstable.org/principles/ and *Civil Rights Principles for Hiring Assessment Technologies,* July 2020, THE LEADERSHIP CONFERENCE FOR CIVIL AND HUMAN RIGHTS, http://civilrightsdocs.info/pdPrif/policy/letters/2020/Hiring_Principles_FINAL_7.29.20.pdf.

I. EDCI Tools Are Inherently Flawed and Pose Great Risks to Marginalized Communities

The use of biometric tools that aim to infer human emotion, disposition, character, or intent ("EDCI" or "emotion tools") is rapidly increasing in the government and private sectors, despite broadly identified concerns related to EDCI's technological flaws, scientific invalidity, and the ability of these tools to entrench existing racial and other bias. These risks underscore the urgent and critical need for federal intervention and oversight.

a. EDCI tools make broad assumptions about human emotion and behavior that are not scientifically supported.

Biometric technologies cannot accurately interpret all human emotion based on biological expression across all populations.[5] Rather, the use of EDCI tools assumes that a set of observable biological reactions, such as facial expressions, changes in tone of voice, or a spike in heart rate correlates to a defined list of human sentiments and characteristics.[6] This blanket assumption, however, is inherently flawed because it ignores the complexity of humans, their biology, and their emotions.[7]

In fact, psychologists and researchers have consistently noted the absence of a scientific basis supporting the use of EDCIs.[8] This is particularly because an array of social, cultural, and

[5] Cheryl Teh, '*Every smile you fake' — an AI emotion-recognition system can assess how 'happy' China's workers are in the office*, INSIDER (June 15, 2021), https://www.insider.com/ai-emotion-recognition-system-tracks-how-happy-chinas-workers-are-2021-6 ("It would be unlikely for an algorithm to accurately understand humans' highly complex emotional state via facial expressions alone."); Lisa Feldman Barrett, Ralph Adochs, and Stacy Marsella, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, *Psychological Science in the Public*, https://journals.sagepub.com/stoken/default+domain/10.1177%2F1529100619832930-FREE/pdf; *Automatic Analysis of Facial Expressions: The State of the Art*, 22 IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE 1424, 1425—27 (December 2000) https://ibug.doc.ic.ac.uk/media/uploads/documents/PAMIfinal.pdf (listing a variety of problems with automating facial expression analysis, including difficulty with the interpretation of facial expressions and the inability of AI to capture situation- and individual-specific data regarding emotional expression).

[6] Teh, *supra* note 5; Gary D. Friedman & Thomas McCarthy, *Employment Law Red Flags in the Use of Artificial Intelligence in Hiring*, AM. BAR. ASS'N. (Oct. 1, 2020) https://www.americanbar.org/groups/business_law/publications/blt/2020/10/ai-in-hiring/.

[7] Bibi Imre-Millei, *No Lies: The Problem with Biometric Emotion Detection*, OBSERVER (Mar. 20, 2021) https://theobserver-qiaa.org/no-lies-the-problem-with-biometric-emotion-detection; Jayne Williamson-Lee, *Amazon's A.I. Emotion-Recognition Software Confuses Expressions for Feelings*, Medium (Oct. 28, 2021) https://onezero.medium.com/amazons-a-i-emotion-recognition-software-confuses-expressions-for-feelings-53e96007ca63. ("Any company which currently claims to recognize emotion is confusing measurements (e.g., a scowl) with the interpretation of what those measurements mean (e.g., anger) . . . . One problem with this approach is that the posed faces in the images represent stereotypes of emotions — imitations of what we *think* a person expressing an emotion would look like) (emphasis added).

[8] *See* Barrett, *supra* note 5 at 47-48 ("At the moment, the science of emotion is ill-equipped to support any of these [emotion-reading technological] initiatives. So-called emotional expressions are more variable and context-dependent than originally assumed, and most of the published research was not designed to probe this variation and characterize this context dependence. As a consequence, as of right now, the scientific evidence offers less actionable guidance to consumers than is commonly assumed. *In fact, our review of the scientific evidence indicates that very little is known about how and why certain facial movements express instances of emotion, particularly at a level of detail sufficient*

environmental factors influence one's emotions and behaviors, and, therefore, biological expressions fluctuate based on the many factors that create one's own world experience.[9] Put differently, "[n]o matter how well an algorithm can catalogue each tiny movement in a face, each spike in blood pressure, each fiddle of the hands, the link between expression and actual thoughts, emotions, and intentions is social and cultural."[10] For example, marginalized groups may alter or conceal their natural biological expressions or emotions in white-majority or privileged spaces.[11] A Black person encountering a police officer may feel and behave differently than an individual whose community has not experienced a collective history of violence at the hands of law enforcement.[12] Similarly, women are more socialized to smile in the presence of men, even if they feel discomfort.[13] Because EDCI tools cannot account for every cultural and social influence that informs an individual's emotions and behavior, these tools cannot dependably discern the vast range of human emotions from biological expressions, and neatly correlate them to a defined list that accurately identifies ways in which all people behave and emote.[14] Accordingly, using biometric tools to infer human intention or read emotions remains seriously flawed and unreliable,[15] at best.

for such conclusions to be used in important, real-world applications.") (emphasis added); Kate Crawford, Roel Dobbe, et al., *2019 Report*, AI NOW (Dec. 2019) at 12 https://ainowinstitute.org/AI_Now_2019_Report.pdf, ("Affect recognition, which claims to 'read' our inner emotions by interpreting physiological data such as the micro-expressions on our face . . . has been a particular focus of growing concern in 2019—not only because it can encode biases, *but because we lack a scientific consensus as to whether it can ensure accurate or even valid results.* This was confirmed in 2019 by the largest metastudy to date on the topic.") (citing Barrett, *supra* note 5) (emphasis added).

[9] *See e.g.,* Dave Zielinski, *Facial Analysis Technology in the Workplace Brings Risks*, SHRM (July 9, 2020), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/facial-analysis-technology-workplace-brings-risks.aspx ("To understand micro-expressions . . . would require a deeper understanding of that one person's behaviors and not just a crowdsourced base line of everyone's expected expressions." Even in fairly homogenous cultures, it is clear that some people may use an expression to communicate an emotion, and another may use the same expression while feeling something entirely different.).

[10] Imre-Millei, *supra* note 7.

[11] Aysa Gray, *The Bias of 'Professionalism' Standards*, STANFORD SOCIAL INNOVATION REVIEW (Jun. 4, 2019), https://doi.org/10.48558/TDWC-4756 ("The standards of professionalism . . . are heavily defined by white supremacy culture—or the systemic, institutionalized centering of whiteness. In the workplace, white supremacy culture explicitly and implicitly privileges whiteness and discriminates against non-Western and non-white professionalism standards related to dress code, speech, work style, and timeliness.").

[12] *See e.g., United States v. Knights*, 989 F.3d 1281, 1296 (11th Cir. 2021), *cert. denied*, No. 21-198, 2021 WL 5869416 (Dec. 13, 2021) (Rosenbaum, J., concurring) ("Because of these circumstances, Black Americans' lived experiences make them materially less likely than white Americans to believe they have the freedom to leave an interaction with the police. . . . For Black citizens, the fear of violence often overlays the entire law-enforcement encounter.").

[13] Ursula Hess, Reginald B. Adams, Jr., et al., *Who may frown and who should smile? Dominance, affiliation, and the display of happiness and anger,* 19 COGNITION & EMOTION, 515, 516 (2005) (evaluating the impact of social roles, status, and gender on emotional expression). "Women feel that a failure to smile will be socially disapproved." *Id.* Further, "women generally have less power or status than men and . . . smiling in women is therefore a form of appeasement behaviour that is adaptive." *Id. See also* Marvin A. Hecht & Marianne LaFrance, *License or Obligation to Smile: The Effect of Power and Sex on Amount and Type of Smiling*, 24 PERSONALITY & SOC. PSYCH. BULLETIN 1332 (1998) (finding social power and gender affect the amount and type of smiling in an experimental setting).

[14] *See* Friedman & McCarthy, *supra* note 6; *see also* Will Knight, *Job Screening Service Halts Facial Analysis of Applicants*, WIRED (Jan. 12, 2021, 8:00 AM) https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/ (noting empirical emotional analysis research suggests "it is a bad idea to make psychological inferences, and therefore determine people's outcomes, based on facial data alone").

[15] Zielinski, *supra* note 9 (quoting Frida Polli, CEO of Pymetrics, a New York based AI company, who described "the science of the technology" as "extremely new and not well-validated"); *see also* Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally,* WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-

b. EDCI tools have a high risk of excluding marginalized communities from critical economic and other opportunities, subjecting them to long-lasting harms.

In addition to its technological failings, the use of EDCIs pose significant risks of magnifying and reinforcing already-present racial and other biases and discrimination.[16] And because biometric technologies are increasingly used to determine access to employment,[17] education,[18] housing,[19] and other key services,[20] they essentially function as technological gatekeepers to key opportunities in these sectors. This, coupled with historical and contemporary systemic discrimination, means the use of EDCIs may exclude marginalized communities from access to opportunities in the most consequential areas: those that affect an individual's ability to earn a livelihood, build stability, and experience safety.

For example, many employers use EDCI tools to determine if an applicant should be offered employment or promotion.[21] However, for decades Black workers have remained severely underrepresented in the highest-paying employment industries such as information technology, and professional and financial services[22] and overrepresented in lower-paying service industries, such as retail, healthcare, and food services.[23] Today, EDCI tools, like HireVue's employment

struggle-recognize-black-faces-equally/, (noting that testing of Idemia, a facial recognition software used by U.S. police, consistently produced higher match errors for women than men, reflecting a widespread difficulty of AI software to distinguish human faces).

[16] *See e.g.,* Rashida Richardson, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, 36 BERKLEY TECH L. REV. 101, 107 (2021) ("[S]ince White Americans dominate the technology sector, and, as the most research suggests, primarily benefit from racial segregation, it is important to evaluate White Americans' relationship to the problem before examining how racial segregation affects algorithmic designs.").

[17] *See* Ivan Manokha, *Facial analysis AI is being used in job interviews – it will probably reinforce inequality*, THE CONVERSATION (Oct. 7, 2019, 11:13 AM), https://theconversation.com/facial-analysis-ai-is-being-used-in-job-interviews-it-will-probably-reinforce-inequality-124790.

[18] Marcela Hernandez-de-Menendez, Ruben Morales-Menendez, Carlos A. Escobar, & Jorge Arinez, *Biometric applications in education*, 15 INT'L. J. ON INTERACTIVE DESIGN & MANUFACTURING 365, 366 (July 2021), https://link.springer.com/content/pdf/10.1007/s12008-021-00760-6.pdf ("[B]iometric identification systems are becoming popular" in educational institutions.).

[19] Rebecca Heilweil, *Tenants sounded the alarm on facial recognition in their buildings. Lawmakers are listening*, VOX (Dec. 26, 2019) HTTPS://WWW.VOX.COM/RECODE/2019/12/26/21028494/FACIAL-RECOGNITION-BIOMETRICS-PUBLIC-HOUSING-PRIVACY-CONCERNS

[20] *See e.g.*, Nadejda Alkhaldi, *Biometrics in healthcare: use cases, benefits, and things to consider,* ITREX (Sept. 14 2021) https://itrexgroup.com/blog/biometrics-in-healthcare-applications-advantages-challenges/.

[21] Manokha, *supra* note 17. For example, HireVue's EDCI tool claims to evaluate employment candidates' external expressions, such as brow furrowing, tone of voice, use of passive or active words, sentence length, speaking speed, the amount eyes widen or close, lip tightening, chin raising, smiling, and more.

[22] McKinsey & Company, *Race in the workplace: The Black experience in the US private sector*, (Feb. 21, 2021) https://www.mckinsey.com/featured-insights/diversity-and-inclusion/race-in-the-workplace-the-black-experience-in-the-us-private-sector (noting that Black workers account for only 12% of the entry-level workforce and only 7% of managerial workforce); *see also* Courtney Connley, *Why Black workers still face a promotion and wage gap that's costing the economy trillions*, CNBC (Apr. 16, 2021), https://www.cnbc.com/2021/04/16/black-workers-face-promotion-and-wage-gaps-that-cost-the-economy-trillions.html (noting it will take about "95 years before Black employees reach parity at all levels in the private sector." Further, "'Black workers, on average, are not being hired, promoted or paid according to what would signal their level of productivity based on their experience or their education.").

[23] *See* McKinsey & Company, *supra* note 22 ("In retail, 73 percent of Black workers fall into this [low-income] category; in accommodations and food service, that share is 84 percent.").

assessment, uses historical data from an employer's previous hires, and other employees in a particular industry, to learn how an employer defines a successful or "model" applicant.[24] Though neither the EDCI tool nor the employer may explicitly exclude Black applicants from job offers or promotions, the limited representation of past Black hires means the characteristics, traits, of Black applicants are also underrepresented in the data used to determine the standard for an ideal or "model" applicant.[25] Further, because an individual's environment, background, and access to opportunity shape their characteristics and the very indications of emotion that EDCI employment tools seek to evaluate, the characteristics that an EDCI prioritizes may correlate to identifiers like one's race, ethnicity, educational background, past employment opportunities, and more.[26] Thus, by applying EDCIs to an industry riddled with racial inequity and data from previous hiring and promotion patterns, there is a significant likelihood that the EDCI tool will magnify and further entrench the existing and historical biases that have resulted in low rates of Black employees. And even if an EDCI's algorithm is set to explicitly ignore information depicting race, age, and other protected characteristics from its analysis and decision-making process, the tool may exclude employment candidates based on traits that equate to the same protected characteristics it sought to avoid, without detection[27]--nevertheless creating a risk that the tool will penalize Black applicants for not conforming to the "model" employee standard. Accordingly, the unmonitored use of EDCIs risks subjecting communities that have historically been subject to discrimination to *further* exclusion from economic advancement and opportunities for upward mobility.[28]

In addition to exclusion from employment opportunities, EDCIs, if used for law enforcement purposes, again, include great risk: increased police interaction, wrongful arrest,

[24] Drew Harwell, *HireVue's AI face-scanning algorithm increasingly decides whether you deserve the job*, THE WASHINGTON POST (Nov. 6, 2019) https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ (describing HireVue's biometric hiring process).
[25] *Id*.
[26] See Knight, *supra* note 14 (noting that "HireVue's chief data scientist, says the company screens for bias on gender, race, and age by collecting that information in training data and looking for signs of bias . . . but she acknowledges that it may be more difficult to know if the system is biased on factors such as income or education level, or if it could be affected by something like a stutter"); *see also* Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 657 (2017) ("[S]ome screening protocols may rely on rationales that are facially neutral but ultimately based on impermissible classifications.").
[27] *See e.g.*, Reva Schwartz et al., *A Proposal for Identifying and Managing Bias in Artificial Intelligence*, NAT'L INST. OF STANDARDS & TECH., US DEP'T OF COMMERCE (June 2021), at 3, https://doi.org/10.6028/NIST.SP.1270-draft (noting that use of proxy criteria, such as the use of past arrests to measure "criminality" and participation in certain sports to measure "employment suitability," obscures normative choices made about the types of data incorporated into ML models). See also the Equal Credit Opportunity Act, Fair Credit Reporting Act, and the Fair Housing Act's prohibitions on intentional discrimination against protected classes through the use of proxies. Equal Credit Opportunity Act, 15 U.S.C. 1691; Fair Credit Reporting Act, 15 U.S.C. § 1681; Fair Housing Act, 42 U.S.C. § 3604(f)(1). *See also Pac. Shores Properties, LLC v. City of Newport Beach*, 730 F.3d 1142, 1160 n. 23 (9th Cir. 2013) ("Proxy discrimination is a form of facial discrimination.").
[28] See Manokha, *supra* note 17. *See also* Danyelle Solomon, Connor Maxwell, & Abril Castro, *Report: Systemic Inequality and Economic Opportunity*, CENTER FOR AMERICAN PROGRESS (Aug. 7, 2019), https://www.americanprogress.org/article/systematic-inequality-economic-opportunity/ (describing historical employment discrimination for marginalized groups); Maryam Jameel & Joe Yerardi, *Workplace discrimination is illegal. But our data shows it's still a huge problem*, Vox (Feb. 28, 2019, 8:29 AM), https://www.vox.com/policy-and-politics/2019/2/28/18241973/workplace-discrimination-cpi-investigation-eeoc (highlighting the continuation of employment discrimination against marginalized individuals, despite legal prohibitions against such discrimination).

incarceration, and other enforcement action.[29] One company's description of its emotion inferring software boasted that "[b]ased on the analysis of one's facial features, the system can calculate how confrontational, stressed, or nervous an individual is," among other metrics, and "can analyze the person's emotional response and figure out if they are up to anything suspicious."[30] [31] Research, and countless community voices, have shown that historically and contemporarily, Black and Brown communities in particular, are often mislabeled as suspicious or threatening.[32] These misperceptions have proven dangerous, frequently leading to increased interactions with law enforcement, officers' use of unjustified physical violence, and even death.[33]

EDCIs replicate and further engrain these harmful misperceptions. In a study of EDCI tools' use of facial recognition software to interpret human emotions, for example, Dr. Lauren Rhue tested two separate EDCI systems by using photographs of Black and White basketball players and found that both systems consistently misinterpreted Black faces as having more negative emotions than white faces with similar facial positions.[34] One system, Face++, interpreted Black faces as angry twice as frequently as white faces, even after controlling for their degree of smiling.[35] The other EDCI system, Microsoft, registered contempt instead of anger, and therefore interpreted Black players as expressing contempt three times more often than their white counterparts, even when their facial expressions were ambiguous and overall, registered Black faces as 20% less happy.[36] Translating these misperceptions of negative emotions into the criminal

[29] Nayef Al-Rodhan, *Behavioral Profiling and the Biometrics of Intent*, HARV. INT'L. REV. (June 17, 2016, 9:00 AM), https://hir.harvard.edu/behavioral-profiling-and-the-biometrics-of-intent/ ("[T]his biometric technology hopes to intercept an individual's hostile intent before it materializes into an actual hostile act. . . . In airports, stadiums and other public areas, the measurement of behavioral signals, such as heart rate, breathing, eye movement, body temperature or fidgeting, are expected to help identify and locate potentially dangerous individuals.").
[30] *See* Teh, *supra* note 5.
[31] See *supra* notes 5, 7, and 8. *See also* Barrett, *supra* note 5, at 47 ("Technology companies, for example, are spending millions of research dollars to build devices to read emotions from faces, erroneously taking the common view as a fact that has strong scientific support. A more accurate description, however, is that such technology detects facial movements, not emotional expressions.")
[32] *See* Jennifer L. Eberhardt et al., *Seeing Black: Race, Crime, and Visual Processing*, 87 J. PERSONALITY & SOC. PSYCH. 876, 876 (2004), https://www.prisonpolicy.org/scans/Seeing_black.pdf; Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SOCIAL SCIENCE RESEARCH NETWORK (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765 (confirming through experimental research that Black faces are more frequently interpreted as displaying hostile and/or negative emotions). *See also Stop-and-Frisk in the de Blasio Era*, New York Civil Liberties Union (March 2019), https://www.nyclu.org/sites/default/files/field_documents/20190314_nyclu_stopfrisk_singles.pdf (finding that, based on data about New York City's stop-and-frisk program, 80% of Black and Latino males who were stopped on suspicion of criminal activity were innocent).
[33] *See generally* Eberhardt et al., *supra* note 32, at 890; *see also* Brando Simeo Starkey, *'The words 'I thought my life was in danger' allow police to kill black people without fear of reprisal*, THE UNDEFEATED (June 28, 2017) https://theundefeated.com/features/the-words-i-thought-my-life-was-in-danger-allow-police-to-kill-black-people-without-fear-of-reprisal/ (noting that in the officer-involved murder of Philando Castile, a Black man reaching for his identification during a traffic stop, the police officer testified, "I was scared to death . . . I had no other choice.").
[34] Rhue, *supra* note 32, at 2—5.
[35] *Id*.
[36] *Id.* at 3.

legal system where they may be used to justify wrongly inferring criminality is reckless and perilous for Black and Brown communities.[37]

The above examples are alarming and make clear that use of EDCI tools gambles with the livelihoods, security, and safety of entire communities.[38]

II. The Use of Biometric Tools Should be Subject to Rigorous Transparency and Oversight Mechanisms to Prevent and Discerning Bias and Discrimination

Even outside of EDCIs, the rapid and unchecked expansion of biometric technologies[39] in systems of racial injustice and social inequality, gives these technologies the capacity to scale the impact of systemic discrimination in ways previously inconceivable, across a variety of domains including policing, housing, education, economic security, and more. To reduce these harms, we recommend the following:

1) Ensure that biometric tools comply with civil and human rights laws at the federal, state and local levels.

Biometric technologies risk replicating racial and other biases and discrimination, which would not only harm Black and Brown communities, but also violate federal, state and local laws.[40] Civil rights principles and legal obligations should be essential guardrails to the development of biometric tools. Accordingly, designers, developers, vendors, and users must be able to demonstrate that their use would not result in any violation of the rights of legally protected groups. OSTP should make clear that these legal obligations extend throughout the lifecycle of biometric tool and that failure to comply with those obligations can expose developers and those who use the tool to legal action.

[37] Alex Engler, Why President Biden should ban affective computing in federal law enforcement, Brookings, Aug. 4 2021, ("[L]aw enforcement agencies and companies are experimenting with using affective computing to extract personality information, detect deception, and identify criminal behavior. Yet, there is insufficient evidence that these technologies work reliably enough to be used for the high stakes of law enforcement. Even worse, they threaten core American principles of civil liberty in a pluralistic society by presuming that facial movements, physical reactions, and tone of voice can be evidence of criminality."), https://www.brookings.edu/blog/techtank/2021/08/04/why-president-biden-should-ban-affective-computing-in-federal-law-enforcement/.

[38] Crawford, *supra* note 8, at 6 ("[Affect recognition technology] should not be allowed to play a role in important decisions about human lives, such as who is interviewed or hired for a job, the price of insurance, patient pain assessments, or student performance in school".) *Id.* ("[R]egulators should ban the use of affect recognition in important decisions that impact people's lives and access to opportunities."); *see also* Al-Rodhan, *supra* note 29 ("The risks due to miscalculations, wrongful accusations or tracking of innocent suspects are immense.").

[39] *See e.g.,* U.S. Gov't Accountability Off., GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks (2021), at 16-18 https://www.gao.gov/assets/gao-21-518.pdf (noting the expansion of federal and local law enforcement agencies' use of facial recognition technology). without uniform guidance or reporting requirements, despite the technologies' many documented failings.

[40] Several jurisdictions have already began drafting or passing legislation that either ban or restrictions on the use of biometric technology in assessing job candidates, and more states have proposed similar legislation. *See* 820 ILL. COMP. STAT. 42 (2020) (Illinois); Baltimore City Council Bill 21-0001 (2021) (Maryland); Assembly Bill 3625/4211 (New Jersey; pending); Wash. Rev. Code §19.375 (2017).

2) *Ensure biometric tools are subject to rigorous transparency and oversight mechanisms at all stages withing the tools' lifecycle.*

The development, use, and datasets underlying biometric tools are often shielded from public scrutiny.[41] The complexity and opacity of many algorithmic systems, including vendors' failure to disclose how certain inputs lead to a decision, make it nearly impossible to pinpoint an exact reason for an algorithmic determination or inference, or critically, detect patterns of bias and discrimination.[42] Accordingly, rigorous transparency and oversight mechanisms should be implemented during the design, development, sale, and use of the tools. These pre[43] and post-deployment oversight mechanisms should include, but are not limited to: 1) independent audits, conducted prior to deployment and at least annually during the course of their use,[44] assessing all forms of bias and unlawful discrimination, taking into account the historical context, the industry in which the tool will be used, and anticipated methods of use; 2) a demonstration of scientific validity and effectiveness; and 3) rigorous evaluation of racial and other bias and discrimination, including racial and other adverse impact assessments.

In particular, audits should assess whether the tool's application uses the least discriminatory method available; if the parameters, training data, or other input components of the tool have been or should be updated or modified to mitigate any potential adverse impacts; whether and how the decisions, recommendations, scores, or other outputs of the tool have had an adverse impact on members of any protected class; whether the tool relies on any protected attribute or any proxy for a protected attribute to make a determination; and any new sources of adverse impact that may arise during the tool's future use; and the effectiveness of efforts identified during prior audits. To ensure transparency, the results of all audits, impact assessments, and demonstrations of scientific validity should be publicly available, disaggregated by categories of protected classes and identified proxies that correlate to those protected classes—such as geographic location and income. The vendor and users of the tool at issue should take all reasonable efforts to correct any adverse impact on protected classes including disparate treatment, disparate impact, use of proxy criteria, or any other related discriminatory impact identified in the audit—including ceasing the use or sale of the tool.

[41] Daniel Newman, *Emotional Recognition Tech – Is It Dangerous to the Recruitment Process?*, FUTURUM (April 28, 2020), https://futurumresearch.com/emotional-recognition-tech-dangerous-to-recruitment-process/ ("[C]ompanies using it rarely disclose the results of their analysis to candidates—which means they not only never get the benefit of the doubt, they also don't get the benefit of the ability to dispute the analysis."); *see also* Harwell, *supra* note 24. ("HireVue offers only the most limited peek into its interview algorithms, both to protect its trade secrets and because the company doesn't always know how the system decides on who gets labeled a 'future top performer.').

[42] See Roy Maurer, *AI-Based Hiring Concerns Academics*, *Regulators*, SHRM (Feb. 14, 2020), https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/ai-based-hiring-concerns-academics-regulators.aspx, ("Often thousands of data points have been analyzed to evaluate candidates from social media sites, words in resumes, and other available data. Many systems operate as a black box, meaning vendors of algorithmic systems do not disclose how inputs lead to a decision.").

[43] Here, pre-deployment refers to those procedure occurring when the biometric tool and/or its algorithm is first being designed, developed, trained, tested, and validated for use.

[44] The auditing obligation should extend to the developers, vendors, *and* users of the biometric tool at issue.

3) ***Ensure individuals subject to biometric tools receive advanced notice and are provided alternatives and methods to challenge the tool's application***.

Companies may not—and often cannot—explain to an individual subject to a biometric technology how the tool works, what characteristics it will assess, how the assessment relates to an ultimate determination, what happens after one is subject to a biometric tool, or how one may challenge the tool's application.[45] This leaves those subject to biometric tools largely in the dark about how and why their biometric data is used.[46] To remedy this, prior to being subject to the tool, individuals should be informed of the use of the biometric tool, the data and processes it uses, and the characteristics it analyzes to make an ultimate determination. Additionally, individuals should be provided access to the results of the tool's pre and post-deployment audits and assessments of the tool. These notifications should be provided in plain language, in an easily accessible manner, and in compliance with all laws involving disability accommodation or discrimination. After notification, the entity utilizing the tool should provide the individual with a meaningful opportunity to request a modified version of the tool's application or an alternative process not involving a biometric tool. Individuals should also be informed of the process for challenging the tool's applicability or its determinations, and the ability to seeking legal recourse.

4) Ensure engagement with impacted or historically marginalized groups and civil rights and racial justice organizations, at every stage of an algorithmic tool's life cycle, including pre-development, development, sale, and use.

The communities most impacted by systemic discrimination, both historically and contemporarily, are significantly underrepresented in the development, sale, use, and evaluation of biometric technologies. Meaningful efforts to eliminate these harms requires deep engagement with marginalized communities and the incorporation of their voices. Similarly, civil rights and racial justice organizations with a longstanding history of advocating on behalf of, and in partnership with marginalized communities—like LDF—are uniquely positioned to identify the potential harms of algorithmic tools, are able to suggest safeguards to avert those harms and should be consulted at every stage of a biometric technology's life cycle.

[45] For example, in the employment context even when job applicants are aware that a technological tool will analyze their biometric responses, they typically are not informed of the analytical processes or datasets used in a particular decision. Harwell, *supra* note 24 (Nathan Mondragon, HireVue's chief industrial-organizational psychologist, noted that "the standard 30-minute HireVue assessment includes half a dozen questions but can yield up to 500,000 data points, all of which become ingredients in the person's calculated score."). Another example is HireVue's Facial Action Units, which "assess how a person's face moves to determine, for instance, how excited someone seems about a certain work task or how they would behave around angry customers," can constitute *29 percent of a person's score*; the words they say and the 'audio features' of their voice, like their tone, make up the rest."

[46] Al-Rodhan, *supra* note 29 ("With these systems, passengers in an airport might step on a 'smart carpet' or rest on a 'smart seat' full of biometric sensors, all without their knowledge.").

5) ***Mandate the retention of all data, code, and all other information necessary to allow for subsequent independent audits and investigations regarding the lawfulness and validity of the tool.***

This should include but is not limited to records of each challenge; requests for accommodation, modification, alternative selection or identification procedure; requests to opt-out of the tool's application; the user's response to each challenge or request; and any other information that is relied upon during a pre-deployment or ongoing audit.

Conclusion

The development of AI and emerging technologies presents an array of challenges to protecting the civil and human rights, livelihoods, and security of Black and Brown communities. Federal policymakers must play a more active role to protect the civil rights of protected classes from discrimination caused or exacerbated by AI systems. We urge you make clear the applicability of existing civil rights laws to the use of AI technology and to prioritize the enactment of comprehensive regulations regarding the development of AI and other emerging technologies that respects the civil and human rights of all people.

Thank you for considering these comments. If you have any questions, please contact Katurah Topps, Policy Counsel, at [redacted] or (212) 965-2200.

Sincerely,

[redacted]

Lisa Cylar Barrett, Director of Policy
Katurah Topps, Policy Counsel
NAACP Legal Defense &
Educational Fund, Inc.
40 Rector St. 5th Floor,
New York, New York 10006

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

National Association of Criminal Defense Lawyers

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Ave.
Washington, D.C. 20504

INTRODUCTION

The National Association of Criminal Defense Lawyers (NACDL) is the preeminent organization in the U.S. advancing the goal of the criminal defense bar to ensure justice and due process for persons charged with a crime or wrongdoing. NACDL serves as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system; redressing systemic racism; and ensuring our members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level. NACDL is concerned that the rapid deployment of untested and unregulated technologies will entrench and exacerbate the racial disparities that have existed for as long as the criminal legal system, and that these technologies will undermine efforts for reform. For the reasons below, the Office of Science and Technology Policy (OSTP) should not endorse any state-sponsored biometric-tracking, -storing, or -sharing technologies nor capabilities.

The below comment focuses primarily on face recognition software because it is currently the most studied biometric technology with the most widely available analyses. That said, the entire spectrum of biometric surveillance technologies—including (but not limited to) facial recognition, gait recognition, iris and retinal scanning, keystroke dynamics, and voice recognition—poses enormous risk to already over-policed communities, depriving them of due process and reinforcing racist police practices. Advances in technology will only magnify these problems while raising additional privacy concerns associated with real-time and historical searches of videos and images.

To date, it has been difficult for defense lawyers to challenge the use of face recognition or other biometrics. When law enforcement uses such technologies, they do so surreptitiously, affording the accused and their defense counsel no notice whatsoever nor any opportunity to challenge its use. Even when notice is given, the defense is often denied needed discovery due to claims of "trade secrets" and proprietary software, leaving them unable to scrutinize and validate the tools used against their clients. These clandestine police practices impermissibly interfere with the accused's constitutional rights to a fair trial and to confront the witnesses against them.

Biometric technologies are powerful and invasive tools, especially in the hands of law enforcement. Before regulating or disseminating such tools, the Administration should first consider whether such tools have any place in law enforcement. NACDL believes they do not, and OSTP's primary recommendation regarding law enforcement's use of biometric surveillance technologies should be one of outright prohibition. And if such technology is used by law enforcement, it must be disclosed to the accused—and their defense counsel—with full transparency. NACDL's recommendations beyond a prohibition are not an endorsement of the use of such technology. Rather, they are made with the understanding that many law enforcement agencies are already using such technologies, and notice and transparency for the accused and their defense counsel are important mitigation measures.

COMMENT

Biometric surveillance technologies are incredibly powerful tools. They are also notoriously inaccurate in identifying people, particularly women and Black, Indigenous, and People of Color ("BIPOC") individuals. Even if these tools were 100% accurate, the persistent and invasive nature of the surveillance would still raise grave constitutional concerns. And in the hands of law enforcement agents—i.e., those capable of depriving people of their liberty and even their lives—these tools do more harm than good. This is especially true for BIPOC communities, who are already subjected to racially biased policing and surveillance.[1]

Biometric surveillance does not solve any longstanding problem in the criminal legal system; rather, it entrenches racist practices already thriving within it.[2] Before our society adopts

[1] *See generally* NAT'L ASS'N OF CRIM. DEF. LAW., GARBAGE IN, GOSPEL OUT (2021), https://www.nacdl.org/Document/GarbageInGospelOutDataDrivenPolicingTechnologies.
[2] *Id.* at 16-17.

new technology to solve an alleged problem, it is important that we understand both the problem(s) that new technology is attempting to solve and its supposed ability to solve it. We should not put the proverbial cart before the horse, asking what uses we can conjure for this new, potentially omniscient technology. Instead, we must first spend as much time and resources as necessary to properly identify and frame those problems that need solving. Only after that can we begin trying to determine whether the technology at issue can solve that thoroughly identified—and understood—problem.

There is simply no data to back up the idea that biometric technologies, as they currently exist or perhaps ever, are the right tools for "reducing crime" even though they are often promoted as doing exactly that. Because biometric surveillance technology like facial recognition performs worse with darker skinned individuals and women[3]—and due to racist policing practices and the racially biased databases these surveillance technologies reference[4]—the more plausible result of its rollout is to exacerbate the over-policing of BIPOC communities and feed mass incarceration.

It is also important to note that *people* write the code underlying these algorithms and *people* choose the datasets used to train them. Because *people* harbor implicit bias, and because datasets reflect past bias, the computer's instructions (i.e., its code) are tainted with what's referred to as algorithmic bias.[5] Ultimately, people are fallible. And within the criminal legal system,[6] that fallibility can determine whether someone is deprived of their liberties. The Administration should hold off on using any biometric surveillance technology that is not yet fully understood nor serves as a clear solution to a stated problem. To do otherwise gives far too much power to private companies that are designing a dangerous (and profitable)[7] "solution" without an identified problem.

[3] *See* sources cited *infra* note 8.
[4] *See* Najibi, *infra* note 8.
[5] *See, e.g.*, Rebecca Heilweil, *Why Algorithms Can Be Racist and Sexist*, VOX: RECODE (Feb. 18, 2020, 12:20 PM), https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency.
[6] Outside the criminal legal system context, biometric algorithm inaccuracies can cause drastically negative consequences in areas like unemployment insurance. *See* Todd Feathers, *Facial Recognition Failures Are Locking People out of Unemployment Systems*, VICE: MOTHERBOARD (June 18, 2021, 3:27 PM), https://www.vice.com/en/article/5dbywn/facial-recognition-failures-are-locking-people-out-of-unemployment-systems.
[7] *See* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 20 (2017), https://www.nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf ("Through different mechanisms intended to promote their own interests and profits, these [surveillance technology] companies exert control over the police long after their products have been adopted.").

NACDL acknowledges that many law enforcement agencies are already using biometric surveillance tools for all types of offenses, including low-level crimes and misdemeanors. While we oppose all biometric surveillance for all offenses, its use for low-level offenses is particularly harmful to BIPOC communities because racist police practices result in BIPOC being more frequently stopped, questioned, and arrested by law enforcement. This creates a pernicious feedback loop: BIPOC who live in over-policed communities are stopped by police at a disproportionately higher rate, regardless of offense severity; their biometrics are run against face image databases using algorithms that perform poorly with darker skin tones and women, meaning they're more likely to result in false positives; the arrest data gets fed back into law enforcements' data-driven police practices and further entrenches the biased policing of BIPOC communities, increasing the chances these individuals will again be stopped and queried against these databases in the future.

1. Facial recognition algorithms misidentify BIPOC and women's faces at a much higher rate, exacerbating an already discriminatory policing system that preys on multi-marginalized communities.

By now, it is well documented that facial recognition algorithms' performance varies based on age, skin tone, and gender. Time and again, studies have shown these algorithms' ability to match faces drops significantly when tasked with analyzing younger individuals, darker skinned individuals and women, with the worst error rates occurring for women of color.[8] This is extremely concerning, given the also well documented policing practices that disproportionately target BIPOC communities, particularly Black people.[9]

The fact cross-racial eyewitness identification has proven deeply problematic also plays a role here. Eyewitness identifications are notoriously unreliable, even more so when they are

[8] *See, e.g.*, Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV. GRADUATE SCH. SCI. NEWS (SPECIAL EDITION) (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ ("A growing body of research exposes divergent error rates across demographic groups, with the poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old. . . . [F]ace recognition technologies across 189 algorithms are least accurate on women of color."); *see also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 1 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[9] *See, e.g.*, *Fatal Force*, WASH. POST, https://www.washingtonpost.com/graphics/investigations/police-shootings-database/ (last updated Jan. 15, 2022); Lynne Peeples, *What the Data Say About Police Brutality and Racial Bias — and Which Reforms Might Work*, NATURE (June 19, 2020), https://www.nature.com/articles/d41586-020-01846-z (last updated May 26, 2021).

cross-racial.[10] Facial recognition systems, by design, seek a face in the referenced database(s) that looks like the one law enforcement agents are trying to find.[11] In other words, the system searches for a doppelganger. Furthermore, these systems (at least in the U.S.) are trained on datasets made up of primarily white, male faces.[12] As a result, facial recognition systems regularly misidentify BIPOC—especially darker-skinned women.[13]

It doesn't take much imagination,[14] then, to see where too hastily implementing facial recognition or other biometric surveillance technologies could lead: When law enforcement agencies rely on facial recognition systems that by design find a person who looks like the referenced photo and misidentify BIPOC faces at a higher rate—and then show that "match" to an eyewitness for cross-racial identification purposes—the potential for an inaccurate identification, already high, is compounded. Inevitably, people will be mis-identified, charged, and prosecuted, and the inequities faced by BIPOC communities in the criminal legal system will be exacerbated.[15]

2. Mugshot databases disproportionately include Black faces, and, regardless, the faces queried against them and other databases are disproportionately BIPOC individuals' faces.

The facial recognition techniques most widely used today involve either: 1) "face matching," the practice of comparing an unknown person's faceprint against a database of

[10] *See, e.g.*, Jed S. Rakoff & Elizabeth F. Loftus, *The Intractability of Inaccurate Eyewitness Identification*, 147 DAEDALUS 90 (2018), https://doi.org/10.1162/daed_a_00522; Laura Connelly, *Cross-Racial Identifications: Solutions to the "They All Look Alike" Effect*, 21 MICH. J. RACE & L. 125 (2015), https://repository.law.umich.edu/mjrl/vol21/iss1/5; Michael Barbella, *More Than Meets the Eye in Cross-Racial IDs*, N.J. ST. B. FOUND. (May 7, 2021), https://njsbf.org/2021/05/07/more-than-meets-the-eye-in-cross-racial-ids/.
[11] The photo of the unknown person whose identity law enforcement is trying to determine is typically called the "probe" photo.
[12] Buolamwini & Gebru, *supra* note 8; *see also* Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.
[13] *See* sources cited *supra* note 8.
[14] To be frank, it takes no imagination. Shoddy police work coupled with overreliance on facial recognition's false promise of accuracy has already caused mistaken arrests that result in nights spent in a holding cell and trauma to both the arrestee and those close to them, not to mention time spent away from home and work at things like arraignments and other court hearings. *See* Robert Williams, *I Did Nothing Wrong. I Was Arrested Anyway.*, ACLU (July 15, 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.
[15] This potential is all the more problematic because some who advocate for increasing the use of computers in policing tout the incorrect idea that because a computer makes the decision, it is somehow more objective than were a person to do so. As stated above, computer code is *created by people* who are just as guilty as anyone of exercising implicit bias. *See* Heilweil, *supra* note 5.

known faceprints to determine the unknown person's identity;[16] or 2) "face verification," the type of facial recognition that, for example, unlocks a smartphone when it recognizes the user's face.[17]

Due to historically racist policing practices, mugshot databases are themselves discriminatory, overrepresenting BIPOC because they are overpoliced and therefore arrested at higher rates.[18] Even if the referenced database were not itself discriminatory (e.g., a database of driver's license photos from one of the 32 states that permit use for facial recognition),[19] the problem persists because BIPOC—again due to racist policing practices—are stopped, arrested, and run against all databases more frequently. In other words, even if the database of faces were more representative of the country or a particular state, the faces of those who are queried against it tend to be BIPOC faces because racist police practices result in their more frequently being stopped and having their faces *inaccurately* analyzed.

Again, looking at this from a criminal legal system lens puts the concerns regarding this surveillance technology into stark relief: Members of over-policed BIPOC communities are more likely to be inaccurately matched and subject to future invasive surveillance, because the technology performs worse with darker skin tones; because BIPOC faces are disproportionately represented in mugshot databases; and, since they're more likely to be stopped or arrested, because their faces are more likely to be referenced against any database.[20]

[16] Bennett Cyphers, Adam Schwartz & Nathan Sheard, *Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-Time Tracking, and More*, ELEC. FRONTIER FOUND.: DEEPLINKS (Oct. 7, 2021), https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification ("[Face matching] is often done by taking a faceprint from a new image (e.g. taken by a security camera) and comparing it against a database of 'known' faceprints (e.g. a government database of ID photos). If the unknown faceprint is similar enough to any of the known faceprints, the system returns a potential match. This is often known as 'face identification.'").

[17] *Id.* ("Face matching can also be used to figure out whether two faceprints are from the same face, without necessarily knowing whom that face belongs to. For example, a phone may check a user's face to determine whether it should unlock . . . .").

[18] *See* Radley Balko, Opinion, *There's Overwhelming Evidence that the Criminal Justice System Is Racist. Here's the Proof.*, WASH. POST (June 10, 2020), https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/.

[19] As of 2019, at least 30 states' driver's license databases were available to law enforcement agencies for facial recognition searches. Clare Garvie, Opinion, *You're in a Police Lineup, Right Now*, N.Y. TIMES (Oct. 15, 2019), at 1:02, https://www.nytimes.com/2019/10/15/opinion/facial-recognition-police.html ("You could be picked out, investigated, possibly arrested and sent to jail, because you got a driver's license in one of these 32 states.").

[20] *See* Najibi, *supra* note 8 ("The Black presence in such systems creates a feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance. . . . [I]nclusion in these monitoring databases can lead to harsher sentencing and higher bails—or denial of bail altogether.").

3. Despite our recommendations against more biometric data and surveillance tools in the State's hands, if OSTP ultimately recommends biometric regulations, it should require full transparency.

A. No positive identification

Currently, individual law enforcement agencies and sovereigns determine whether biometrics may serve as sufficient identification to make an arrest.[21] OSTP must ensure that any time a law enforcement agency—or any entity capable of depriving liberty—relies on biometrics, the biometric is supplemented by other, adequate investigatory material.

Given the numerous problems identified above—e.g., well-documented issues with cross-racial eyewitness identification, over-policing of multi-marginalized communities; overrepresentation of Black people's faces in mugshot databases and disproportionate querying of BIPOC faces against all other databases; biometric algorithms' potential for false positives with BIPOC faces—such biometric identification methods should never be the sole evidence that law enforcement agents rely on to arrest or search an individual.

B. Providing notice and ending black box defenses

When law enforcement uses biometric surveillance technology, the accused in a criminal case must be provided notice regarding such technology's use. If the accused's liberty may be determined by (fallible) computer algorithms, then the Sixth Amendment[22] and fundamental fairness require the accused be given a chance to confront the evidence against them and validate the technology. Too often where biometric surveillance is involved, prosecution and law enforcement entities bury its use by saying it was only used for lead generation purposes. This cannot continue. As per *Daubert* and *Frye* hearings, defense attorneys must be given notice and the opportunity to assist their clients in assessing the validity and reliability of the technology used to bolster the government's case.

[21] *See Facial Recognition Technology: Part II Ensuring Transparency in Government Use Before the H. Comm. on Oversight & Reform*, 116th Cong. 4 (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Federal Bureau of Investigation), https://www.govinfo.gov/content/pkg/CHRG-116hhrg36829/pdf/CHRG-116hhrg36829.pdf (stating the FBI "pioneered" its facial recognition practices and that "photo candidates returned are not to be considered positive identification").

[22] U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . .").

There is a relevant *Brady*[23] argument to make here, too: If law enforcement used facial recognition to come up with 75 potential matches for an unidentified suspect's face, the accused, under *Brady*, has the right to know about the other 74 potential matches that the system thought looked like the face in the "probe" or "source" photo as potentially exculpatory evidence. The prosecution should not be permitted to circumvent this by simply saying the technology was used only for lead generation purposes.

Relatedly, OSTP must require that when any biometric technology is used to investigate the accused, that individual has a right to fully examine the technology so they may determine whether it in fact does what the government claims. For this purpose, the accused may require and must be permitted the assistance of relevant experts. Currently, the private companies that design these algorithms and technologies have successfully hidden their code from public scrutiny by relying on trade secret law and non-disclosure agreements.[24] This "black box" strategy should never have been permitted in the first place; but it cannot continue if biometric surveillance is to be regulated by the federal government.

The constitutional imperative is clear and unavoidable: The accused must be allowed, under discovery rules, to determine how they (and not someone else with similar biometric characteristics) were identified as the suspect that law enforcement ultimately arrested and charged.

C. Validation and standardization

We recognize that OSTP may not be the entity that would ultimately standardize biometric surveillance technologies. But we note that before biometric surveillance tech is federally regulated, there is a prerequisite to determine how it will be assessed. Doing so will better prepare all stakeholders—defense counsel, prosecutors, or computer programmers and private actors who develop the code—to facilitate the inevitable validation hearings that must occur if such technology is going to be relied upon going forward.

Standardization will promote the accused's ability to subject these discriminatory surveillance technologies to *Daubert* or *Frye* evidentiary hearings aimed at determining the

[23] Brady v. Maryland, 373 U.S. 83 (1963) (holding the prosecution must disclose materially exculpatory evidence within their possession to the accused).
[24] NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 1, at 51-52; *see also* Rebecca Heilweil, *Why We Don't Know As Much As We Should About Police Surveillance Technology*, VOX: RECODE (Feb. 5, 2020, 9:00 AM), https://www.vox.com/recode/2020/2/5/21120404/police-departments-artificial-intelligence-public-records.

technology's reliability and validity. Rather than allowing companies to dictate standards through product development or allowing law enforcement agencies to determine for themselves how much of a match is adequate before pursuing a suspect, there must be some established minimum requirements for every biometric technology. Without any form of standardization for these complex technologies, there is no way defense counsel can properly assess or validate them. Such standardization will further defense attorneys' abilities to subject these technologies to validation hearings and ultimately determine whether they have any place within the criminal legal system.

CONCLUSION

Biometric surveillance technologies provide the government with an unprecedentedly powerful tool. And that tool in the State's hands can be an incredibly dangerous one, especially when it is weaponized against BIPOC communities, already subjected to biased and excessive enforcement at the hands of police.

These biometric surveillance tools do not solve any articulated problems because they were never designed to—they were conceived, coded, and marketed by private companies looking to make a profit by selling or leasing them to law enforcement agencies. They are means without ends, "solutions" without problems. The stakes here are extremely high, and not just for those who may be convicted: The repercussions from an arrest alone can cause someone to lose their job, access to housing, or even custody of their children. Unreliable pseudo-solutions that perpetuate racist police practices should not be mainstreamed.

Rather than trying to find uses for this new technology, the Administration must first identify and understand the problems within the criminal legal system that need solving. Then—and only then—can the Administration begin to select the tools, technological or otherwise, needed to fix them. Going the reverse route, the path that law enforcement is currently on, exacerbates the harmful, racist practices already present in the criminal legal system. The Administration should hold off on any endorsement or adoption of biometric surveillance tools.

NACDL recommends that OSTP refrain from promulgating or recommending any biometric surveillance regulations, as these technologies are too powerful and too unreliable. With the understanding that various jurisdictions already use these tools and to the extent that

OSTP ultimately does promulgate regulations, it is crucial that some critical requirements be met before any wider rollout is considered.

First, biometric identification methods should never be the sole basis to search or arrest someone.

Second, defense lawyers must be given notice of any technology that was part of the investigation process. Additionally, defense lawyers must be afforded the opportunity to examine the technology to assess any potential flaws and have access to other potential candidates that the technology identified who may provide exculpatory evidence. The prosecution and the companies that design these algorithms cannot be permitted to hide behind intellectual property law when life and liberty are at stake.

Finally, biometric surveillance methods must be sufficiently standardized so that proper validation hearings may be held. Only after standardization will it be possible for peer-reviewed studies to determine key metrics, such as the technology's reliability and error rates. These factors are essential for *Daubert* and *Frye* hearings and central to the accused's due process rights.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

National Center for Missing & Exploited Children

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Submission by Ann Park on Behalf of The National Center for Missing and Exploited Children, a Nonprofit Organization, in Response to the Office of Science and Technology Policy's Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

I. Background on The National Center for Missing and Exploited Children (NCMEC) and Its Use of Biometric Technologies to Help Find Missing Children, Identify Victims of Online Sexual Exploitation, and Recover Victims of Child Sex Trafficking

The National Center for Missing & Exploited Children (NCMEC) is a private, non-profit organization created as a grassroots response to an unthinkable tragedy. In 1981, 6-year-old Adam Walsh was with his mother in a Florida shopping mall when he vanished without a trace. The search for Adam revealed many inadequacies that plagued missing children investigations at the time. There was no coordinated response to search for Adam, no AMBER Alert system to quickly deliver critical information to the public, and no place for families to go for guidance or emotional support. Revé and John Walsh endured 10 excruciating days searching for Adam before he was found murdered 100 miles away. The Walshes channeled their grief and came together with other child advocates to create NCMEC in 1984. Over the past 37 years, NCMEC has grown to become the leading nonprofit organization and the nation's congressionally designated clearinghouse and resource center on missing and exploited children issues. Today NCMEC's more than 380 employees manage numerous public-private partnerships and utilize NCMEC's unique resources to prevent child abduction, recover missing children, and combat child sexual victimization through five main programs of work relating to: (1) missing children; (2) exploited children; (3) community outreach; (4) education and professional resources; and (5) family support.

Over the past decade, crimes against children have evolved and become increasingly technology-based. In response, NCMEC has incorporated the use of biometric information, including DNA, fingerprints and dental records, along with biometric technologies, such as facial recognition, often coupled with artificial intelligence and machine learning tools, throughout its operational programs so it can continue to help identify and recover missing children and child victims of sexual exploitation and sex trafficking. While facial recognition technology is still in the early stages of development, NCMEC has found it to be highly effective in helping to identify and locate child victims of sex trafficking. NCMEC also facilitates collection of biometric information, including DNA, dental records, and fingerprints to help law enforcement and families find missing children and identify unknown deceased children. Most recently, NCMEC has paired artificial intelligence (AI) and machine learning (ML) technologies with biometric data to help identify victims of online sexual exploitation; develop potential locations of children in sexually abusive situations; and prioritize cases involving children in imminent danger.

NCMEC does not use biometric information, including facial recognition technology, or AI or ML tools in any monitoring capacity, does not have access to non-publicly available image content, and uses such technology solely to identify and locate child victims. Additionally, NCMEC's use of such technologies are limited to comparing curated sets of information relating to a missing or exploited child with publicly available images.

A. NCMEC's Programs to Combat Child Sex Trafficking and Use of Facial Recognition to Help Identify, Locate, and Recover Children Victimized by Sex Trafficking

Child sex trafficking is any instance in which a child under the age of 18 is advertised, solicited, or exploited for a sex act in exchange for anything of value (e.g., money, drugs, or food/shelter). NCMEC has received cases of child sex trafficking from every state and territory in the United States and from every community, including urban, rural, suburban, and tribal lands. There is no single pattern to how this crime is perpetrated on children, and NCMEC has worked on cases involving pimp-controlled, familial, gang-controlled, and buyer-perpetrated trafficking involving children as young as 10. To date, NCMEC has worked on more than 113,000 reports of child sex trafficking, including 17,283 reports in 2021.

NCMEC's multi-disciplinary team provides professional education, case management, clearinghouse resources, analytical support, and recovery services assistance on cases of child sex trafficking. One of NCMEC's most recently adopted and impactful tools in fighting child sex trafficking is facial recognition technology. Through a partnership with Thorn, a nonprofit organization that creates technology to combat the exploitation of children, NCMEC has access to an online advertisement aggregator tool called Spotlight, which was developed to improve the effectiveness and efficiency of identifying victims of sex trafficking. NCMEC uses Spotlight to compare images of children reported missing to NCMEC against online advertisements for sex trafficking that are compiled by Thorn. When Spotlight generates a potential match between a missing child's image and an online posting, NCMEC staff review each advertisement and compile information from the advertisement, such as the location or contact information, which can be critical to enabling law enforcement to locate and recover the child.

Most notably, Spotlight's facial recognition technology has allowed NCMEC to identify missing children who were not previously identified as potential victims of child sex trafficking by law enforcement or the child's social worker, parent or guardian. In these instances, the facial recognition powered by Spotlight not only provides a lead on locating the missing child, but also is critical to ensure that appropriate services and resources are prepared for the child upon recovery. As such, Spotlight's facial recognition technology has been pivotal in providing critical information to identify, recover, and support victims of child sex trafficking in ways that are not always possible with traditional human analyst review.

From May 12 to December 31, 2021, Spotlight identified 2,681 potential matches between children reported missing to NCMEC and online sex trafficking advertisements. Out of these potential matches, 370 were confirmed by NCMEC analysts to be accurate matches of actively missing children. Additionally, 39 matches arose from online sex trafficking advertisements where the missing children were not initially identified by NCMEC or law enforcement as possible victims of child sex trafficking.

The following examples demonstrate how facial recognition enables NCMEC to recover children from sex trafficking situations:

Case Example #1
A 14-year-old child went missing from a New York foster care facility. After a year, no leads had emerged in the child's case. NCMEC then used Spotlight to search the child's image against online escort advertisements, and 87 matches were located advertising the missing child for commercial sex over the past 8 months. Prior to this search there were no indications that the child might be a victim of sex trafficking. Based on active escort advertisements depicting the missing child, law enforcement launched an investigation and recovered the missing child within two days. Upon recovery, the child disclosed that she was forced to take photographs for the ads and was sold for sex in exchange for a place to stay.

Case Example #2
A 15-year-old child went missing from her home in Texas. After four months with no leads, law enforcement recovered the child at a hotel. The child was hospitalized, and law enforcement contacted NCMEC as they prepared to interview the child. Law enforcement suspected the child may have been trafficked for sex. NCMEC searched the child's social media accounts and phone number but located no information indicating the child had been trafficked. NCMEC then used Spotlight to compare images of the child from her missing child poster against online escort advertisements, and several potential matches were located. With this information, law enforcement conducted a trauma-informed forensic interview with the child, and she disclosed that the online escort ads Spotlight located were her images. As a result of the information provided through facial recognition, the child is now receiving services.

Case Example #3
In July 2020, a child called NCMEC's Call Center to report that her 15-year-old friend was being exploited, forced to take drugs, and sold for sex. NCMEC analysts conducted online open source searches and located the child's social media profiles, which indicated that she might be a victim of sex trafficking. Using the publicly accessible image of the child from her social media profile, NCMEC used Spotlight to search the child's face against aggregated online escort advertisements. Ads posted the prior evening were located depicting the child and another minor being sold for sex. NCMEC reported this information to law enforcement and both children were recovered that night.

Case Example #4
A 17-year-old child went missing from a foster care facility in Ohio. The child had previously gone missing and had always been recovered in Ohio. NCMEC compared the child's photo against online escort ads and found several matches, one of which appeared to depict the child in an online escort ad in Michigan from the previous day. NCMEC was able to pass this information along to law enforcement in Michigan who recovered the child shortly after receiving the lead information from NCMEC.

NCMEC has tested various facial recognition products over the years, and the accuracy of this technology has improved tremendously in the past few years. NCMEC now has such a high level of confidence in the accuracy and sophistication of facial recognition technology on the market, that it has fully incorporated this technology into its operational programs of work relating to child sex trafficking. Facial recognition has been proven effective to identify child victims of sex trafficking, accelerate law enforcement investigations to recover these child victims, and prevent future victimization.

B. NCMEC's Programs to Help Identify, Locate, and Recover Missing Children Through Use of DNA, Fingerprint, and Dental Biometric Information

NCMEC utilizes biometric technologies in its missing child case management services and forensic services to support resolution of missing and unidentified deceased child cases. NCMEC's case management team supports parents, legal guardians, social services, and law enforcement on missing child cases categorized as: (1) endangered runaways; (2) family abductions; (3) nonfamily abductions; (4) lost, injured or otherwise missing; and (5) critically missing young adults (ages 18-20). NCMEC case managers compile and analyze information relating to the child, including biometric information, depending on the circumstances of a child's disappearance, the length of time a child has been missing, and other relevant lead information. To date, NCMEC has worked on more than 386,570 reports of missing children, including 27,003 reports in 2021, and assisted law enforcement in recovering more than 376,000 missing children.

NCMEC also employs various forensic services to support missing child cases and cases of unidentified deceased children. Biometric technologies and information are especially crucial to the following NCMEC forensic services utilized to help resolve missing cases and to help identify the decreased remains of a child:

- Forensic Imaging Services: NCMEC's forensic artists age progress missing children's faces to show what they might look like today and also create facial reconstructions when an unidentified deceased child is located to increase the likelihood that someone will recognize them. To date, NCMEC has created more than 7,100 age progressions and created more than 600 facial reconstructions.
- Help ID Me: NCMEC enlists the public's help in identifying unknown deceased children by sharing facial reconstructions and case related information through this public Facebook page www.facebook.com/helpidme, which has more than 167,000 followers.
- Biometric data collection: In 2004, NCMEC began facilitating the collection of biometric data, including DNA, fingerprints, and dental records[1] relating to missing and unidentified deceased child cases. NCMEC also facilitates partnerships between law enforcement and NCMEC's forensic lab and genealogist partners specializing in DNA case work.

[1] Although dental records are not identified as part of the Office of Science and Technology Policy's definition of biometric information, NCMEC considers dental records to be a crucial biometric resource. Dental impressions can be a key identifier for a missing child, and NCMEC emphasizes that parents should know where their child's dental records are stored and how to obtain them in case of an emergency situation. NCMEC facilitates the collection of dental records and works with forensic odontologists to code and upload dental information into the national missing and unidentified person databases.

NCMEC is not currently using facial recognition technology for its missing children programs but is evaluating how this technology could benefit NCMEC's missing children programs. NCMEC staff spend significant time manually comparing images of missing children against potential images of these children on open web sources. For long-term missing children cases, where current photos of the missing child are unavailable, staff use age progressions created by NCMEC forensic artists to try to make facial comparisons. Facial recognition technology would improve the efficiency and accuracy of facial analysis and comparisons and also save staff time on manual reviews. These improved efficiencies would improve NCMEC's ability to provide actionable leads to law enforcement, resulting in faster intervention by law enforcement, and more expedient and successful recoveries of missing children.

i. NCMEC's Facilitation of DNA Comparisons and Related Biometric Processes to Help Identify Missing Children and Unidentified Deceased Children

DNA testing is a critical tool for NCMEC's work to identify missing children and unidentified deceased children. There are still many families whose child has been missing for years and who struggle for new leads and resolution regarding their loved one. When available leads have been exhausted, DNA collection and testing may be one of the few options to provide answers for these families. Since 2004, NCMEC has proactively facilitated law enforcement's collection of DNA samples from family members of missing children. These collected DNA samples are uploaded into CODIS, a national DNA database maintained by the FBI. When law enforcement locates an individual who is unable to identify themselves, or locates unidentified bodily remains, they will take a DNA sample and enter it into CODIS to search for a match against the missing person samples maintained in CODIS.

Over the past 10 years, NCMEC has used DNA to help resolve around 380 cases of missing or unidentified deceased children. Currently, NCMEC is actively using DNA information to help resolve more than 660 cases of unidentified deceased children, and NCMEC has facilitated the collection of DNA samples from around 2,430 family members related to long-term missing child cases.

The following are case examples that demonstrate the critical role DNA testing has played in NCMEC's mission to help identify long-term missing children and unidentified, deceased children:

Case Example #1
In September 1988, a 17-year-old female left her home in South Carolina and was never seen again. The child had gone missing previously and was suspected to be a victim of child sex trafficking. Law enforcement in South Carolina requested NCMEC's assistance in 2011. Originally it was thought that all known family members of the missing child were deceased, but in 2019, NCMEC tracked down a sibling and facilitated DNA collection to be uploaded into CODIS. The sibling's DNA matched to DNA in CODIS from an unidentified deceased child found in Florida in 1993. The CODIS hit confirmed that the body found in Florida was the missing child from South Carolina. The collection of DNA and the CODIS entry led to resolution of this long-term missing child case.

Case Example #2
In July 1971, the body of an unidentified male between the ages of 14 or 15 was located in Oregon. The cause and manner of death was undetermined. In April 2020, law enforcement requested

NCMEC's assistance in identifying the deceased child. NCMEC assisted in securing biometric information from the remains of the deceased child and law enforcement submitted the bone samples to a lab for DNA testing and evaluation with genetic genealogy resources. The child's remains were tentatively identified soon after DNA testing was completed. The deceased was confirmed to be a boy who left his home at the age of 15 shortly after fathering a daughter. The daughter, now an adult, was curious about her parents and had submitted her DNA to an ancestry company, which provided the lead that helped the lab confirm the child's identity.

Case Example #3
A 12-year-old girl went missing in CA in 1995. Twenty years later, NCMEC received a phone call from a woman in Mexico who had seen NCMEC's missing child poster and believed she was the missing child from 20 years ago. The caller told NCMEC that she had been abducted by a stranger in California and taken to Mexico and had just run away from the house where she was being confined with her children. In order to verify her identity, NCMEC obtained DNA samples from the missing child's mother and had them loaded into CODIS. A State Department liaison coordinated DNA comparisons, which confirmed that the caller was the missing child. Given the trauma the child had endured while missing and the insufficient similarities between the women's images and the child's age progressed images, the DNA information was key to identifying the missing child.

ii. Fingerprints

NCMEC also facilitates the collection of fingerprint records and works with fingerprint examiners at the U.S. Secret Service to code and upload fingerprints into the national missing and unidentified person databases. Fingerprints have been especially useful in helping to recover runaway children or children who have been victimized by sex trafficking and are using aliases to hide their identity.

Case Example #1
In 2006, a 15-year-old boy went missing from Pennsylvania. It was later discovered that a few days prior to the boy's disappearance, he had been taken into custody by law enforcement who had collected his fingerprints. In 2012, NCMEC facilitated getting the boy's fingerprints coded and uploaded into the national database. In 2017, NCMEC was notified that there had been a fingerprint hit in the national database to a man who had recently been arrested in Maryland. The man matched the missing boy's description but went by a different name. Law enforcement was able to confirm that the man who had been arrested was in fact the missing boy who was using an alias name.

Case Example #2
In 1985, an unidentified man between the ages of 17 and 25 was found deceased in Georgia. The man had been shot two times in the back of the head. In March 2020, NCMEC facilitated the uploading of the deceased man's fingerprints into the national database. Shortly after, NCMEC was notified that a fingerprint hit in the national database revealed that the deceased man had been identified as a 21-year-old who had gone missing from Georgia and whose prints were on file from a misdemeanor arrest four months prior to his death.

C. NCMEC's Use of Artificial Intelligence and Machine Learning Technologies to Identify and Expedite Leads Relating to Children Exploited Through the Online Distribution of Sexually Abusive Imagery

NCMEC works to combat the online distribution of child sexual abuse material (CSAM) through two core programs: (1) the CyberTipline; and (2) the Child Victim Identification Program (CVIP). Given the pervasive nature of child sexual exploitation crimes, the tremendous volume of CSAM content being shared online, and the image-intensive nature of this abuse, artificial intelligence (AI) and machine learning (ML) technologies are crucial tools that NCMEC uses to facilitate the work of both the CyberTipline and CVIP.

NCMEC does not currently use facial recognition technology for its exploited children programs but continues to evaluate use of such technology to help identify victims of online sexual exploitation. NCMEC anticipates incorporating facial recognition technology in the future to help compare facial images of unidentified children to images that may be publicly available on the internet. This use of facial recognition technology would enable NCMEC to provide a higher volume of relevant leads to law enforcement relating to an unidentified child victim's identity and potential location. Currently, NCMEC analysts manually conduct open source searches on victims as needed, but facial recognition technology would preserve staff resources and increase efficiency and accuracy in identifying victims.

NCMEC's CyberTipline serves as the global online mechanism for members of the public and online technology companies to report incidents of child sexual exploitation, including child sex trafficking, child sexual abuse material, child sexual molestation, the online enticement of children for sexual acts, and several other categories of sexual crimes against children. NCMEC's two primary goals in operating the CyberTipline are: (1) to prioritize reports indicating imminent danger to a child; and (2) to determine where the incident occurred so the report can be made available to the appropriate law enforcement agency. To date, NCMEC has received over 113 million CyberTipline reports, and the volume of content reported to the CyberTipline continues to increase. In 2020, NCMEC received more than 21.7 million reports containing 65.4 million images, videos and related contents and in 2021, NCMEC received more than 29.3 million reports containing 85 million images, videos and related content.

NCMEC's Child Victim Identification Program (CVIP) has a three-part mission to help locate unidentified child victims depicted in sexually abusive images so they can be identified and recovered; to provide information relating to previously identified child victims; and to provide survivor services to child victims who have been identified and recovered. To date, NCMEC CVIP analysts have analyzed more than 350 million images and videos and have helped law enforcement identify more than 20,000 children depicted in online CSAM.

Artificial intelligence (AI) and machine learning (ML) technologies have proven to be highly effective in helping NCMEC quickly process CyberTipline reports and compile lead information that can help law enforcement locate and recover victims of online child sexual exploitation. NCMEC uses a location prediction tool that automatically determines a potential location for incidents reported to the CyberTipline. This tool employs automated searches to process potential location information within

CyberTipline reports, thereby reducing the need for NCMEC analysts to manually look up information relating to the potential locations of reported offenders and/or child victims.

NCMEC also uses an automated machine learning tool to make connections among individuals referenced in CyberTipline reports based on an individual's name, user ID, email address, phone number, and other reported information. This ML tool enables NCMEC to group reports relating to a single offender and/or victim, thereby streamlining work needed to recover and safeguard a child victim. NCMEC also has developed an alert system based on natural language processing technology that alerts NCMEC analysts based on certain key words or phrases that indicate a child is potentially in imminent danger. This automated technology enables NCMEC to prioritize more urgent cases.

Automated image matching tools, such as PhotoDNA and Google's Child Safety Hash Matching API, are among the most powerful technology that NCMEC employs to combat online child sexual exploitation. These hash-matching tools are built into automated processes in NCMEC's CyberTipline to match hashes of newly submitted images to hashes of images previously reported to the CyberTipline and viewed and categorized by NCMEC. These tools provide multiple significant benefits. First, they greatly reduce the need for NCMEC staff to review identical images of CSAM, thereby decreasing NCMEC staff's exposure to this imagery and preventing further revictimization of the children depicted in the sexually explicit content. Second, these tools have improved overall efficiency and speed of reviewing and categorizing CSAM reported to NCMEC's CyberTipline. In 2021, NCMEC used these image matching tools to review and categorize more than 21 million images and videos and has reviewed and categorized more than 28.5 million images and videos to date.

II. Conclusion

Throughout NCMEC's nearly four decades of helping to locate missing children and combat child exploitation and child sex trafficking, it has continuously adapted to new trends of how children are victimized and implemented new technologies to combat crimes against children. As the science of various biometric technologies, including facial recognition, DNA, genealogy, forensic odontology, and fingerprint analysis, has developed in recent years, NCMEC has incorporated these new technologies to identify and locate child victims of sex trafficking and help resolve especially challenging cases involving missing children and cases of unidentified deceased children. Facial recognition greatly increased the efficiency and effectiveness of NCMEC's work to provide actionable leads to law enforcement to locate and recover child victims of sex trafficking. Previously complex missing children cases which had remained open after existing leads were exhausted, leaving many searching families without resolution, were resolved through DNA, fingerprint analysis, genealogy and forensic odontology. Similarly, as child sexual exploitation has proliferated online in recent years and technology has facilitated an explosion in the volume of child sexual abuse material being shared online, NCMEC's incorporation of AI and ML solutions, including image hashing technology, to facilitate automated processes has helped determine the exigency of child exploitation reports and the potential identity and location of children in sexually abusive situations.

As biometric technologies continue to develop in the future, it is essential to evaluate the role of these technologies in terms of how they can benefit the most vulnerable members of our communities.

NCMEC looks forward to serving as a resource to the Office of Science and Technology Policy regarding how NCMEC uses biometric technologies to help find missing children, reduce child sexual exploitation and prevent child victimization.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

National Fair Housing Alliance

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 12, 2022
Dr. Eric S. Lander
Office of Science and Technology Policy
Eisenhower Executive Office Building
Washington, DC 20502

Re: Document No: 2021-21975; Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Dear Director Lander,

The National Fair Housing Alliance submits these comments in response to the Office of Science and Technology Policy's ("OSTP") Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.[1] We applaud the OSTP for seeking input on this important topic and believe the responses below will provide fair housing and lending context for public and private sector biometric technologies. We hope our feedback will help inform the OSTP's policies to address consumer consent, privacy, racial targeting, racial profiling, and other implications of biometric technologies.

I. Summary:

We first address how biometric information is being used to identify people and make inferences them in algorithmic systems like credit scoring, facial recognition technologies, and tenant screening tools. Biometric systems are increasingly being used in the banking, financial services, and insurance (BFSI) industries. The increased usage of biometric information for banking authentication, sign-in applications, customer identification, security, and other applications, raises privacy, discrimination, and consumer consent concerns. The usage of biometric data in such cases may be used to monitor and further marginalize communities of color, women, and other underserved groups and can result in the denial of housing or lending services, identity theft, or higher premiums for homeowners' insurance.

We then go on to address security considerations associated with a particular biometric technology in the context of privacy. Massive data breaches linked to biometric data have already occurred and the potential for criminal activity and fraud, specifically identity theft, is increased after a breach. Leakage of personal data connected to an individual's biometric data can cause irreversible damage such as compromising a credit score to the extent where it is difficult for individuals to secure mortgage loans. For people of color who disproportionately have thin credit files or are credit unscorable, cybercrime due to biometric data breaches may make them vulnerable to privacy risks that prevent them from passing through the early screening stages of a credit application.

Lastly, we address the exhibited and potential harm of facial recognition. Facial recognition is used by law enforcement for surveillance which is concerning considering disparities in error rates across different demographic groups with the least consistent accuracy

[1] National Archives. (2021, October 8). *Notice of request for information (RFI) on public and private sector uses of biometric technologies.* Federal Register. Retrieved January 15, 2022, from https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

found for Black females.[2] Facial recognition for surveillance has a high correlation to insecure housing, loss of employment opportunities, and increased criminalization of surveilled people.[3] Facial recognition for surveillance is also occurring in the housing sector, including in housing owned or supported by funding from the Department of Housing and Urban Development (HUD). Responsible monitoring and oversight over the use of biometric data in the housing space is rare and ineffective. For example, HUD does not monitor the use of this highly sensitive data for the approximately 1.2 million households living in public housing. Nor does HUD carry out research or provide policy guidance for the use of biometric data and instead leaves those most vulnerable in our society to deal with the repercussions.[4] Additionally, the ramifications of false to trivial criminal allegation due to errors in facial recognition loss of access to government relief programs, and other harmful consequences, thus exacerbating existing inequalities through more difficult access to housing and lending opportunities and elevated privacy concerns. .

II. Background:

Biometrics is the automated recognition of people based on the analysis and measurement of their unique physical and/or behavioral attributes.[5] The two main types of biometric identifiers are physiological characteristics and behavioral characteristics. Physiological identifiers derive from structural information of the human body and include the following: facial features, fingerprints, finger geometry (the size and position of fingers), iris, veins, retina, voice, and DNA (deoxyribonucleic acid).[6] Behavioral identifiers include the unique ways in which individuals act, including recognition of typing patterns, mouse and finger movements, social media engagement patterns, walking gait, and other gestures[7]. Biometric technology is being used in sectors such as housing, BFSI, government, defense, and security, and is poised to enter even more sectors.[8] Biometric systems have been deployed in a variety of applications like mobile phones, consumer banking authentication, housing security systems, international border crossing, and national ID programs.[9]

Limitations to implementing biometrics-based systems include cost considerations but the major concerns are the possibility of bias, security breaches, and error rates.[10] As biometric systems become more integrated into society, there must be an effort to increase public understanding of how biometric data is gathered, used, and stored, as well as how it can be

[2] Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face recognition performance: Role of demographic information. IEEE Transactions on Information Forensics and Security, 7(6), 1789-1801.
[3] Urban, N., Yesh-Brochstein, J., Raleigh, E., & Petty, T. (2019, June 9). A Critical Summary of Detroit's Project Green Light and its Greater Context.
[4]Ng, A. (2020, June 22). *US government doesn't know how it uses facial recognition in public housing.* CNET. Retrieved January 13, 2022, from https://www.cnet.com/news/us-government-doesnt-know-how-it-uses-facial-recognition-in-public-housing/
[5] Kloppenburg, S., & Van der Ploeg, I. (2020). Securing identities: Biometric technologies and the enactment of human bodily differences. *Science as Culture,* 29(1), 57-76.
[6] Gillis, A. S., Loshin, P., & Cobb, M. (2021, July 26). *What is biometrics*? Search Security. Retrieved January 13, 2022, from https://www.techtarget.com/searchsecurity/definition/biometrics
[7] Ibid.
[8] Sonawane, K. (2016, June). *Biometric technology market size, share and Industry Forecast - 2022.* Allied Market Research. Retrieved January 11, 2022, from https://www.alliedmarketresearch.com/biometric-technology-market#:~:text=Owing%20to%20its%20unique%20characteristics,gaming%2C%20automobile%2C%20retail)
[9] Thales Group. (2021, June 2). *Biometrics: Definition, use cases, latest news.* Thales Group. Retrieved January 15, 2022, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics J
[10] Ibid.

weaponized against consumers, particularly consumers of color.[11] There must also be increased efforts to regulate how this data and systems built using it are regulated.

III. Descriptions of Use of Biometric Technology for Recognition and Inference:

Biometric technology is being used in sectors such as housing, banking, finance, government, defense, and security.[12] In fact, the global biometric technology market is experiencing exponential growth with some researchers projecting that the biometric technology market will reach $86.61 billion by 2027.[13] As current uses are expanded and more applications are created, the potential for harm to people and unintended consequences increases.

The BFSI industry is turning to biometric technology more and more to reduce risks, identify users, track consumer activity, and keep consumers satisfied by increasing the speed of banking authentication and transactions. Entities like Bank of America, Chase and PNC have given their customers the ability to save their fingerprints or face on smart devices.[14] Lenders are using biometrics to verify identities in a virtual environment where in-person loan closings are rare. Companies are also using this data to detect and mitigate fraud.

Although fingerprint authentication has its benefits, one problem it presents is that it can open the door for familiar fraud which may hurt consumers' capacity to access credit. Familiar fraud is a form of identity theft that is caused by someone familiar to a person, like a family member or friend. It is thought to be under-reported because victims may not want to strain family bonds, or they may believe that authorities may not believe them. Additionally, it may take years before someone realizes they were a victim of familiar fraud.

Axton Betz-Hamilton was one such person. In 2013, Ms. Betz-Hamiliton unearthed a credit report that was taken out by someone who had been stealing her identity since she was 11 years old.[15] She also unearthed a file containing incriminating documents and that is when she realized that the person who had destroyed her life and put her father and grandfather into debt was her now-dead mother. Her mother had "stolen" half a million dollars while Ms. Betz-Hamiliton was left with a 380-credit score, pages upon pages of fraudulent credit-card charges, and collection-agency entries in her name.[16] With a 380-credit score Ms. Betz-Hamiliton may have been faced with high premiums for auto and homeowners' coverage, difficulty renting or buying a home, and difficulty financing other major purchases.

[11] Millett LI, & Pato JN. (2010, January 1). *Cultural, social, and legal considerations.* Biometric Recognition: Challenges and Opportunities. Retrieved January 10, 2022, from https://www.ncbi.nlm.nih.gov/books/NBK219893/

[12] Sonawane, K. (2016, June). *Biometric technology market size, share and Industry Forecast - 2022*. Allied Market Research. Retrieved January 11, 2022, from https://www.alliedmarketresearch.com/biometric-technology-market#:~:text=Owing%20to%20its%20unique%20characteristics,gaming%2C%20automobile%2C%20retail)

[13] MarketWatch. (2022, January 7). *Contactless biometrics technology market scope and Overview, estimates & forecast, by application, segments* 2022?2030. MarketWatch. Retrieved January 11, 2022, from https://www.marketwatch.com/press-release/contactless-biometrics-technology-market-scope-and-overview-estimates-forecast-by-application-segments-20222030-2022-01-07?tesla=y

[14] Lee, J. (2016.). *Banks turn to biometrics to boost security*. NerdWallet. Retrieved January 11, 2022, from https://www.nerdwallet.com/article/banking/biometrics-when-your-bank-scans-your-voice-face-or-eyes

[15] Thernstrom, M. (2019, October 15). *What if the thief who steals your identity is your mom?* The New York Times. Retrieved January 11, 2022, from https://www.nytimes.com/2019/10/15/books/review/the-less-people-know-about-us-axton-betz-hamilton.html

[16] Cohen, S. (2019, October 12). *I lived with the identity thief who ruined my family - and didn't realize until it was too late.* New York Post. Retrieved January 15, 2022, from https://nypost.com/2019/10/12/i-lived-with-the-identity-thief-who-ruined-my-family-and-didnt-realize-until-it-was-too-late/

If this tragedy had occurred during modern times, when companies are relying on biometrics, it is possible the damage to Ms. Betz-Hamilton could have been much worse. In order to establish a false identity, a false doppelganger, Ms. Betz-Hamilton's mother would have had to use her own biometric information to establish an identity for the pseudo Ms. Betz-Hamilton. How would the real Betz-Hamilton ever be able to verify her true identity using her real biometric information when a false identity had already been established for her using her mother's biometric information? Use of biometrics technologies raises serious privacy concerns. Wherever an individual goes, they leave behind biometric information. Fingerprints can be left behind when a person touches an object. A voice can easily be recorded by home devices such as Google Home and Alexa even when not prompted. An individual's image can be taken at any time, even without their knowledge. Not only that, but highly skilled thieves can easily replicate biometrics information such as fingerprints. This becomes worrying especially now that biometric technologies, like facial recognition, are being used by agencies such as the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), U.S Customs and Border Protection (CPB), and police departments like the New York, Chicago, and Detroit Police Departments. These agencies utilize biometric technologies without the consent of individuals which may heighten privacy concerns. In the U.S, surveillance is concentrated among racial and ethnic minorities, particularly - Black and Latino men.[17]

Landlords could use biometric information to discriminate against protected classes. There are no regulations to stop a landlord from denying a prospective tenant just because they do not meet a certain biometric threshold. A landlord may rely on information from a tenant screening selection vendor that utilizes criminal records information to assess potential tenants.[18] This poses potential discrimination challenges since many law enforcement departments utilize facial recognition technology that is notoriously biased toward people of color resulting in higher instances of false identifications and wrongful arrests for this group.[19] The challenge is that tenant screening selection systems can ding a potential tenant just for being arrested – even if the arrest was unjustified.[20] In situations like this, biometrics can form the basis for discriminatory outcomes in a housing context and lead to the disenfranchisement of Black and Brown consumers and the restriction of their ability to fairly access critical housing opportunities.

The hyper-policing of communities of color, which is exacerbated by facial recognition and other biometrics technologies, results in Blacks and Latinos being disproportionately arrested. This biometrics-based data is then fed into systems used in the housing sector, like tenant screening selection technologies, that result in people of color being disproportionately excluded from housing opportunities. This process can reinforce and perpetuate segregation

[17] Remster, B., & Kramer, R. (2018). Race, space, and surveillance: Understanding the relationship between criminal justice contact and institutional involvement. *Socius, 4*, 2378023118761434.

[18] See Shannon Houston, *Center Files Federal Lawsuit Against National Tenant Screening Company*, Connecticut Fair Housing Center, (August 24, 2018). In this case, a mother was denied the right to have her disabled son live with her because the apartment complex where she lived used a tenant screening selection service that flagged the son because he had been arrested as a minor. He was never convicted of committing any crime.

[19] Alfred Ng, *Police are Using Facial Recognition for Minor Crimes Because They Can*, CNET, (October 24, 2020).

[20] Cyrus Farivar, *Tenant Screening Software Faces National Reckoning*, NBC News (March 14, 2021). https://www.nbcnews.com/tech/tech-news/tenant-screening-software-faces-national-reckoning-n1260975

and also lead to "biometric redlining" that prevents Black and Brown individuals from accessing housing opportunities in predominantly White, resource-rich neighborhoods.

When it comes to the gathering of biometric information such as facial images, eye scans, and vocal data , individuals often do not have meaningful ways to opt out of the collection of their personal information. In Knickerbocker Village, an affordable housing complex located in New York City, tenants were required to submit to facial scanning. Tenants' facial scans are assessed by a facial recognition system that tenants, who are predominantly Chinese, complain rarely works.[21] Children as young as 8 years old have had to submit to facial scans and must submit to several more scans as they grow older.

Regulation over the use of facial recognition systems is quite lax. For example, Knickerbocker Village did not submit the necessary application to gain approval from New York's Division of Housing and Community Renewal for use of the facial recognition system.[22] For years, the housing complex has allegedly been illegally using facial recognition technology. Weak regulation and oversight have prompted legislators to take note. Representatives Yvette Clarke, Ayanna Pressley, and Rashida Talib introduced the No Biometric Barriers Housing Act of 2019.[23] It is not clear how companies like Knickerbocker Village use the biometrics data collected in its facial recognition system. While the complex alleges it is only using the data and systems for safety purposes, they create clear barriers for the residents of the community and could be used for surveillance, rather than safety purposes.

Some entities are utilizing biometrics without the consent or knowledge of their target group.[24] Clearview AI created a facial recognition application that was built from more than 3 billion images scraped from websites such as Facebook, YouTube, Venmo, and millions of other websites. This application allows companies to take a picture of a person, upload the image into the application and get public photos of the target with links to the website where the photo was posted. This application infringes on the privacy rights of individuals. There are no regulations preventing a potential landlord from taking a photo of prospective tenants and selling that data to a company like Clearview. Nor are there regulations that would prevent landlords from sending images of tenants' driver's licenses or passports to a company like Clearview.

Systems like those created by Clearview could also be used by potential employers, car lenders, and other entities to discriminate based on biometric data. Given the lax regulatory oversight over these types of utilities, it is difficult to fully understand the full potential for discrimination they can manifest. In housing and lending, applications like Clearview can be used to monitor and cause biometric redlining by denying those deemed "high risk" from renting an apartment or receiving a credit card. Biometric redlining can also be exacerbated by a type of biometric technology that was suggested by PayPal's global head of developer evangelism, Jonathan LeBlanc. LeBlanc suggested replacing traditional biometrics like

[21] Kim, E. (2019, September 18). *'we're like guinea pigs': How an affordable Lower East Side Complex got facial recognition*. Gothamist. Retrieved January 11, 2022, from https://gothamist.com/news/were-guinea-pigs-how-affordable-lower-east-side-complex-got-facial-recognition

[22] Ibid.

[23] See Press Release *Reps. Clarke, Pressley & Tlaib Announce Bill to Ban Public Housing Usage of Facial Recognition & Biometric Identification Technology*

[24] Roussi, A. (2020, November 18). *Resisting the rise of facial recognition*. Nature News. Retrieved January 11, 2022, from https://www.nature.com/articles/d41586-020-03188-2

fingerprints and iris scans with invasive systems.[25] One suggestion included a password pill that could be ingested and powered by stomach acid. Other solutions included “tattoos” incorporating a computer chip, embedded wireless antennas, and sensors that measure temperature, ECG activity, etc. These technologies could be used to track and over police communities of color which infringes on individual rights and these communities‘ right to privacy.

Biometric applications, like the one developed by Clearview, bring up data ownership and personal privacy problems. These applications can also be weaponized against Black and Latino communities and those that oppose powerful organizations. In the future, applications like Clearview can be used by governments to stop civil protests, stalk political opponents for blackmailable information, monitor already disenfranchised communities and so much more.

IV. Security Considerations Associated With A Particular Biometric Technology:

The importance of right to Privacy cannot go unnoticed as technology increases its hold on every facet of the human experience. The misuse of or unauthorized access to biometric data can compromise privacy and could have serious long-lasting implications. While exposure to biometric technology increases and persists in shaping individuals' interactions online, it is important to address real issues of how biometric technologies can enable privacy and integrity attacks in a way never seen before.

Biometric authentication utilizes either human physical or behavioral characteristics to identify an individual and provide access to systems’ data or devices. Biometric characteristics serve as identifiers to authenticate or, in partnership with other means of information, to identify a user. Such private information is progressively collected, stored, and transmitted by IoT (Internet of Things) devices and services in the Cloud thus making individuals more vulnerable to cyberthefts.[26] Biometric data is easier to hack than other types of data and the implications of misusage may be incredibly dangerous.[27] Though there are safer ways to store biometric data such as through chips or end-user devices like smartphones, a biometric server is the most cost-efficient way to store such data.[28] However, data in a biometric server is more susceptible to access breach compared to other types of data, despite allowing for verification in multiple locations, due to how biometric technology— unlike encryption keys and codes— captures a single unique identity that is immutable.[29] The static state of biometric data makes it more prone to identity-based threats. Therefore, through access to biometric data either through data breach or misusage, hackers or other parties can easily steal identities or even tamper with and use such biometric information to the detriment of an individual.

[25] Collins, K. (2015, April 20). *PayPal wants you to swallow your password.* WIRED UK. Retrieved January 11, 2022, from https://www.wired.co.uk/article/paypal-biometric-security-edible-passwords-tattoos

[26] Haber, M. (2019, March 21). *Is Your Identity at Risk from Biometric Data Collection?.* Beyond Trust. Retrieved January 13, 2022, from https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection

[27] Porr, P. (2020, April 13). *The Fear of Biometric Technology in Today's Digital World. CPO Magazine.* Retrieved January 13, 2022, from https://www.cpomagazine.com/data-privacy/the-fear-of-biometric-technology-in-todays-digital-world/

[28] Ibid.

[29] Johansen, A. G. (2019, February 8). *Biometrics and Biometric Data: What is it and is it Secure?* Norton. Retrieved January 13, 2022, from https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Spoofed sensors[30], sensor inaccuracy, host system misconfigurations, and additional fraud capabilities can imperil biometric indicators. Such happened when the U.S. Office of Personnel Management was hacked in 2015 and cybercriminals got access to 5.6 million government employees' fingerprints leaving them vulnerable to identity theft.[31] Then in 2019 a major breach was found in the biometric system utilized by UK Police, defense contractors, and banks.[32] A million people's fingerprints, log data, facial recognition, and additional personal information were compromised and found on a publicly accessible database. Biometric characteristics are immutable and, once stolen, resulting negative consequences may be irreversible. This puts individuals at risk of being affected for the rest of their lives.

The potential for criminal activity and fraud, specifically identify theft, is massive. Leakage of personal data connected to an individual's biometric information can cause irreversible damage such as compromising a credit score to the extent that it makes it difficult for individuals to secure housing, mortgage loans, and other financial services. The types of identity theft that directly impact the purchase of a home include tax identity theft, Social Security identity theft, financial identity theft, and medical identity theft.[33] These types of identity theft will affect an individual's credit score due to how such cybercrime results in unpaid bills, debt from loans, and balances due on credit lines despite being impersonated. Examples of compromised biometric indicators' consequences are endless; thus, it is necessary to address the lack of needed oversight and security to keep biometric data from advanced authentication technology safe.

These complex technical, process, and policy challenges must be addressed to ensure digital data is secured and biometric technology effectively shapes human identity authentication applications for the better.

V. Potential Harms of A Potential Biometric Technology:

Today, an estimated one hundred and thirty countries around the world have data protection laws and almost all these laws cover biometric data protection guidelines.[34] In theory, these laws make sure biometric data is not utilized for instances where customers do not give consent. However, these laws lack attention to racial bias, discrimination, or accuracy, and they are often too complex to faithfully implement in an algorithmic system. Of all dominant biometrics-based technology applications, facial recognition is one of the least accurate and it has a legitimate basis for privacy concerns.[35]

[30] A spoof sensor is used in spoofing attack, a situation in which a person or program successfully impersonates another by falsifying data, to gain an illegitimate advantage. See Jindal, K., Dalal, S., Sharma, K. K. (February 2014), Analyzing Spoofing Attacks in Wireless Networks, 2014 Fourth International Conference on Advanced Computing Communication Technologies: 398–402. doi:10.1109/ACCT.2014.46.

[31] Sanger, D. E. (2015, September 23). *Hackers Took Fingerprints of 5.6 million U.S. workers, Government Says.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html

[32] Doffman, Z. (2019, August 14). *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records*. Forbes. Retrieved January 13, 2022, from https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=4523dc1a46c6

[33] National Consumer Law Center. (2021, December). No Silver Bullet: Using Alternative Data for Financial Inclusion and Racial Justice.

[34] Vioreanu, D. (2021, November 15). B*iometric Tech is Here to Stay – Unveiling the Privacy and Security Risks.* Privacy Hub. Retrieved January 13, 2022, from https://privacyhub.cyberghostvpn.com/privacyhub/privacy-concerns-biometrics/

[35] Najibi, A. (2020, October 26). *Racial Discrimination in Face Recognition Technology. Science in the News.* Retrieved January 13, 2022, from https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Facial recognition's widespread implementation ranges from the ability to unlock a smart phone to law enforcement surveillance to employment and housing decisions. Around half of all adults in America, meaning over 117 million people, have their photos in a facial recognition network used by law enforcement agencies.[36] Law enforcement utilizes the facial recognition network to compare photos of suspects to images of drivers' licenses and mugshots. Such application of facial recognition is taking place largely without awareness, much less individual consent. The widespread implementation of these technologies in a law enforcement context is disturbing, particularly when one considers the pronounced racial bias, especially towards Black people, these systems manifest.[37]

New and growing research reveals puzzling disparities in error rates across different demographic groups with the least consistent accuracy found for 18 to 30-year-old Black females.[38] Additionally, the landmark "Gender Shades" project from 2018 applied an intersectional approach to appraise three different gender classification algorithms including those of Microsoft and IBM.[39] Subjects for the project were put into four categories of darker-skinned females, darker-skinned males, lighter-skinned females, and lighter-skinned males. All three gender classification algorithms performed with the least accuracy on darker-skinned females with error rates that were 34% higher than those for lighter-skinned males.[40] The National Institute of Standards and Technology validated these studies and found facial recognition for 189 algorithms to perform with the least accuracy on women of color.[41]

The research is undeniable, and such harrowing results have led to prompt responses around the conversation of equity in facial recognition. The implications of high error rates in facial recognition systems utilized by law enforcement is troubling due to historical and existing racist patterns of law enforcement which disproportionately hurt the Black community and other marginalized populations. Surveillance through facial recognition technologies by law enforcement threatens important rights such as "privacy, freedom of expression, freedom of association, and due process" as vocalized by the Algorithmic Justice League.[42] Surveillance is could lead to behavioral changes such as self-censorship due to fear of retribution.[43] Fear of retribution due to activism is not unfounded, as facial recognition was utilized to monitor and identify peaceful Black Lives Matter protestors in 2020.[44] Some of the greatest harmful implications of facial recognition technology lies in the criminal justice context where inherently biased facial recognition technologies can misidentify suspects due to the low level of accuracy. This can and has resulted in higher levels of arrest and incarceration of innocent Black

[36] Ibid.
[37] Bedoya, A. M. (2020). Privacy as Civil Right. *NML Rev., 50,* 301.
[38] Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face recognition performance: Role of demographic information. *IEEE Transactions on Information Forensics and Security*, 7(6), 1789-1801.
[39] Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. *In Conference on fairness, accountability and transparency* (pp. 77-91). PMLR.
[40] Ibid.
[41] Grother, P. J., Ngan, M. L., & Hanaoka, K. K. (2019). Face recognition vendor test part 3: demographic effects.
[42] *What is Facial Recognition Technology?* Algorithmic Justice League. (n.d.). Retrieved January 13, 2022, from https://www.ajl.org/facial-recognition-technology
[43] Munn, N. (2016, November 8). *How Mass Surveillance Harms Societies And Individuals - And What You Can Do About It.* CJFE. Retrieved January 13, 2022, from https://www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it
[44] Choudhury, N., & Cyril, M. (2021, November 19). *The FBI won't hand over its surveillance records on 'black identity extremists,' so we're suing.* American Civil Liberties Union. Retrieved January 13, 2022, from https://www.aclu.org/blog/racial-justice/race-and-criminal-justice/fbi-wont-hand-over-its-surveillance-records-black

Americans thereby worsening America's already damaged, biased and discriminatory criminal justice system..

Facial recognition for surveillance gone wrong was most notably seen in Project Green Light, a 2016 model surveillance program.[45] High-definition cameras were installed in the city of Detroit and the cameras' data directly went to the Detroit PD to test for facial recognition against criminal databases, driver's licenses, and state ID photos to include almost every resident of Michigan in this system without any individual consent.[46] The Project Green Light Cameras were not distributed evenly across the city and instead were concentrated in majority-Black areas whilst excluding majority White and Asian areas.[47] Direct consequences of concentrated Project Green Light Cameras in majority Black areas were revealed through a critical analysis of Project Green Light in 2019. The critical analysis reported such surveillance and data collection had a high correlation to insecure housing, loss of employment opportunities, and the increased criminalization and policing of community members who encountered this model surveillance program.[48]

The criminalization and policing of community members due to the concentration of Project Green Light Cameras in majority-Black areas can have dire impacts including lowered credit ratings, denial of housing and lending opportunities, eviction, and the presence of debilitating information on a person's credit report. This can, of course, reduce a person's ability to rent or buy a home or obtain employment.

If any incarcerated individual has outstanding debt, they are not always able to pay such debt from jail, thus negatively impacting their credit score. Moreover, people who are arrested will undoubtedly have to tap into financial resources to cover legal fees or bonds. This can mean piling up credit card debt or even obtaining PayDay loans and both will have a harmful affect on a person's credit score. First, higher debt utilization lowers a person's credit score. Secondly, accessing PayDay loans, which can often have abusive and predatory terms, can more likely result in outcomes, like increased collections activity, that will harm a consumer's financial profile. Additionally, closing credit cards and extreme periods of inactivity on a card can also hurt credit scores and serve as a barrier for buying or renting houses, obtaining homeowners insurance, and more.

Project Green Light is a striking example of the way surveillance through facial recognition can perpetuate racial inequality when there is no regulation. Tawana Petty, director for the data justice program for the Detroit Community Technology Project and lifelong Detroit resident explained "It feels like digital redlining; that people are being regulated to particular neighborhoods and identified in particular ways because those cameras exist."[49]

Though more lawmakers are beginning to push for regulation, it is hard to do so when there is no documentation for or tracking of surveillance applications especially in the location

[45] Harmon, A. (2019, July 8). *As cameras track Detroit's residents, a debate ensues over racial bias.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

[46] Urban, N., Yesh-Brochstein, J., Raleigh, E., & Petty, T. (2019, June 9). A Critical Summary of Detroit's Project Green Light and its Greater Context.

[47] Harmon, A. (2019, July 8). *As cameras track Detroit's residents, a debate ensues over racial bias.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

[48] Urban, N., Yesh-Brochstein, J., Raleigh, E., & Petty, T. (2019, June 9). A Critical Summary of Detroit's Project Green Light and its Greater Context.

[49] Fadulu, L. (2019, September 24). *Facial recognition technology in public housing prompts backlash.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html

Americans spend most of their time, their homes.[50] The Department of Housing and Urban Development (HUD) does not keep track of the way surveillance technology may be used on its 1.2 million households.[51] A letter from HUD to Senator Wyden(OR) stated the agency does not know how many of their public housing programs utilize facial recognition or the way it is allowed to be used.[52] Though these are federally assisted properties under HUD's jurisdiction, rather than monitoring the usage of facial recognition technologies, they leave such responsibilities to individual Housing Authorities that implement housing programs. HUD also never carried out research or implemented policies or guidance for how facial recognition can be used in public housing.[53]

While many multi-family housing corporations assert, they are utilizing systems fueled by biometric data to address safety concerns, there is ample evidence that these systems are being used to conduct surveillance on inhabitants. In the Fall of 2018, tenants at the Atlantic Plaza Towers received a concerning letter in the mail stating their landlord was going to install facial recognition technology to access their building and replace the key-fob system they previously.[54] Not every tenant knew of these changes and five tenants convened in the lobby to spread the word. A couple of days later, those five tenants, who were Black women, received a note from the property management company stating that the lobby was not "a place to solicit, electioneer, hang out, or loiter," along with pictures of them convening.[55] New York State law gives tenants the right to meet peacefully in any location of the building as long as they are not obstructing passageways which the women are not shown to be doing as evidenced by the pictures. [56] It is clear that the property management firm was utilizing the facial recognition system to police tenants and that the company's interpretation of what the tenants were doing was inaccurate.

The ramifications of false or trivial criminal allegation through surveillance by facial recognition carry heavy consequences. Individuals in public housing or the rental market may face civil asset forfeiture, eviction, or loss of access to government benefits and relief programs in the future. Such consequences are already dominant for people of color and women, thus unregulated facial recognition could exacerbate existing structural inequalities in the U.S. impeding access to fair housing, lending, and other opportunities and presenting privacy and due process, consumer consent concerns.[57]

[50] Ng, A. (2020, June 22). *US government doesn't know how it uses facial recognition in public housing.* CNET. Retrieved January 13, 2022, from https://www.cnet.com/news/us-government-doesnt-know-how-it-uses-facial-recognition-in-public-housing/
[51] Ibid.
[52] Ibid.
[53] Fadulu, L. (2019, September 24). *Facial recognition technology in public housing prompts backlash.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html
[54] Bellafante, G. (2019, March 28). T*he landlord wants facial recognition in its rent-stabilized buildings. why?* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html
[55] Ibid.
[56] Ibid.
[57] Ng, A. (2019, July 22). *Lawmakers to introduce Bill to ban facial recognition from public housing.* CNET. Retrieved January 13, 2022, from https://www.cnet.com/home/smart-home/facial-recognition-may-be-banned-from-public-housing-thanks-to-proposed-law/

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

National Immigration Law Center

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

COMMENTS ON:

Executive Office of the President, Office of Science and Technology Policy, Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

To: BiometricRFI@ostp.eop.gov
Re: *<RFI Response: Biometric Technologies>*

SUBMITTED BY THE NATIONAL IMMIGRATION LAW CENTER

The National Immigration Law Center (NILC) submits the following comments on the Executive Office of the President, Office of Science and Technology Policy (OSTP), Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.[1] Established in 1979, the National Immigration Law Center (NILC) is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights and opportunities of low-income immigrants and their families. In response to Topic Nos. 1, 4, and 6, NILC's comments focus on the development and future implementation of the Department of Homeland Security's (DHS) enormous database of personal information, including biometrics, called Homeland Advanced Recognition Technology (HART).[2]

As a threshold matter, NILC notes that OSTP is just now seeking public input about biometric technologies, though DHS's development of HART is well underway. DHS has been constructing HART surreptitiously, without transparency or accountability. HART's eventual scope is known only to DHS. The components that DHS has included to date lay the groundwork for a pervasive and invasive system of immigration enforcement, surveillance of immigrants and citizens alike, and use of tools, such as facial recognition technology or behavioral predictions, that are already known to discriminate against immigrants and people of color, or that are untested.

DHS has described HART as a database containing biometrics and associated biographic information,[3] but even its current components depict inclusion of massive amounts of information far beyond that. Data collected when individuals are encountered by immigration

[1] *See* Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Executive Office of the President, Office of Science and Technology Policy, 86 Fed. Reg. 56300 (Oct. 8, 2021), https://www.govinfo.gov/content/pkg/FR-2021-10-08/pdf/2021-21975.pdf.
[2] For more detailed information regarding HART, see generally National Immigration Law Center (NILC), Homeland Advanced Recognition Technology (HART): DHS is Building a Massive Database of Personal Information (Dec. 2021), https://www.nilc.org/wp-content/uploads/2021/12/HART-factsheet-2021-11-10.pdf.
[3] *See* Department of Homeland Security, Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA 1-2 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf [hereinafter HART PIA].

officers or agents, officer comments, derogatory information, relationship patterns and more yet-to-be-disclosed data will also be included.[4] DHS will use the information for purposes so sweeping as to be limitless, and it intends to share the information in HART about non-citizens and citizens widely, both domestically and internationally.

HART's Full Scope is Clouded in Secrecy, and DHS Has Not Divulged the Full Range of Biometrics that Will Be Included in HART

DHS's ultimate vision for HART is steeped in vagueness. As the agency outlined in 2015, HART will centralize access to federal and international databases, provide real-time access in the field, and involve the use of "multi-modal biometrics."[5]

DHS is developing HART in four increments, only the first of which is in progress.[6] Its amorphous descriptions of the increments offer few clues to HART's ultimate content and use, but clearly indicate that its reach will expand, and that personal information will be consolidated and shared widely. And while DHS issued a Privacy Impact Assessment (PIA) in 2020 about Increment 1 of HART,[7] the agency has not issued a System of Records Notice (SORN) that describes HART's full operation.

Even though many of the key pieces of HART remain unclear, HART is set to replace DHS's current biometrics database IDENT (Automated Biometric Identification System),[8] which, at present, stores fingerprints, photographs, and signatures.[9] Both IDENT and HART are meant to serve wide-ranging and undefined law enforcement, national security, immigration, and administrative purposes.

[4] *Id.* at 28, 49-50.
[5] Zack Martin, *Homeland Security Releases Biometric Framework*, SecureIDNews (Aug. 31, 2015), https://www.secureidnews.com/news-item/homeland-security-releases-biometric-framework/. For an overview, see Joint Requirements Council, *Biometrics Webinar*, Department of Homeland Security (Oct. 20, 2015), https://www.dhs.gov/sites/default/files/publications/DHS%20Biometrics%20%20Strategic%20Framework%20Webinar%20Slidedeck%20-%20October%2020%202015_2.pdf. The Strategic Framework referenced in the Biometrics Webinar no longer appears to be publicly available.
[6] *See* HART PIA, *supra* note 3, at 3.
[7] HART PIA, *supra* note 3.
[8] *See* Supplemental Programmatic Environmental Assessment (SPEA) for the Proposed Establishment and Operations of the Office of Biometric Identity Management and the Homeland Advanced Biometric Technology (HART), Department of Homeland Security, National Protection and Programs Directorate, 81 Fed. Reg. 90862, 90862 (Dec. 15, 2016), https://www.govinfo.gov/content/pkg/FR-2016-12-15/pdf/2016-30187.pdf.
[9] *See generally* Department of Homeland Security, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) (December 7, 2012), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf. DHS describes IDENT as "a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context." Privacy Act; IDENT System of Records, Department of Homeland Security, 72 Fed. Reg. 31080–82 (June 5, 2007), https://www.govinfo.gov/content/pkg/FR-2007-06-05/html/07-2781.htm. Currently, IDENT "holds more than 260 million unique identities and processes more than 350,000 biometric transactions per day." *Biometrics*, Department of Homeland Security (last updated June 9, 2021), https://www.dhs.gov/biometrics.

DHS currently describes the term biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition" and are "used to detect and prevent illegal entry into the U.S., grant and administer proper immigration benefits, [for] vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification for visa applications to the U.S."[10]

DHS's fuzzy description of biometrics does not begin to make clear the full gamut of physical and behavioral characteristics that "biometrics" may encompass. In September 2020, during the Trump administration, DHS issued a Notice of Proposed Rulemaking (NPRM) that offered a sweeping definition of biometrics to include a wide range of intimate physical and behavioral characteristics, such as fingerprints, palm prints, photographs (including "facial images specifically for facial recognition, as well as photographs of physical or anatomical features such as scars, skin marks, and tattoos"), signatures, voice prints, iris images, and DNA test results.[11] DHS, under the Biden administration, withdrew the NPRM.[12]

But there is no indication that the current administration has rejected the NPRM's definition of biometrics or that it will take a narrower approach to expanded biometrics inclusion in HART. In fact, the notice of withdrawal explicitly approved the proposed rule's goal of flexibility in biometrics collection practices and policies and in biometrics use.[13] And, as described below, one of the components of HART – the External Biometric Records (EBR) System of Records – already put in place in 2018 an expanded biometrics definition, namely: facial images, fingerprints, latent fingerprints, iris images, palm prints, voice prints, scars, marks, and tattoos, DNA or DNA profiles, and other modalities.[14]

DHS is offering some clues about how the definition of biometrics could expand even further. The agency recently issued a system of records notice which defined biometric data to include

[10] *Biometrics*, Department of Homeland Security (last updated June 9, 2021), https://www.dhs.gov/biometrics.
[11] Notice of Proposed Rulemaking, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, Department of Homeland Security, 85 Fed. Reg. 56338, 56341 (Sept. 11, 2020). https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf [hereinafter Biometrics NPRM].
[12] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services; Withdrawal, Department of Homeland Security, 86 Fed. Reg. 24750 (May 10, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-10/pdf/2021-09671.pdf.
[13] *See id.* at 24750.
[14] Privacy Act of 1974; System of Records titled "Department of Homeland Security/ALL–041 External Biometric Records (EBR) System of Records," Department of Homeland Security, 83 Fed. Reg. 17829, 17831 (Apr. 24, 2018), https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08453.pdf [hereinafter EBR SORN].

"typing cadence, cardiac signature, [and] vascular patterns."[15] Data about an individual's gait, heart rate, or breathing pattern, and electrodermal activity[16] potentially could be included in a biometrics database.

HART Will Include Personal Information Beyond Biometrics

DHS has used piecemeal "system of records" notices (SORNs) to stealthily build HART's enormous capabilities well beyond the problematic biometrics context. The two components that DHS has identified to date are External Biometrics Records (EBR)[17] and Enterprise Biometric Administrative Records (EBAR).[18]

But these records systems will include far more than biometrics and will provide a means for DHS to centralize a wide range of unverified information about noncitizens and citizens that can be shared broadly. EBR and EBAR will include:

HART COMPONENT	WHAT'S INCLUDED AND FOR WHAT PURPOSES	SOURCES AND SHARING
DHS/ALL–041 External Biometric Records (EBR)	EBR will include biometrics, associated biographic information identifiers for derogatory information, miscellaneous officer comment information, encounter data, and records related to the analysis of relationship patterns among individuals and organizations. The data may be used for law enforcement; national security, immigration screening; border enforcement; intelligence, national defense, and background investigations relating to national security positions,	Allows DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS foreign and domestic entities. Either formal or informal information sharing agreements or arrangements or simply the approval of the entity from which information is obtained may be used to obtain "external information."

[15] Privacy Act of 1974; System of Records titled "DHS/Science & Technology Directorate (S&T)-001 Research, Development, Test, and Evaluation System of Records," Department of Homeland Security, 86 Fed. Reg. 58084, 58086 (Oct. 20, 2021), https://www.govinfo.gov/content/pkg/FR-2021-10-20/pdf/2021-22849.pdf.
[16] *See id. See generally* Bryn Farnsworth, *What is EDA? And How Does It Work?*, iMotions (June 4, 2019), https://imotions.com/blog/eda/ ("Electrodermal activity (EDA; sometimes known as galvanic skin response, or GSR) refers to the variation of the electrical conductance of the skin in response to sweat secretion (often in minute amounts).").
[17] EBR SORN, *supra* note 14.
[18] Privacy Act of 1974; System of Records titled "Department of Homeland Security/ALL–043 Enterprise Biometric Administrative Records (EBAR), Department of Homeland Security, 85 Fed. Reg. 14955 (Mar. 16, 2020), https://www.govinfo.gov/content/pkg/FR-2020-03-16/pdf/2020-04979.pdf.

	credentialing, and certain positions of public trust.	
DHS/ALL–043 Enterprise Biometric Administrative Records (EBAR)	EBAR will cover the administrative and technical records associated with IDENT and HART. DHS's only listed example of EBAR's function is that it will "link individuals with their encounters, biometrics, records, and other data elements."	Sharing of EBAR data within DHS agencies will be based on their "need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions." DHS may also share information with "appropriate" federal, state, local, tribal, territorial, foreign, or international government agencies.

As described below, HART will also include data from other records systems not mentioned in the notices. And DHS component U.S. Customs and Border Protection has even extended biometrics collection, including photographs, as well as collection of personal and family information to undocumented noncitizens before they even reach a port of entry.[19] That data will no doubt be included in HART and available for facial recognition purposes or sharing with foreign governments, whether or not the individual ever reaches the border or is allowed to enter the U.S. to apply for asylum.

DHS Is Outsourcing Data Collection to Unregulated Commercial Enterprises and Public Sources

HART will collect data not only from government entities, but according to the 2020 PIA, "HART may use information from publicly available sources, collected according to the data provider's authority. Specific publicly available sources are discussed in more detail in the appropriate data provider's privacy compliance documentation."[20] This outsourced and unrestricted data collection would prevent oversight, accountability, and transparency of commercial data that finds its way into HART.

[19] *See* Notice, Collection of Advance Information from Certain Undocumented Individuals on the Land Border, Department of Homeland Security, U.S. Customs and Border Protection, 86 Fed. Reg. 53667 (Sept. 28, 2021), https://www.govinfo.gov/content/pkg/FR-2021-09-28/pdf/2021-20988.pdf.
[20] *See* HART PIA, *supra* note 3, at 18.

Commercial entities have become a major source of data for immigration enforcement.[21] Companies with a record of unfettered biometrics collection, data sharing, and analytics continue to build and host systems for U.S. Immigration and Customs Enforcement (ICE); yet little is known about their contracts or their use, collection, and third-party sharing of data with other federal, local, and state agencies or other companies.[22] And on the infrequent occasions when reviews are performed (for example, the Government Accountability Office's review of U.S. Customs and Border Protection's supervision of companies' compliance with privacy standards for facial recognition programs), DHS's failure to conduct audits was soundly criticized.[23]

Reliance on private companies that sweep up personal information, including biometrics, and sell it to the federal government is an end run around state and local sanctuary policies that impose legal requirements on sharing personal information for use in immigration enforcement.

HART Will Enable Government Surveillance and Will Rely on Techniques that Discriminate Against Immigrants and People of Color

The Biden administration has not rejected the Trump administration's explicit policy of extreme and continuous vetting of noncitizens, based on a "person-centric" model that aggregates data on individuals with biometrics as a key element.[24] Once collected, biometrics and other information are available for all surveillance purposes.

And, as the EBR and EBAR table above shows, HART will facilitate DHS's ability to share biometrics and sweeping categories of unverified information, such as derogatory information and relationship patterns, with federal, state, and local law enforcement, intelligence community entities, and foreign governments.

DHS will be able to collect and use individuals' physical and behavioral characteristics, often without their consent or knowledge. Use of unreliable technology, such as facial recognition, is

[21] *Who's Behind ICE: The Tech and Data Companies Fueling Deportations*, Mijente, National Immigration Project of the National Lawyers Guild, and Immigrant Defense Project, (Aug. 2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf; *The War on Immigrants: Trump's Tech Tools Powered by Palantir*, Mijente (Aug. 2019), https://mijente.net/wp-content/uploads/2019/08/Mijente-The-War-Against-Immigrants_-Trumps-Tech-Tools-Powered-by-Palantir_.pdf.

[22] *See, e.g.,* Felipe De La Hoz, *DHS Plans to Start Collecting Eye Scans and DNA – With the Help of Defense Contractors*, The Intercept (Nov. 17, 2020), https://theintercept.com/2020/11/17/dhs-biometrics-dna/; Press Release, Center for Constitutional Rights, "Immigrant Rights Groups, Law School and Legal Organization FOIA for Info on Thomson Reuters, RELX Group Contracts with ICE" (Sept. 14, 2020), https://ccrjustice.org/home/press-center/press-releases/immigrant-rights-groups-law-school-and-legal-organization-foia-info.

[23] *See* De La Hoz, *supra* note 22.

[24] *See* Biometrics NPRM, *supra* note 11, at 56340.

already built into DHS's biometrics plans, as is the use of mobile devices in the field to collect biometrics.

In 2020, DHS contracted for biometrics analytics and services with the company Clearview AI.[25] At the time the contract was signed, ICE refused to say whether its facial recognition technology would be used in its enforcement and removal (ERO) operations.[26] Clearview AI is now poised to obtain a patent[27] on its facial recognition technology that will cover "Clearview's 'methods of providing information about a person based on facial recognition,' including its 'automated web crawler' that scans social networking sites and the internet and its algorithms that analyze and match facial images obtained online."[28]

Increased collection and storage of biometrics information in HART, will undoubtedly exacerbate racial disparities that are already present in law enforcement databases, systems, and tools. Facial recognition has a discriminatory impact and significant error rates across gender and skin color. [29] In particular, it is "notoriously unreliable for identifying Black people, women, and young people" and relies on photographs collected in a discriminatory criminal justice and immigration databases.[30] The unrestricted collection, storage, and sharing of biometrics and other personal information that HART enables have additional harmful and wide-ranging effects:

> This massive expansion of biometrics collection also threatens First Amendment protected activity. By collecting and retaining biometric data like face recognition and sharing it broadly with federal, state, and local agencies, as well as with contractors and foreign governments, DHS lays the groundwork for a vast surveillance and tracking network that could impact individuals and communities for years to come. DHS could soon build a database large enough to identify and track all people in public places, without their knowledge—not just in places the agency oversees, like at the border, but

[25] Kim Lyons, *ICE Just Signed a Contract with Facial Recognition Company Clearview AI*, The Verge (last updated Aug. 14, 2020), https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration.
[26] *See* Ryan Mac & Brianna Sacks, *Controversial Facial Recognition Firm Clearview AI Raised $8.6 Million*, Buzzfeed News (last updated Sept. 24, 2020), https://www.buzzfeednews.com/article/ryanmac/controversial-clearview-ai-raises-8-million.
[27] *See* Patent Application of Clearview AI, Inc., U.S. Patent and Trademark Office (filed Aug. 7, 2020), https://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&f=G&l=50&p=1&r=1&s1=20210042527.PGNR.&u=%2Fnetahtml%2FPTO%2Fsrchnum.html.
[28] Alexandra S. Levine, *Clearview AI on Track to Win U.S. Patent for Facial Recognition Technology*, Politico (Dec. 4, 2021), https://www.politico.com/news/2021/12/04/clearview-ai-facial-recognition-523735.
[29] *See generally* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research* (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[30] Comments Regarding Notice of Proposed Rulemaking on the Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (USCIS Docket No. USCIS–2019–0007, 85 Fed. Reg. 56338), Electronic Frontier Foundation (Oct. 13, 2020), https://www.regulations.gov/comment/USCIS-2019-0007-5370, at 26.

> anywhere there are cameras. This burden falls disproportionately on communities of color, immigrants, religious minorities, and other marginalized groups.[31]

HART's capability to share information with law enforcement, intelligence communities, and foreign governments would implement a system of persistent and biased surveillance. This would put people of color at greater risk for being "identified" for crimes they did not commit and for immigrants of color, funnel them into deportation pipeline.

And use of mobile devices by individual agents in the field means that DHS agencies are able to collect fingerprints, photographs and perhaps more in unregulated "encounters" where abuse is harder to monitor.

The Data Collection and Sharing that HART Enables Will Facilitate the Unlawful Entanglement Between Local Police and Federal Immigration Authorities

Every year, local police send thousands of individuals into the immigration enforcement system through a web of resource- and information-sharing processes.[32] Local police work with ICE to support immigration enforcement directly and indirectly through mechanisms such as providing physical access to jails and detained individuals; facilitating technological access to law enforcement databases, information systems, and records; participating in joint operations; as well as communicating informally with ICE agents to share resources and information.

The availability of programs and practices that entangle local policing efforts with federal immigration operations and tools incentivizes unconstitutional behavior, including racial and ethnic profiling and selective enforcement. In anticipation of a transfer to immigration authorities, local authorities have frequently arrested and detained individuals who normally would not have been detained, such as for minor infractions or traffic violations.[33] These harms

[31] *Id.* at 23-24.
[32] *See generally Untangling the Immigration Enforcement Web,* National Immigration Law Center (Sept. 2017), https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.
[33] *See, e.g.*, *Unalienable: Data Sharing Between Agencies,* ACLU Mississippi (Mar. 2021), https://www.aclu-ms.org/sites/default/files/final_data_sharing_brief.pdf (describing the racially discriminatory effects of Secure Communities, a program that allows local officers to check fingerprint data against the FBI's biometric data); Rachel Harmon, *Federal Programs and the Real Costs of Policing*, 90 N.Y.U. L. Rev. 870, 916 (2015) ("[I]n order to gain the benefits of increased immigration enforcement pursuant to a 287(g) agreement[—a local-federal collaboration program—], jurisdictions must arrest suspects who—absent the 287(g) program—would likely have been released."); Randy Capps et al., *Delegation and Divergence: A Study of 287(g) State and Local Immigration Enforcement* 37 (2011), https://www.migrationpolicy.org/sites/default/files/publications/287gdivergence.pdf, ("[I]mmigrant-and civil-rights groups, service providers, elected officials, and other community respondents . . . expressed concerns that enforcement efforts lead to racial profiling by police . . ."); Trevor Gardner II & Aarti Kohli, *The C.A.P. Effect: Racial Profiling in the ICE Criminal Alien Program* 5-7 (2009), https://www.law.berkeley.edu/files/policybrief_irving_0909_v9.pdf (describing the effect of a program called Criminal Alien Program in "creat[ing] incentives for local police to target Hispanics for discretionary arrests for minor offenses").

are disproportionately felt by Latino and Black communities.[34] HART's enormous capacity to collect, store and share biometric and other data will therefore encourage local authorities to target, stop, and arrest individuals, often on pretextual bases, in order to check their information within HART and facilitate immigration enforcement. As a result, the deployment and use of HART by enforcement agencies thus expose immigrants—particularly immigrants of color—to more risk and vulnerability when they are stopped by or encounter the police.

DHS Is Evading Transparency, Relevancy, Accountability, and Other Privacy Protections

DHS is building HART on a foundation of opacity and unaccountability by exempting each component from multiple provisions of the Privacy Act. DHS recognizes that "[t]he Privacy Act of 1974, 5 U.S.C. 552a, provides protection to individuals by ensuring that personal information collected by federal agencies is limited to that which is legally authorized and necessary, and is maintained in a manner which precludes unwarranted intrusions upon individual privacy."[35] Nonetheless, DHS consistently exempts HART components from the full range of the Privacy Act's accuracy, notice, and redress requirements. For example, DHS exempted EBR from various Privacy Act requirements, as listed in 5 U.S.C. 552a, including the requirements to provide an accounting to individuals of disclosures; permit individuals to have access to and request amendment of records that are not accurate, relevant, timely, or complete; only maintain records that are relevant and necessary; collect records directly from the individual to the greatest extent possible; inform the individual of the information's collection and use; notify individuals of procedures to find out if information is about them; notify individuals of the content of records and how to contest their content; maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; notify individuals when records are made available under compulsory legal process; establish procedures for notice to individuals and review of records; and provide a civil remedy when Privacy Act provisions are violated. [36]

Notwithstanding DHS's sweeping Privacy Act exemptions, even where the Privacy Act still manages to apply to HART's current and/or future components, immigrants other than lawful permanent residents are not covered by the Privacy Act. Therefore, the population most at risk and affected by the development, implementation, and use of HART is left without any meaningful protection over individual privacy rights or recourse for violations.

[34] *See* Shamira Ibrahim, *Ousman Darboe Could be Deported Any Day. His Story is a Common One for Black Immigrants*, Vox (last updated Feb. 5, 2020), https://www.vox.com/identities/2019/9/30/20875821/black-immigrants-school-prison-deportation-pipeline; *The State of Black Immigrants, Part II: Black Immigrants in the Mass Criminalization System* 20, NYU Immigrant Rts. Clinic & Black Alliance for Just Immigration http://stateofblackimmigrants.com/wp-content/uploads/2018/09/sobi-fullreportjan22.pdf.
[35] DHS Privacy Act Statement (Oct. 2020), https://www.dhs.gov/publication/privacy-act-statement.
[36] *See* EBR SORN, *supra* note 14, at 17833; see also 5 U.S.C. § 552a.

The HART Increment 1 PIA recognizes that HART presents serious privacy risks.[37] According to the PIA, some risks can't be mitigated at all, such as risks related to the inclusion of derogatory information, information sharing with foreign partners, or inaccurate database "hits" or results for juveniles whose physical characteristics change as they age.[38] And some risks can only be partially mitigated such as data sharing with unauthorized groups, sharing too much data, and the inability of non-U.S. persons to correct inaccurate information.[39] These privacy risks put immigrants in particular peril, especially if they are refugees or asylum seekers whose information is shared with other countries or if incorrect information interferes with obtaining legal status.

And as mentioned above, DHS's acquisition of commercial data prevents accountability and oversight over that data.

Conclusion

DHS's surreptitious construction of HART, the components of which lay the groundwork for pervasive surveillance and immigration enforcement, is of serious concern. DHS's plans to amass and share out a vast swath of personal information including biometric information through HART, with little regard for the civil and privacy rights of immigrants and people of color, is completely unacceptable. We therefore ask the OSTP to:

- Oppose and recommend freezing any expansion of HART, and support an immediate moratorium on additional appropriations for HART;
- Investigate DHS's proposed vision for HART and advocate for greater accountability and transparency measures over its current and/or future development; and
- Meet with immigrants' rights advocates, community groups, and affected stakeholders to discuss the above concerns.

Thank you for the opportunity to provide these comments. If you have any questions regarding these comments, please contact Sarah Kim Pak at [redacted] or [redacted].

Sincerely,

Sarah Kim Pak
Staff Attorney
National Immigration Law Center

[37] *See* Dave Nyczepir, *DHS's Forthcoming Biometrics System Presents Unmitigated Privacy Risks*, FedScoop (May 6, 2020), https://www.fedscoop.com/dhs-biometrics-system-privacy-risks/.
[38] HART PIA, *supra* note 3, at 24, 29, 32.
[39] HART PIA, *supra* note 3, at 22, 27, 28-29, 31, 33, 36.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

NEC Corporation of America

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

NEC Corporation of America
4201 Wilson Blvd, Suite 505
Arlington, VA 22203

January 15, 2022

BY ELECTRONIC MAIL
Mr. Suresh Venkatasubramanian
Assistant Director, Science and Justice
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Document No. 2021-21975: NEC Corporation of America Comments in Response to the Office of Science and Technology Policy's Request for Information on Public-Sector and Private-Sector Uses of Biometric Technologies

Mr. Venkatasubramanian:

NEC Corporation of America (NEC) is pleased to submit comments in response to the Office of Science and Technology Policy (OSTP) Request for Information (RFI) regarding public and private sector uses of biometric technologies.[1] As a key member of the information and communications technology (ICT) industry and a major global supplier of biometric technologies, NEC appreciates OSTP's effort to learn about biometric technologies from a variety of stakeholders while working to develop an AI Bill of Rights. We are committed to building digital trust by producing biometric technologies that are reliable, secure, and supportive of human rights and social justice, and we support OSTP's efforts to seek information about biometric technologies and input on approaches to governing the use of biometric technologies.

We respectfully submit these comments to share information pertaining to several topics in the RFI, including: (1) descriptions of use of biometric information for recognition and inference; (2) procedures for and results of data-driven and scientific validation of biometric technologies; (3) security considerations associated with a particular biometric technology; (4) exhibited and potential harms of a particular biometric technology; (5) exhibited and potential benefits of a particular biometric technology; and (6) governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case.

I. Overview of NEC and Our Biometric Technologies

NEC delivers one of the industry's strongest and most innovative portfolios of biometrics, security, analytics, and ICT solutions for enhanced customer experience, safety, and productivity. Headquartered in Irving, Texas, NEC (https://www.necam.com/) is a subsidiary of NEC Corporation, a global technology firm with $28 billion in annual revenue, a presence in over 160 countries and regions, and more than 110,000 employees worldwide. NEC Corporation has had a presence in the United States since 1963, and, today, our major U.S. offices span 16 states and employ over 2,000 people. One of the world's top patent-producing companies, NEC Corporation combines advanced technologies, services, knowledge, and our 120 years of operating experience to help promote safety, security, fairness, and efficiency and build a more sustainable world in which all people have the opportunity to reach their full potential.

For over thirty years, NEC has been a leader in the biometrics industry. We invest significant resources in research and development and proudly provide both public-sector and private-sector customers with effective, efficient, and secure biometrics solutions, including predictive genotyping technologies and unimodal and multimodal face, voice, iris, fingerprint, latent print, palm print, and tenprint technologies.[2]

[1] *See* Office of Science and Technology Policy, *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies*, 86 FR 56300-02, Document No. 2021-21975 (pub. Oct. 8, 2021) (Public Notice).
[2] We have also developed ear acoustic and gait recognition capabilities.

We began our biometrics business as a leading provider of Automated Fingerprint Identification Systems (AFIS) to state and local law enforcement agencies, and we built on our law enforcement expertise to become a trusted biometric technology provider to the U.S. Federal Government. Additionally, we provide commercial customers in the aviation, health care, entertainment, financial services, and hospitality industries with a variety of unimodal and multimodal biometric solutions.

U.S. Customs and Border Protection (CBP) uses NEC's face recognition algorithm to fulfill its Biometric Entry/Exit mandate and improve security and traveler experiences at air, land, and maritime ports of entry in the United States. CBP has built and implemented its biometrics capabilities through public-private partnerships with airlines and airports that are working to modernize air travel and keep pace with the customer experience and security demands in the global aviation market. CBP's biometrics programs have been the subject of numerous audits and reviews, including Privacy Impact Assessments,[3] Government Accountability Office (GAO) reports,[4] and congressional hearings.[5] These reviews and audits have highlighted the accuracy of NEC's algorithm, the numerous data privacy and cybersecurity protections that CBP and its partners leverage to safeguard traveler data, and the overall benefits that the programs produce.[6]

NEC has also developed and deployed multimodal biometric solutions that can help improve airport safety during the COVID-19 pandemic. These solutions incorporate both face detection or recognition and thermal sensing technologies that help detect elevated body temperatures among travelers and airport and airline employees. By enabling contactless elevated body temperature detection, identification, and/or identity verification, similar solutions can help employees in other industries safely return to work.

Star Alliance uses NEC's face recognition technology on a mobile application (the Star Biometrics Hub) and at bag drops, kiosks, check-in, membership lounges, and gate boarding.[7] The Star Biometrics Hub (SBH) is an opt-in digital identity platform with robust cybersecurity measures and privacy protections, including limitations on personal data storage and sharing, in compliance with European Union General Data Protection Regulation requirements. With a single enrollment, travelers can use the service with any participating airline and at any participating airport. Because the NEC face recognition algorithm that SBH leverages is highly accurate with face masks, travelers do not have to remove their masks in order to move throughout the airport in a fast, accurate, contactless manner and without showing documents that contain personally identifiable information.

In the entertainment and hospitality industries, amusement parks and entertainment and sports venues use NEC fingerprint and face recognition technologies to facilitate opt-in ticketless entry and VIP access control. By integrating face recognition technologies into exhibits that also use digital touch screens, virtual

[3] https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service

[4] https://www.gao.gov/assets/gao-20-568.pdf

[5] Of particular significance, on February 6, 2020, the House Committee on Homeland Security held a hearing that explained how the Department of Homeland Security (DHS) is utilizing face recognition technology in Biometric Entry/Exit programs. This hearing followed the December 2019 release of NIST's *FRVT Part 3: Demographic Effects (NISTIR: 8280)* report, which provided insight into how different vendors' face recognition algorithms performed across demographic groups. Witness testimony and Committee questions conveyed several important findings from this NIST report, including that NEC's algorithm and other top-performing algorithms do not exhibit detectable differences in false positive error rates across demographic groups. Ranking Member Rogers stated, "NIST determined that [the] facial recognition algorithm being adopted by DHS has no statistically detectable race or gender bias. In other words, NIST could find no statistical evidence that facial recognition algorithms that DHS is adopting contains racial bias." John Wagner confirmed that "CBP is using an algorithm from one of the highest-performing vendors identified in the report" and that CBP is "not seeing those demographic-based error rates in its deployments." After the hearing, Chairman Thompson said, "I want to put the safeguards in place so that as we roll out technology we can assure the public that this is not an invasive technology." He continued, "We're not prying in folks' bedrooms. This is strictly a method of identification that helps keep us safe."

[6] On its website, CBP explains its efforts to secure personal data in its biometrics programs through robust requirements for partners who collect data and through CBP's own data management, including secure encryption and authentication, biometric template protections, brief retention periods, and secure storage practices. https://www.cbp.gov/travel/biometrics/biometric-exit-faqs; https://biometrics.cbp.gov/#privacy.

[7] https://www.staralliance.com/en/biometrics; https://www.nec.com/en/press/202012/global_20201201_02.html

reality technologies, and gesture technologies, NEC helped a museum create a personalized experience for guests who opt in. A beach resort uses our face recognition technologies to give guests who choose to use these technologies the freedom to leave their wallets behind and move through the resort using their faces to access amenities and make payments.

NEC's state and local government customers use biometric technologies to promote public safety. State departments of transportation and motor vehicles leverage NEC face recognition technologies to compare photos in applications for new or renewed driver's licenses to existing photo databases, in order to help detect potential attempts to create multiple identities or to use fraudulent identities. These identity theft and fraud detection solutions include a case management system that enables oversight of face recognition technology query results, and we help customers integrate these solutions into more comprehensive processes that include multiple levels of trained human review. State and local law enforcement agencies also use NEC's Multimodal Biometric Information Systems (MBIS) as tools to query existing state or federal databases to more efficiently and effectively generate leads in criminal investigations. The results from these biometric technology queries do not independently constitute grounds for arrest, and the biometric technologies do not substitute, but rather only support, traditional investigative techniques.

We partner with NGOs, international organizations, and governments around the world to leverage our biometric technologies in ways that help solve societal problems[8] and make progress towards achieving the United Nations Sustainable Development Goals.[9] For example, we collaborated with the United Nations High Commissioner for Refugees and the United Nations Development Programme to provide a refugee registration system and a voter registration system that use NEC fingerprint technologies. In partnership with Gavi and Simprints, we have worked to improve immunization coverage in developing countries around the world by developing and deploying the world's first scalable fingerprint identification solution that gives children aged one through five a digital ID linked to an accurate, complete medical record. We have also worked with the International Committee of the Red Cross to harness biometric technologies to deliver critical humanitarian aid more efficiently and effectively. Furthermore, we have memorandums of understanding for biometrics projects with other international organizations, including the World Food Programme and the United Nations Industrial Development Organization.

NEC is proud of the benefits that our biometric technologies have brought to communities around the world and of the successful international partnerships that produced these beneficial solutions. We are committed to supporting efforts to help communities worldwide continue to simultaneously benefit from biometric technologies and mitigate the risks that the technologies can pose. Below, we provide more information about biometric technologies, the risks and benefits that biometric technologies can produce in different settings, our ongoing initiatives to promote responsible use of biometric technologies, and biometric technology governance approaches.

II. Biometric Technology Definitions, Functional Applications, and Testing/Validation

Definitions of biometric technologies vary, but commonalities exist across definitions.[10] In general terms, biometric recognition technologies provide an automated means by which to determine an individual's identity based on the individual's unique biological characteristic/feature. Many biometric recognition technologies accomplish this task by generating a mathematical representation of an individual's unique physical attribute (often called a biometric "template") and then comparing the newly generated template (often called a "probe" template) to one or more templates that are stored in a gallery, in order to determine the degree of similarity between the probe template and gallery template(s). When the biometric recognition technology compares the probe template to a single individual's gallery template, the technology

[8] https://www.nec.com/en/global/about/brand/

[9] https://www.nec.com/en/global/sdgs/index.html

[10] *See, e.g.*, https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en; https://csrc.nist.gov/glossary/term/biometrics; https://www.biometricsinstitute.org/what-is-biometrics/; https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf

is performing "verification" (often denoted "1:1 comparison"). When the biometric recognition technology compares the probe template to many or all individuals' gallery templates, the technology is performing "identification" (often denoted "1:N comparison").

Many individuals and organizations use the term "biometric technologies" to refer only to biometric recognition technologies,[11] but some individuals and organizations use the term "biometric technologies" to also include biometric detection and biometric characterization technologies.[12] Biometric detection technologies provide an automated means by which to help determine whether a person and/or particular biometric feature is present, without attempting to determine the person's identity. Biometric characterization technologies provide an automated means of estimating or inferring a person's emotional state or demographic characteristics based on the person's biological characteristic(s)/feature(s), but these technologies also do not attempt to identify the person. In this comment letter, we use the term "biometric technologies" to refer only to biometric recognition technologies.

Biometric technology providers store biometric information in the form of biometric templates that are unique to each vendor and product, and vendors employ sophisticated measures to protect biometric templates and promote data privacy and data security. Biometric templates generally contain less information than the original images and audio files do, and biometric templates include data protection measures that prevent restoration of the original image or audio file from the biometric template. Furthermore, unlike a single password that multiple systems may store as the same set of characters, because the biometric template that each vendor/algorithm generates for a given biometric modality is unique, biometric templates for the same biometric feature differ across vendors and products. Therefore, even if a bad actor breached and decrypted the biometric data, the breach would not compromise individuals' information across all biometric systems. Moreover, similar to the way that vendors can change individuals' alphanumeric passwords, vendors can change individuals' biometric templates, which means that individuals would not need to change their physical features in order to mitigate the negative consequences of a biometric data breach.

In large part due to their demonstrated accuracy and the aforementioned privacy and security attributes, a wide variety of users are increasingly interested in leveraging biometric technologies to help facilitate secure and efficient authentication, access control, remote and digital identification, and process automation.[13] In addition to internal testing that companies perform on their own algorithms, independent standards bodies and testing authorities around the world help validate and improve many biometric technologies' performance.[14] For example, the National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) organize and direct biometric technology vendor testing of biometric algorithms and full biometric systems, respectively. NIST conducts benchmark testing that evaluates fingerprint, iris, and face verification (1:1 comparison) and identification (1:N comparison) algorithms from vendors around the world.[15] DHS S&T Biometric Technology Rallies test full biometric technology systems' performance.[16] Vendors also work to build trust

[11] https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf; https://www.mitre.org/sites/default/files/publications/biometric-face-recognition-references-for-policymakers.pdf; https://itif.org/publications/2020/04/08/itif-technology-explainer-what-facial-recognition; https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition

[12] *See, e.g.*, https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/ (referring to the face characterization technologies used in the *Gender Shades* study as "facial recognition systems").

[13] *See, e.g.*, https://www.gao.gov/assets/gao-20-522.pdf; https://www.gao.gov/assets/gao-21-526.pdf.

[14] Before selling or deploying new biometric technologies, vendors largely agree that conducting internal and/or external testing to evaluate performance and accuracy overall and across demographic groups and other challenging use cases is crucial. *See, e.g.*, https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf; https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/#core.

[15] https://www.nist.gov/programs-projects/biometrics

[16] https://www.dhs.gov/science-and-technology/biometric-technology-rally

in and validate their biometric technologies by complying with standards from the International Standards Organization (ISO), Organization of Scientific Area Committees for Forensic Science (OSAC) Facial Identification Subcommittee and Facial Identification Scientific Working Group (FISWG), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), and similar organizations.

NEC recognizes the importance of validating and improving our biometric technologies' performance and of contributing to the global development of standards and best practices for biometric technology development, deployment, and use. To do so, we participate in biometric technology standards working groups, work to adhere to relevant biometric technology standards and best practices, and seek out opportunities to submit our biometric technologies to independent, third-party testing. Specifically, to obtain independent evaluations of our biometric algorithms' accuracy overall and across demographic groups and other challenging use cases, NEC has been participating in NIST vendor tests for well over a decade and in DHS S&T Biometric Technology Rally testing since its inception. We have consistently ranked among the top providers of fingerprint (ranked first eight times since 2003), iris (ranked first twice since 2018), and face (ranked first six times since 2009) recognition algorithms in NIST tests. Most recently, we earned the top rank in NIST's 2021 1:N iris recognition benchmark test[17] and the top rank for identifying individuals in law enforcement mugshot photos and border images (10+ years) in NIST's 2021 1:N face recognition benchmark test.[18] NEC face recognition technologies also were the most accurate at identifying individuals both wearing and not wearing face masks in DHS S&T's 2020 Biometric Technology Rally.[19]

III. Biometric Technology Benefits, Risks, and Risk Mitigation Approaches

The risks and benefits that biometric technologies can produce differ based on the biometric modality and functional application selected and the setting and way in which users deploy the technologies. Technology vendors; end users; other privacy experts; and federal, state, and local government entities have developed strategies and techniques to help mitigate many of the risks that biometric technologies can pose, but continued policymaker and multi-stakeholder risk mitigation efforts would be helpful.

A. Different biometric technology modalities and functional applications can create different opportunities and challenges across use cases.

The industry widely recognizes several biometric technology modalities, including face, iris, voice, fingerprint, palm print, latent print, tenprint, finger vein, ear acoustic, and gait.[20] Many also consider DNA and predictive genotyping technologies to be biometric technologies.[21] Generally, the more unique and consistent a biological feature is, the more accurate of an identifier that feature is. For example, an individual's DNA sequence is very unique and stays consistent over time. In contrast, an individual's gait is less unique and consistent over time. However, even the most accurate identifiers are not only or always the best choice for a given use case, and different modalities create distinct benefits and risks.

The visibility of the biological feature; the ease, speed, comfort, and cost of gathering information about the biological feature; and other considerations can impact whether or not a biological feature is an appropriate modality candidate for a given use case. For example, people's faces are highly visible in public, and taking photos of individuals' faces is relatively easy and inexpensive to do and can occur at a distance and in a contactless manner. On the other hand, people's fingerprints are not as visible in public, and capturing individuals' fingerprints can be challenging at a distance and/or without requiring individuals to make contact with or get very close to a surface or object. Due to these differences, biometric technologies that help identify individuals based on their faces may be more useful in settings where contactless

[17] https://www.nec.com/en/press/202109/global_20210922_02.html
[18] https://www.nec.com/en/press/202108/global_20210823_01.html
[19] https://www.businesswire.com/news/home/20210309005244/en/NEC-Tops-Competition-in-Identifying-Subjects-Wearing-Face-Masks-at-DHS-2020-Biometric-Technology-Rally
[20] https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/
[21] https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

identification is a priority. Where contactless identification is less of a priority and where environmental conditions make capturing high-quality face images difficult, biometric technologies that help identify individuals based on their fingerprints may be more useful.

i. Modality-Specific Risks Related to Enabling Unlawful Ongoing Surveillance

Different biometric technology modalities and functional applications also pose different risks, including privacy and broader civil rights and civil liberties risks related to enabling unlawful ongoing surveillance.[22] For example, because capturing fingerprints in real time requires a person to touch or get very close to a specific object and cannot easily occur at a distance, fingerprint technologies, such as those that many people use to unlock devices and access secure facilities, are unlikely to infringe on individual privacy by enabling unlawful ongoing surveillance. At the same time, having many individuals come into close contact with the same objects could contribute to the spread of infectious diseases, like COVID-19. Iris and voice recognition technologies do not necessarily require an individual to touch an object, but they are not effective at significant distances. Plus, iris recognition technologies require individuals to look directly at a specific point under specific lighting conditions, and voice recognition technologies are less effective when background noise is present. Therefore, iris and voice recognition technologies are unlikely to enable unlawful ongoing surveillance in public spaces or crowded private spaces.

Face recognition systems that require an individual to take a photo at a kiosk, such as those that enable contactless payment and contactless access control, require active user engagement and do not capture an individual's biometric information at a great distance or on an ongoing basis. Therefore, these face recognition systems are also unlikely to contribute to unlawful ongoing surveillance. In contrast, if misused, real-time video monitoring face recognition (and, in particular, identification) solutions could enable unlawful ongoing surveillance because these technologies could potentially enable users to identify and track individuals in real time, at a distance, and without the individuals' awareness. However, these same real-time video monitoring face identification solutions can help perform tasks like identifying missing and exploited children and human trafficking victims in security camera footage.[23]

These examples illustrate that some modalities and functional applications pose greater risks of enabling unlawful ongoing surveillance than other modalities do. Yet, the same modalities and functional applications that could enable unlawful ongoing surveillance can also support lawful public health and safety efforts. Consequently, as we explain in more detail below, to simultaneously protect privacy and reap the benefits that biometric technologies can produce, taking a tailored approach to risk mitigation that differentiates between modalities and functional applications is important.

ii. Risks Related to Perpetuating Harmful Bias

Policymakers and media outlets have been increasingly focused on investigating and addressing ways in which biometric technologies could potentially perpetuate harmful impacts of bias. We appreciate the focus on this important issue and are dedicated to working with other stakeholders on initiatives that aim to ensure that the use of biometric technologies helps advance racial and broader social justice. Biometric technology bias issues are multifaceted and complex, and they vary across functional applications and use cases, but they generally fall into two main categories: (1) technical issues in the biometric technologies that produce inconsistent performance across demographic groups and (2) ways in which the use of biometric technologies can perpetuate bias in society.

Any biometric technology modality can exhibit bias by performing differently across demographic groups, and several components of biometric technologies can contribute to these demographic performance differences. One such component is the biometric algorithm. For example, NIST's December 2019 *FRVT*

[22] *See, e.g.*, https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem; https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Beyond%20Bans%20Policy%20Options%20for%20Facial%20Recognition%20and%20the%20Need%20for%20a%20Grand%20Strategy%20on%20AI.pdf.
[23] https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/

Part 3: Demographic Effects (NISTIR: 8280) report found that many face recognition algorithms do exhibit significant differences in performance across demographic groups and exhibit lower accuracy rates for darker-skinned women than lighter-skinned men.[24] However, this report also found that several algorithms, including NEC's, had "undetectable" false positive error rate differences across demographic groups and that NEC's algorithm had the lowest false negative demographic differential.[25]

The capture device is another component of the biometric technology system that can impact system performance across demographic groups. If capture devices, such as cameras, fingerprint scanners, iris scanners, and sound recording devices, generate poorer quality probe images or audio files for individuals who are members of particular demographic groups, these devices can contribute to lower accuracy rates across those demographic groups. Further research into capture device performance across demographic groups and the ways in which capture device quality impacts biometric technologies' operational performance would be helpful, but DHS S&T has already done commendable work evaluating certain biometric technologies' full system performance. As we mentioned above, NEC has consistently ranked among the top technology vendors in DHS S&T Biometric Technology Rally tests, most recently achieving face recognition technology accuracy rates of >98% with face masks and >99% without face masks.[26]

Questions about face recognition technologies' performance across demographic groups have received the most media and policymaker attention in recent years, but other biometric technologies have encountered and overcome demographic performance issues as well. For example, fingerprint technologies did not always perform consistently across racial groups and have historically struggled to identify very young children due to the small size and limited development of child fingerprints. Nonetheless, NEC's partnership with Gavi and Simprints provides a practical example of how fingerprint technologies have advanced enough to accurately identify one-year-olds who are members of diverse racial groups.

Using inaccurate biometric technologies has the potential to perpetuate bias and inequity in society. Technologies that do not perform accurately overall and across demographic groups can reinforce the harmful impacts of bias by contributing to more frequent misidentifications of individuals who are members of marginalized groups. Without adequate oversight and mitigation, these misidentifications can contribute to processing delays, unnecessary contact with law enforcement officials, and other negative experiences for individuals who already face disproportionate challenges and barriers in our society. Conversely, when used appropriately, biometric technologies that perform highly accurately overall and across demographic groups can help reduce the harmful impacts of bias by making identifications more accurate.

Furthermore, because biometric technologies compare templates without making assumptions about an individual's demographic characteristics, highly accurate biometric technologies can act as a check on inherent biases that often contribute to misidentifications, including in high-stakes criminal justice settings. Nonetheless, even biometric algorithms that are highly accurate overall and across demographic groups can perpetuate biases when they increase the speed and accuracy of processes, institutions, and systems that produce biased outcomes. Considering and addressing the impact of biases in processes, institutions, and systems are important elements of multi-stakeholder efforts to support ethical use of biometric technologies.

B. The risks and benefits that each biometric technology modality and functional application can produce vary across use cases.

Using biometric technologies to aid in identification and identity verification tasks creates different degrees of risk in different settings. Generally, higher-risk use cases are those in which the use of biometric technologies substantially contributes to decisions that most significantly impact civil rights, civil liberties, and/or human rights. Because accurately identifying individuals (or verifying their identities) is especially

[24] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
[25] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; *see also* https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms; https://www.gao.gov/assets/gao-20-522.pdf
[26] https://www.businesswire.com/news/home/20210309005244/en/NEC-Tops-Competition-in-Identifying-Subjects-Wearing-Face-Masks-at-DHS-2020-Biometric-Technology-Rally

important in these use cases, using biometric technologies in ways that improve identification and identity verification accuracy, including as part of processes that incorporate trained human review and other safeguards, can also be especially beneficial.[27]

Although commercial uses, and especially uses pertaining to healthcare systems, financial institutions, and payment systems, can pose risks that are important to consider and address, public-sector uses of biometric technologies can create higher risks. Within the public-sector, law enforcement uses of biometric technologies tend to pose the greatest risks, followed by use cases that deal with access to essential government services, like driver's license applications and benefits administration. Law enforcement use of real-time video monitoring face recognition technologies is widely regarded as the highest-risk potential biometric technology use case. Regardless of who does the tracking, automatically tracking an individual's location and monitoring an individual's behavior from a distance and potentially without the individual's consent or awareness could be concerning from a privacy and broader civil rights perspective. If law enforcement agencies are the ones using real-time video monitoring face recognition technologies, the automated tracking and monitoring could contribute to an individual's arrest and, later on, incarceration. This makes law enforcement use of these technologies particularly high-risk. Because other identifications in law enforcement settings, such as those that help generate investigative leads, can also contribute to arrest decisions, such use cases are also relatively high-risk and require additional policy safeguards to mitigate unintended consequences.

IV. NEC Promotes Responsible Use of Biometric Technologies through Our Commitment to Building Digital Trust and Upholding Our AI and Human Rights Principles

NEC Corporation's Digital Trust Business Strategy Division (DTBSD) works with multiple corporate functions on several environmental, social, and governance (ESG) initiatives.[28] Key among those ESG initiatives are ongoing efforts to formulate and implement a strategy for promoting human rights in our biometrics and broader AI business. In 2018, DTBSD leveraged internal and external expert perspectives to develop the NEC Group AI and Human Rights Principles, which promote: (1) fairness; (2) privacy; (3) transparency; (4) responsibility to explain the effects, value, and impacts of AI utilization; (5) proper utilization of AI technology; (6) continued development and improvement of AI technologies; and (7) dialogue with multiple stakeholders. We are committed to upholding our AI and Human Rights Principles through corporate governance initiatives, product risk management practices, customer and partner relationship management approaches, and internal and external multi-stakeholder engagements.

One global corporate governance priority that helps operationalize the Principle of privacy is continuing to update and comply with the NEC Corporation Privacy Policy and our personal information protection management system requirements. Both our Privacy Policy and our personal information protection management system mandate handling personal information in accordance with applicable laws and relevant industry standards, including the requirements in Japan's Act on the Protection of Personal Information and JIS Q 15001, the Japanese industrial standard for safe and appropriate management of personal information in corporations' and other organizations' operations. We have also implemented data breach response procedures to help ensure that, if a data breach does occur, we are well positioned to respond effectively and in a manner that minimizes harm to the individuals whose personal information we retain. In recognition of these efforts, we have been PrivacyMark-certified for many years and first earned our certification in October 2005.[29] As of March 2021, NEC Corporation and thirty of our affiliated companies hold the PrivacyMark certification.

[27] https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner; https://www.gao.gov/assets/gao-21-435sp.pdf.

[28] https://www.nec.com/en/global/csr/index.html

[29] To earn the PrivacyMark certification, companies must comply with JIS Q 15001 and gain third-party organization recognition for having systems in place to ensure appropriate protection measures for personal information. The PrivacyMark certification also prohibits companies from collecting information that could economically impact an employee, such as bank account and

To develop, manage, and improve other policies, programs, and practices as part of our global human rights promotion strategy, DTBSD consults diverse experts from around the world about human rights issues relevant to our business and to the communities in which we operate. DTBSD also collaborates with other internal teams worldwide, including the People and Organization Development Division, global quality management and cybersecurity teams, and regional subsidiary teams that are working to build digital trust in their local markets. One such regional subsidiary team is the U.S.-based Digital Trust Initiative (DTI), which takes a three-pillared approach to building digital trust by promoting (1) reliability, (2) ethics and human rights, and (3) security in our business practices, services, and technologies. One of DTI's top priorities is continuing to operationalize the NEC Group AI and Human Rights Principles in our U.S. biometrics business.

In our biometrics business, we uphold the NEC Group AI and Human Rights Principles in our approaches to product design and development, customer and partner screening, product deployment, and customer support and training. Throughout the process of designing and developing our biometric technologies, NEC leverages safeguards such as encryption (including homomorphic encryption[30]), data minimization, data aggregation, data anonymization, and algorithm layering. We also test our biometric technologies' performance internally and submit our technologies to third-party testing authorities, like NIST and DHS S&T, to verify that our technologies perform accurately overall and across demographic groups. Before selling our highest-risk biometric technology solutions through new partners and/or to new customers, we believe that considering the prospective partners' and customers' human rights records and risk mitigation policies is important. We aim to sell only through trusted partners and to trusted customers, and we are willing to decline business opportunities that we determine may pose too great a risk to human rights. After we decide to sell a biometric technology solution to a customer, we work with the customer (and, if applicable, the partner(s)) to plan and execute deployments and to train individuals operating the biometric technology systems on proper use. We recommend that customers adopt use policies that require safeguards, such as appropriate human review of query results and continuous system performance monitoring, and we provide system operators with ongoing support via a customer service helpline and field site visits. We also work with our partners and customers around the world to facilitate multijurisdictional legal compliance (including by completing privacy impact assessments) and to consider ethical issues that may arise in the context of customers' biometric technology deployments. Our consideration of these ethical issues reflects perspectives gained through collaboration with diverse internal and external stakeholders.

Internally, we are actively working to strengthen human rights literacy and to promote diversity, equity, and inclusion (DEI) throughout NEC, and particularly on our biometrics and broader AI teams. In addition to providing training programs and advancing other education and information sharing initiatives, we recognize the importance of continuing to deepen collaboration between our DEI Steering Committee, our Digital Trust Initiative, and our broader product and leadership teams. This collaboration will help NEC more completely embed our commitments to DEI and social justice into our policies, programs, and practices for designing, developing, deploying, and evaluating our biometric and other AI technologies.

To inform our perspectives and positions on issues at the intersection of biometric technologies and civil and human rights, we also participate in dialogues with a wide array of external stakeholders, including policymakers, civil society organizations, think tanks, industry groups, end user groups, and academic and government researchers around the world. We welcome opportunities to serve as a resource to policymakers

credit card information; sensitive information, such as birthplace; or highly private information, such as a mobile telephone number, without obtaining consent. https://privacymark.org/about/outline_and_purpose.html

[30] "Homomorphic encryption for biometric matching holds the promise of data protection even in use, and NEC Corporation is the latest technology provider to develop a system that it says delivers on this promise, with the key difference that the company says it can be used for one-to-many searches. Biometric data encrypted between collection and transmission to a server or service provider for matching prevents the leakage of raw images, which can be subsequently utilized in spoofing attacks. In the system developed by NEC, the decryption key is held by the user, rather than the service provider, providing users with additional assurance their information is protected." https://www.biometricupdate.com/202112/nec-streamlines-1n-biometric-matches-for-homomorphic-encryption-to-protect-data; *see also* https://www.nec.com/en/press/202112/global_20211216_02.html.

and other stakeholders who are interested in learning more about biometric technologies and developing approaches to mitigating biometric technology risks while realizing biometric technology benefits.

V. Policymakers Can Develop Governance Frameworks to Promote Responsible, Trustworthy Use of Biometric Technologies

Developing governance frameworks that promote privacy and other civil rights and civil liberties, racial and broader social justice, safety, security, economic efficiency, and technological innovation requires a nuanced analysis and approach to regulating different types of biometric technologies in different settings.

Many of the biometric technology governance principles, frameworks, and recommendations that technical experts, government agencies, privacy professionals, and scholars have developed[31] require strong cybersecurity protections; appropriate and feasible notice and consent to the use of biometric technologies and related data collection; limitations on data handling, storage, retention, and transfer; both internal and independent, third-party testing before and after deploying biometric technology systems; operator training; public reporting and oversight to the degree appropriate for various use cases; meaningful human review of high-stakes biometric technology query results; prohibitions on discrimination in decision-making based on biometric technology query results; and other use limitations that ensure existing constitutional protections appropriately demarcate uses of biometric technologies in the United States. Although these types of requirements are common across numerous proposed governance principles and frameworks, the specific details of each requirement vary based on the risk associated with each biometric technology modality, functional application, and use case.

In addition to establishing requirements for the use of biometric technologies, policymakers can develop governance frameworks that promote transparent government procurement and deployment of high-quality, regularly upgraded biometric technology systems. These governance frameworks can also support continued biometric technology research by NIST, DHS S&T, academic institutions, and public-private partnership teams. Such research should address topics such as the performance of full biometric technology systems and particular system components across demographic groups, risk mitigation strategies for biometric technology design and deployment, operational testing of biometric technologies to evaluate accuracy both overall and across demographic groups, and best practices for human operation of biometric technologies and human review of biometric technology query results to promote accuracy and to identify and overcome any bias.

VI. Closing

We recognize that, due to space constraints, our comments in this letter only begin to address the complex issues that OSTP's RFI raised. We would welcome future opportunities to discuss the risks and benefits that biometric technologies can produce and potential biometric technology governance approaches in greater depth. In particular, we would be interested in participating in working groups and/or multi-stakeholder dialogue sessions that specifically address particular biometric technology use cases, modalities, and/or functional applications.

Sincerely,

Shin Takahashi
Chairman and Head of Government Relations and Public Policy

[31] https://www.gao.gov/assets/gao-20-522.pdf; https://www.mitre.org/sites/default/files/publications/biometric-face-recognition-references-for-policymakers.pdf; https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape; https://www.gao.gov/assets/gao-21-435sp.pdf; https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf; https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

New America's Open Technology Institute

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

OPEN TECHNOLOGY INSTITUTE | NEW AMERICA

New America's Open Technology Institute Input to the Office of Science and Technology Policy (OSTP) RFI on Public and Private Sector Uses of Biometric Technologies

January 2022

AI-based biometric technologies are increasingly being developed and deployed in the public and private sectors, posing numerous threats to privacy, civil rights, and fundamental freedoms. New America's Open Technology Institute (OTI) welcomes the opportunity to submit comments on the use of such biometric technologies for identity verification, identification of individuals, and inference of attributes including individual mental and emotional states. As OTI outlines below, a range of AI-based biometric surveillance tools are deployed by law enforcement and U.S. immigration authorities. Additionally, numerous private entities develop and use biometric technologies to fuel their marketing and advertising practices. Despite the expansive use of AI-based biometric tools, there are few existing safeguards to protect privacy and generate fairness, accountability, and transparency.

AI-Based Biometric Surveillance Technologies: Use of AI-based biometric surveillance technologies pose a variety of serious risks, including threatening individual and community privacy by allowing invasive and persistent tracking and targeting, disproportionately misidentifying certain demographics, and threatening individuals' rights because their use is so often secretive and undisclosed, or otherwise very difficult to challenge. These problems are true of many AI-based biometric technologies, but one exemplary tool that highlights the gravest issues with biometric technologies is facial recognition, which we will focus on below. Many of these concepts are not unique to facial recognition tools, however, and apply more widely.

Facial Recognition: First, use of facial recognition threatens individual and community privacy by allowing invasive and persistent tracking and targeting. Law enforcement agencies routinely use facial recognition technology to compare an image from CCTV cameras or other sources with face image databases maintained by local, state, and federal agencies. Potentially more than 133 million Americans are included in these databases, with at least thirty-one states giving police access to driver's license images to run or request searches,[1] and twenty-one states giving the FBI access to the same.[2] Law enforcement use of these databases for investigations places millions of Americans in what has been called a "perpetual line-up,"[3] posing particular risk to

[1] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.
[2] *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains,* Government Accountability Office (June 4, 2019), https://www.gao.gov/products/GAO-19-579T.
[3] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.

privacy and access to public space for Black and Brown people, immigrants, and other groups who are routinely targeted by police.

Facial recognition, especially when used with persistent surveillance camera networks, further erodes anonymity in public spaces, allowing law enforcement to perpetually track the movements of nearly any person at any time. Major American cities have piloted persistent facial surveillance, which continuously scans live video to identify individuals.[4] Such tracking undermines fundamental rights to association, expression, and privacy.[5] The Supreme Court's 2018 decision in *Carpenter v. United States* held that warrantless location tracking using cell site location data for more than seven days is unconstitutional.[6] Persistent face surveillance can "catalogue every single movement" of individuals in the same way, and it's arguable that such tracking would be unlawful under a *Carpenter* analysis.[7]

Numerous studies have shown that facial recognition technology contains alarming inaccuracies, and is particularly less accurate on certain groups, including women and people with darker skin.[8] The National Institute of Standards and Technology's Face Recognition Vendor Test found significant variation in both false positive and false negative error rates[9] across race, sex, and age with the highest false positives for U.S. law enforcement mugshots among Black, Asian, and Indigenous people.[10] In a comparison of match rates by country of origin, photos of people from East African countries had false positive rates 100 times higher than the baseline rate.[11]

In fact, multiple cases have come to light in the past couple years of facial recognition misidentifications leading to wrongful police action--all involving Black men. In late June 2020, Robert Williams, a Black man from the Detroit area, shared his story of being wrongfully arrested due to facial recognition technology.[12] Williams was imprisoned for robbery after the technology misidentified him. And more recently, another Black man in Detroit, Michael Oliver, came forward to tell his similar story of wrongful arrest based on facial recognition.[13] Much like Williams, Oliver was imprisoned for a larceny he did not commit. Both the cases of Robert

---

[4] Clare Garvie and Laura Moy, *America Under Watch: Face Surveillance in the United States*, (May 16, 2019), https://www.americaunderwatch.com.

[5] *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.")

[6] 138 S.Ct. 2206 (2018).

[7] *Id.* at 2217, quoting *Jones* at 430 (Alito, J., concurring).

[8] *See, e.g.,* Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[9] A false positive occurs when a person is incorrectly matched to a photo in the database when it is not actually them. A false negative occurs when the system incorrectly fails to match a person to their photo in the database.

[10] Patrick Grother, Mei Ngan, and Kayee Hanaoka. "NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects." National Institute of Standards and Technology (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[11] *Id.* at 40.

[12] https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/

[13] https://www.vice.com/en_us/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing

Williams and Michael Oliver – and likely plenty more misidentifications that have gone unreported – add to the already compelling evidence that the technology is biased and dangerous in the hands of law enforcement.

But the technology is dangerous even when accurate. Even aside from the bias and inaccuracy issues inherent in the technology, facial recognition and all surveillance technologies are deployed in our imperfect nation, where law enforcement biases, misuse, uneven application, and disproportionate use in Black and Brown communities mean that those communities are much more vulnerable to its harms.

Police use of facial recognition technology not only invades privacy through its omnipresence, it also chills speech. FBI and even local police have a long history of surveilling civil rights protests.[14] And facial recognition technology, one of the most powerful surveillance tools imaginable, can identify thousands of protestors from a single CCTV camera. While such surveillance is not new, tracking of this scope and scale is, and undermines a foundational principle of our democracy—our right to free speech. But reports confirm that police in many jurisdictions have continued to use facial recognition technology to monitor Black Lives Matters protestors.[15]

Law enforcement use of facial recognition can also easily violate due process rights and otherwise infringe upon procedural justice. New technologies, including these systems, often allow law enforcement to circumvent existing legal protections for individuals. Due process requirements govern law enforcement actions throughout the criminal legal process, including stop-and-frisks, investigations, searches, arrests, and beyond. Yet, in the twenty years that facial recognition has been used in some jurisdictions, defendants' rights to due process protections have been essentially non-existent when it comes to the technology.[16] The ability to assess the reliability of both the facial recognition systems and the ways in which they are used is critical to ensuring due process of law. Protecting due process rights and preserving *Brady*[17] rights would require that law enforcement agencies disclose key details about the design and use of the system that impact the reliability of matches.

And because prosecutors and law enforcement often conceal the use of facial recognition in criminal trials, it may be difficult, if not impossible to ensure that defendants are able to exercise

---

[14] https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html

[15] https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram

[16] Jennifer Valentino-DeVries, *How The Police Use Facial Recognition, And Where It Falls Short,* N.Y. Times (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[17] *Brady v. Maryland*, 373 U.S. 83 (1963). "The *Brady* Rule," or "*Brady* rights," as they are commonly known, require that prosecutors disclose materially exculpatory evidence in the government's possession to the defense.

their Sixth Amendment rights.[18] Under the Sixth Amendment, any evidence that is considered "testimonial" in a case should be subject to examination in order to uphold those rights. Facial recognition is increasingly used to identify the accused,[19] meaning that each step in the design and use of the technology must be disclosed in detail to defendants, who then have the right to challenge those procedures and algorithms in court. Complicating these issues, companies often make intellectual property claims to trade secrets to protect their algorithms and prevent their inner workings from coming to light, impeding defendants' rights to confront evidence in court.[20]

Immigrant Surveillance:

Law enforcement is also using AI-enabled biometric technologies extensively to surveil immigrants, and some of the most invasive technologies are used in the immigration context. For example, the Department of Homeland Security (DHS) is planning to build the Homeland Advanced Recognition Technology (HART) database[21], an expansive biometrics collection database that will store sensitive personal information about individuals, including facial recognition data, digital fingerprints, iris images, palmprints, voice prints, DNA records, political affiliations, religious activities, and familial and friendly relationship patterns.[22] The HART database is poised to replace DHS' existing Automated Biometric Identification System (IDENT), and it will be interoperable with the biometric databases used by the Department of Justice, State Department, and Department of Defense. The contents of the HART database will also be available to state and local governments in the United States as well as many foreign governments, such as Mexico, El Salvador, Jamaica, and Guatemala, who will have access to the data via information sharing agreements.[23]

The creation and operation of the HART database will have numerous implications for immigrant communities. When an individual seeks out an immigration benefit, such as a green card or DACA, the U.S. government will be able to use the database to access a broad range of

---

[18] Karen Gullo & Jennifer Lynch, *When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them, EFF Tells Court*, EFF.org (March 12, 2019), https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain.
[19] Kashmir Hill, *Wrongfully Accused By An Algorithm,* N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Jennifer Valentino-DeVries, How The Police Use Facial Recognition, And Where It Falls Short, N.Y. Times (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[20] *See, e.g., Wisconsin v. Loomis*, 371 Wis.2d 235, 243 (Wisc. 2016).
[21] "DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1," Department of Homeland Security Publications Library, last modified 2020, https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1.
[22] Jennifer Lynch, "HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' 'Non-Obvious Relationships,'" Electronic Frontier Foundation, last modified June 7, 2018, https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.
[23] Immigrant Defense Project, Just Futures Law, and Mijente, "Freeze Expansion of the HART Database," Just Futures Law, last modified April 2021, https://justfutureslaw.org/wp-content/uploads/2021/04/HART-Appropriations-2022.pdf.

biometric information on the applicant. However, many of the biometrics in the database, such as facial recognition and voice prints may be unreliable, particularly for marginalized communities.[24] The use of these biometrics therefore creates risks that these individuals will be further marginalized and subject to erroneous enforcement. Additionally, the collection and use of biometrics such as DNA samples raise ethical concerns.[25] Despite these concerns, the HART database would be used to make consequential immigration decisions for millions of people.

In addition, the use of the HART database poses several privacy and civil liberties concerns. According to the DHS Office of Biometric Identity Management (OBM), the office responsible for building HART, individuals may not always be aware that the biometrics collected when submitting an immigration-related application will be stored in HART and can be shared with other government branches. But, OBM has noted that this privacy risk cannot be mitigated. OBM also recommends, rather than requires, individuals to review the data that is collected on them to ensure accuracy, completeness, and quality, raising concerns around the validity of data used to inform immigration-based decisions.[26] Lastly, given the massive amounts of data in the HART database, it could be used to identify and track individuals in real time, undermining their ability to exercise their rights to protest, assemble, associate and conduct other daily activities.[27]

In addition, U.S. Customs and Border Protection (CBP) also currently operates a comprehensive biometric entry and exit program which relies on facial recognition technology known as Biometric Facial Comparison Technology. According to CBP, when a traveler (U.S. citizen and non-citizen alike) is arriving in or departing from the United States, they are subject to a biometric face scan.[28] This scan is cross-referenced with an existing passport or visa photo of the traveler, which is stored in a database operated by DHS, to verify the traveler's identity. During this process, a CBP officer may also interview the traveler to determine admissibility.[29]

Since the project's inception in 2017, numerous advocates have noted that these technologies pose a significant threat to privacy and civil liberties. In particular, these tools allow CBP to conduct facial recognition covertly and at scale.[30] As previously outlined, biometric and facial recognition programs operated by law enforcement in the United States have been found to generate flawed and problematic results, particularly for marginalized populations, such as

[24] Immigrant Defense Project, Just Futures Law, and Mijente, "Freeze Expansion," Just Futures Law.
[25] Aziza Ahmed, "Ethical Concerns of DNA Databases used for Crime Control," Harvard Law Petrie-Flom Center, last modified January 14, 2019, https://blog.petrieflom.law.harvard.edu/2019/01/14/ethical-concerns-of-dna-databases-used-for-crime-control/#:~:text=Issues%20with%20using%20DNA%20testing%20in%20law%20enforcement%3A%20Errors&text=These%20issues%20include%20basic%20human,a%20surge%20in%20racial%20disparities.
[26] "DHS/OBIM/PIA-004 Homeland," Department of Homeland Security Publications Library.
[27] Lynch, "HART: Homeland," Electronic Frontier Foundation.
[28] CBP Biometrics, https://biometrics.cbp.gov/.
[29] Spandana Singh, "Biometric Tracking of U.S. Citizens at the Border Poses Significant Risks to Privacy," New America's Open Technology Institute, last modified March 15, 2018, https://www.newamerica.org/oti/blog/biometric-tracking-us-citizens-border-poses-significant-risks-privacy/.
[30] "EPIC v. CBP (Biometric Entry/Exit Program)," Electronic Privacy Information Center, last modified March 2019, https://epic.org/documents/epic-v-cbp-biometric-entry-exit-program/.

people of color.[31] The deployment of this technology therefore creates significant new risks of profiling and further marginalizing these communities at borders. Further, the use of this technology underimes U.S. citizens' ability to manage their identity, which is concerning in the context of First Amendment rights of free association and freedom of expression.[32]

At the moment, there are few measures in place to prevent or opt-out of participating in the program, and there are also few regulations that govern how such biometric information is collected, used, disseminated, and retained, raising serious privacy concerns. Despite these concerns, Biometric Facial Comparison Technology has been deployed across the country. According to CBP, the technology is in use at 199 airports for air entry, including all 14 CBP Preclearance locations, 32 airports for air departure, 12 seaports for use by cruise lines, and at almost all pedestrian and bus processing facilities along the U.S.' northern and southern land borders. Between June 2017 and November 2021, CBP has deployed Biometric Facial Comparison Technology to process 117 million passengers.[33]

AI-Based Biometric Technologies for Marketing and Advertising

Over the past several years, many retailers have adopted the use of AI-based biometric technologies such as facial recognition for security purposes. Beginning in 2016, for example, Saks Fifth Avenue began deploying facial recognition to track shoplifters.[34] More recently, retailers have expanded their use of online and offline biometric technologies to fuel their marketing and advertising practices. Developers and deployers of these technologies assert they can enhance retailers' abilities to understand their consumers, deliver personalized experiences, and turn a profit.[35] However, the use of these technologies is highly invasive, and often occurs without consumer awareness or consent, and with few safeguards to govern data practices.

In an offline context, retailers in the United States – and around the world – have deployed behavioral tracking and facial and voice recognition tools to monitor consumers in their storefronts.[36] These technologies can identify and track shoppers while they are in brick-and-mortar stores to gather data about how long a customer is in a storefront, what items they spent the most time looking at, what facial expressions and gestures they exhibited when

[31] Georgetown Law Center on Privacy & Technology, *Not Ready For Takeoff: Face Scans at Airport Departure Gates*, December 21, 2017, https://s3.documentcloud.org/documents/4334243/Georgetown-Law-report-on-airport-facial.pdf.
[32] "EPIC v. CBP (Biometric," Electronic Privacy Information Center.
[33] CBP Biometrics.
[34] EMarketer Editors, "How Retailers Are Using Biometrics to Identify Consumers and Shoplifters," eMarketer Intelligence Insider, last modified October 3, 2019, https://www.emarketer.com/content/how-retailers-are-using-biometrics-to-identify-consumers-and-shoplifters.
[35] "Biometric Technology Means Big Things for Retail and Hospitality," NCR Global, last modified February 22, 2021, https://www.ncr.com/blogs/biometric-technology-retail-hospitality.
[36] Victoria Petrock, "Biometric Marketing 2019," eMarketer Intelligence Insider, last modified October 3, 2019, https://www.emarketer.com/content/biometric-marketing-2019.

looking at certain items, and more.[37] By combining this information with data like purchasing history, age, and gender,[38] retailers can target consumers with promotions via text and push notifications in real time, and via online advertisements after the consumer has left the store.[39]

Many businesses also collect biometric information from consumers when they are browsing online. For example, numerous retailers use sensors built into smartphones and website code to track and collect information including the angle at which people hold their devices, the pressure consumers apply on a keyboard, how they navigate a mousepad, how quickly a consumer scrolls, and what content consumers spend the most time looking at.[40] Many entities also rely on phone cameras to enable facial recognition tools. Using this information, retailers can generate expansive profiles which can be used to identify consumers within seconds, and inform subsequent marketing and advertising strategies to drive consumer engagement and purchases.[41]

Entities that develop and deploy biometric technologies in online and offline settings argue that the tools confer numerous benefits, including allowing retailers to better understand their consumers and deliver a personalized and more "valuable" experience to their customers.[42] Additionally, some organizations, such as banks, claim these behavioral biometrics enable them to instantly verify identities, therefore promoting greater security for their customers.[43]

However, when businesses deploy these biometric technologies in the online and offline environments, they typically do not disclose when and how they are collecting, using, and sharing consumer biometric data. As a result, these companies are collecting highly sensitive and invasive data on their consumers without providing these individuals with any opportunity to opt-out or control if and how their data is being collected and used.

In addition, the use of biometric technologies to fuel marketing and advertising efforts is particularly concerning given the extensive targeted advertising practices that already exist in the digital world. As OTI has highlighted in our work, targeted advertising practices rely on the vast collection and monetization of internet users' personal data, as this data enables advertisers to precisely select and segment audiences based on their interests, demographics, behavioral characteristics, personally identifiable information (PII), and more.[44] As targeted advertising

[37] Podcast: Attention, Shoppers–You're Being Tracked," *MIT Technology Review*, December 21, 2020, https://www.technologyreview.com/2020/12/21/1015409/podcast-attention-shoppers-youre-being-tracked/.
[38] "New In-Store Biometric Solutions Are Shaping the Future of Retail Services," *NEC Technical Journal* 13, no. 2 (2018): https://www.nec.com/en/global/techrep/journal/g18/n02/180210.html.
[39] Kim Hart, "Facial Recognition Surges in Retail Stores," Axios, last modified July 19, 2021, https://www.axios.com/facial-recognition-retail-surge-c13fff8d-72c6-400f-b680-6ae2679955d4.html.
[40] Stacy Cowley, "Banks and Retailers Are Tracking How You Type, Swipe and Tap," *New York Times*, August 13, 2018, https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html.
[41] Cowley, "Banks and Retailers".
[42] "Biometric Technology," NCR Global.
[43] Cowley, "Banks and Retailers".
[44] Spandana Singh, *Special Delivery: How Internet Platforms Use Artificial Intelligence to Target and Deliver Ads*, February 18, 2020, https://www.newamerica.org/oti/reports/special-delivery/

practices have become more ubiquitous, particularly on platforms such as Facebook and Google, it has resulted in a vicious cycle of personal data collection. This is because the more personal user data advertising companies and businesses are able to collect, the more "relevant" advertisements they are able to deliver.[45] The collection of consumers' sensitive biometric data, both online and offline, feeds into and spurs these surveillance capitalism-based advertising practices, encouraging companies to commodify users and their data and creating little incentives for such entities to reign in these invasive practices and offer consumers agency over their data.[46]

Despite the fact that the AI-based biometric technologies used to fuel marketing and advertising are highly invasive, the United States has very few safeguards in place to govern how such technologies are developed and deployed, and how biometric data is stored, used, and shared. Some U.S. states have taken action in this regard. For example, in California the California Consumer Privacy Act (CCPA) considers biometric information such as fingerprints and facial images to be protected personal data.[47] In addition, cities including Portland, Oregon have instituted bans on the use of facial recognition by government, police, and commercial enterprises including retail stores.[48] However, there are no safeguards at the federal level, enabling businesses to deploy biometric technologies at scale and collect vast amounts of sensitive user data to fuel already intrusive advertising practices.

Going forward, online and offline businesses will rely on biometric technologies more. Recent reporting suggests that some businesses are considering using technologies that can interpret facial expressions and emotional state, identify galvanic skin response (e.g. when someone is sweating), or monitor heart rates.[49] If entities are allowed to collect and use such personal data without safeguards, it will foster further privacy-intrusive practices, undermine consumer rights, and establish a significant power imbalance that leaves consumers with little agency.

Accountability and Mitigation Tactics:

As outlined, the use of AI-based biometric technologies poses significant risks to the rights and freedoms of individuals across the United States and around the world. In cases of some technologies, outright bans might be necessary, where we already know the tech is highly invasive, racially-biased, and antithetical to the First and Fourth amendments, such as facial recognition. In other instances, we believe developers and deployers of these technologies as

[45] Singh, *Special Delivery*.
[46] Bruce Sterling, "Twenty Years of Surveillance Marketing," *WIRED*, November 21, 2018, https://www.wired.com/beyond-the-beyond/2018/11/twenty-years-surveillance-marketing/.
[47] "California Consumer Privacy Act (CCPA)," State of California Department of Justice, https://oag.ca.gov/privacy/ccpa.
[48] Tim Becker, "City Council Approves Ordinances Banning Use of Face Recognition Technologies by City of Portland Bureaus and by Private Entities in Public Spaces," news release, September 9, 2020, https://www.portland.gov/smart-city-pdx/news/2020/9/9/city-council-approves-ordinances-banning-use-face-recognition.
[49] Cowley, "Banks and Retailers".

well as the U.S. government can institute numerous safeguards to ensure these tools are used responsibly and with restraint. In particular, we recommend:

1. All developers and deployers of AI-based biometric technologies engage in a robust and comprehensive set of assessments (e.g. algorithmic audits, impact assessments) to identify risks their technologies pose to individual's fundamental rights and society, understand appropriate use cases for their tools, and mitigate any identified risks and instances of bias.[50] These entities should conduct such assessments throughout the lifecycle of these tools, including during the design phase, pre-deployment, and post-deployment to account for any changes in how the tools operate.[51] In addition, entities creating and using AI-based biometric technologies should also use of other accountability tools, as appropriate, such as machine learning documentation practices and procurement mechanisms to promote greater fairness, accountability, and transparency (FAT) around these tools.[52] Lastly, entities should also provide meaningful transparency around the kinds of evaluations they have performed and their findings, as a mechanism for building trust and confidence in these tools.[53]

2. Entities responsible for developing AI-based biometric technologies should engage with and solicit feedback from a broad set of stakeholders before introducing any new products or features.[54] Such multi stakeholder engagements, including with users and civil rights and public policy experts can ensure entities develop tools that are reliable and non-invasive and policies that promote sufficient FAT.[55]

3. Where biometric information is collected, it must be subject to strict safeguards that go beyond typical data safety requirements. Comprehensive privacy legislation is needed at the federal level, and should address further requirements that apply to biometric information, which is some of the most sensitive personal data. The following principles should serve as a guide to policymakers:

    a. **Meaningful consent:** Companies must obtain meaningful consent to collect, process, and use biometric data.
    b. **Transparency:** Congress should require notices to be accessible to those with limited English proficiency and to be available in a machine-readable format.

[50] Spandana Singh and Leila Doty, *Cracking Open the Black Box: Promoting Fairness, Accountability, and Transparency Around High-Risk AI*, September 8, 2021, https://www.newamerica.org/oti/reports/cracking-open-the-black-box/recommendations/.
[51] Lauren Sarkesian and Spandana Singh, "OTI Comments on NIST Proposal for Identifying and Managing Bias within Artificial Intelligence," New America's Open Technology Institute, https://newamericadotorg.s3.amazonaws.com/documents/NIST_AI_Letter.pdf.
[52] Singh and Doty, *Cracking Open*.
[53] Singh and Doty, *Cracking Open*.
[54] Sarkesian and Singh, "OTI Comments," New America's Open Technology Institute.
[55] Singh and Doty, *Cracking Open*.

c. **Data Minimization**: Collection of personal biometric data should be limited to what is strictly necessary for the given purpose.
d. **Limited Retention Period**: The data collected must not be retained by companies or law enforcement authorities indefinitely. Legislation should define a retention period for personal data.
e. **Prohibition on Secondary Uses:** Personal data must be used for intended, consented to purposes only and legislation should prohibit secondary uses.
f. **Data Security:** Companies must maintain best security practices to safeguard the collected data. Such practices include decentralized implementation, de-identification methods like differential privacy, and encryption.
g. **Equity:** Companies must take steps to prevent disparate impacts on certain populations and demographics. Legislation should include a prohibition on discriminatory uses of data related to protected characteristics, including denial of access to education, housing, and employment opportunities.

4. Finally, there must be clear oversight and transparency practices that provide the public with notice of the use of these technologies, impacts, and opportunities for redress. There should be a process in place that also provides the public with the opportunity to provide input into whether, and how, such technologies are used. At the very least, democratic processes must be put in place surrounding the acquisition and use of surveillance technologies at a local level. Through the Community Control Over Police Surveillance (CCOPS) initiative (organized in 2016 by 18 organizations including OTI, and led by the ACLU), over twenty jurisdictions nationwide have passed ordinances that require transparency into what police technologies are in use, and allow opportunities for community input before deployment.[56]

Conclusion

Concerningly, a growing range of AI-based biometric surveillance tools are being deployed, often in secret and without public awareness or accountability, by law enforcement at the federal and local levels, as well as U.S. immigration authorities, and other government entities. Further, numerous private companies are now developing and using biometric technologies to fuel their marketing and advertising practices, in the absence of any federal commercial privacy law restricting or otherwise limiting these practices. At a minimum, safeguards to protect privacy and generate fairness, accountability, equity, and transparency must be put in place to protect the public from invasive biometric technologies.

[56] American Civil Liberties Union, Community Control Over Police Surveillance https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

New York Civil Liberties Union

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

BY ELECTRONIC MAIL to BiometricRFI@ostp.eop.gov

Suresh Venkatasubramanian
Assistant Director
Office of Science and Technology Policy
White House
1600 Pennsylvania Ave NW
Washington, DC 20500

January 14, 2022

RE: Request for Information Response: Biometric Technologies

Dear Assistant Director Venkatasubramanian:

The New York Civil Liberties Union ("NYCLU") submits these comments in response to the White House Office of Science and Technology Policy's ("OSTP") Request for Information regarding Biometric Technologies (document number 2021-21975) dated October 8, 2021.

The NYCLU, the New York State affiliate of the American Civil Liberties Union, is a nonprofit, nonpartisan organization with eight regional offices and more than 200,000 members and supporters across the state. The NYCLU's mission is to defend and promote the fundamental principles, rights and values embodied in the Bill of Rights of the U.S. Constitution and the Constitution of the State of New York.

We work to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil rights and liberties are enhanced rather than compromised by technological innovation. We have a long history of vigorously defending students' rights, including access to education and privacy rights, as well as protecting New Yorkers from abusive policing, including through challenging invasive and discriminatory surveillance practices. Bringing together these areas of expertise, we are the leading organization advocating for a ban on the use of biometric surveillance against public school students and have advocated against the use of biometric surveillance by New York law enforcement and other government agencies.

Biometric surveillance technologies, which include face, voice, and gait recognition, give unprecedented power to track who we are, where we go, and who we meet, enabling an invasion of privacy that reaches far beyond traditional surveillance techniques. They are highly flawed and racially biased. The use of these technologies by government agencies presents a clear danger to our civil rights and liberties and threatens to erode our fundamental rights to privacy, free speech, and equal treatment under the law. It is urgently imperative that the federal government act to stop the proliferation of biometric surveillance and ban its use.

1. The Lockport City School District's Deployment of Facial Recognition Technology

In spring 2018, the NYCLU was notified by concerned community members that the Lockport City School District ("Lockport" or the "District") purchased facial recognition technology to use in its schools, using funding from New York's Smart Schools Bond Act ("SSBA"). The SSBA, approved by voters in 2014, authorized $2 billion in general obligation bonds for schools to upgrade their infrastructure and technology to "improve learning and opportunity for students throughout" New York.[1] Many schools used these funds to improve wireless internet connectivity or purchase computers, tablets, and 3D printers for use in the classroom.

NYCLU
ACLU of New York

Lockport, however, spent almost all the $4 million it was awarded for "new cameras and wiring…to provide viewing and automated facial and object recognition of live and recorded surveillance video," as well as "additional surveillance servers…to provide enhanced storage of recorded video and processing."[2] The decision to implement this technology appears to have been made without sufficient public involvement as required by state law, and involved a security consultant who may have had a conflict of interest.[3]

Over the course of the next 18 months, the NYCLU repeatedly contacted the New York State Education Department ("NYSED") with concerns over issues of accuracy, bias, privacy, transparency, and data security with Lockport's system. At the NYCLU's urging, NYSED engaged with the District and required it to undertake a privacy assessment, reviewed Lockport's draft privacy policies, and prohibited Lockport from testing its face recognition system multiple times.[4]

On November 27, 2019, however, NYSED issued a determination letter granting Lockport permission to utilize its biometric surveillance system, despite unanswered questions about the system's functionality and the risks of this technology. On January 2, 2020, Lockport deployed its facial recognition system in schools, impacting more than

[1] Smart Schools Bond Act (2014), http://www.p12.nysed.gov/mgtserv/smart_schools/home.html; *see also* Smart Schools Bond Act Implementation Guidance, http://www.p12.nysed.gov/mgtserv/documents/SSBAGuidancerev_6_1_18_Final.pdf.
[2] Lockport City School District, Smart Schools Investment Plan (2016-2017), http://p1232.nysed.gov/mgtserv/documents/LOCKPORTCITYSD.pdf (last modified October 23, 2017) (emphasis added) ("Lockport SSBA Plan").
[3] Lockport City School District, August 17, 2016 Proceedings of the Board of Education, https://www.nyclu.org/sites/default/files/field_documents/lockport_board_meeting.pdf. Despite the lack of comment at the hearing, the District certified on its application that it had engaged all four categories of stakeholders – parents, teachers, students, and community members. *See* Lockport SSBA Plan, at 1. In addition, the president of the Lockport Education Association stated that teachers were not consulted in a discussion of how to use the funding, as was required. *See* Tim Fenster, *Trying for More Secure Schools: Lockport district turning to facial recognition software*, Lockport Union-Sun & Journal, Mar. 4, 2018, http://www.lockportjournal.com/news/local_news/trying-for-more-secure-schools-lockport-district-turning-to-facial/article_f1cc9cfa-0898-5da0-ac5d-d600df21bed7.html.
[4] *Shultz v. NYSED*, Index No. 904134-20, Docket Entry 73, Amended Petition, New York Supreme Court, Albany County 2020; *see also* Davey Alba, *The First Public Schools in the US Will Start Using Facial Recognition Next Week*, May 30, 2019, Buzzfeed News, https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis.

4,000 students.[5] This was short lived as the COVID-19 pandemic forced Lockport to close schools in March 2020.

In June 2020, the NYCLU, on behalf of four parents, sued NYSED over its approval of Lockport's system, alleging that the agency's decision violated state privacy laws intended to protect student data.[6] Shortly thereafter, the New York State Legislature passed A6787/S5140, the first statewide bill in the country prohibiting the use of biometric identifying technology in schools.[7] The bill was signed in December 2020, enacting section §106-b of the New York State Technology Law, which prohibits the purchase or use of biometric identifying technology[8] in all public and nonpublic elementary and secondary schools until the Department of Information Technology, in partnership with NYSED, issues a report on the risks and benefits of this technology in schools. The moratorium is in effect until July 2022 or until the Commissioner of Education authorizes the use of biometric identifying technology following the report – whichever comes later.[9] This law was a direct response to Lockport's purchase and concerns over the racial disparities in identification of people of color, risks of data breaches, and access to the highly sensitive data produced by the system.

NYCLU
ACLU of New York

Currently, the moratorium remains in place and Lockport's system remains deactivated. It does not appear that the Department of Information Technology or NYSED has initiated the study required by the law. Additionally, the state committee tasked with reviewing school district funding proposals, the Smart Schools Review Board (the "Review Board"), has approved multiple school districts' grant applications that include biometric identifying technology. We believe this is due to an ignorance of the law, misunderstanding of the technology, and relentless pressure on school districts by for-profit entities attempting to sell these products.

On February 24, 2021, it was reported that the Smart Schools Review Board approved $21.2 million of SSBA funds for "high tech security" projects,[10] including seven school district plans for surveillance technologies which include facial recognition capabilities or other "self-learning analytics."[11] On August 12, 2021, the Review Board approved another school district proposal explicitly including "self-learning video

[5] *January 2020 AEGIS Security System Update*, https://www.smore.com/utzgy.
[6] *Shultz et al v. New York State Education Department*, https://www.nyclu.org/en/cases/shultz-et-al-v-new-york-state-education-department.
[7] A6787 (Wallace)/S5140 (Kavanagh), https://www.nysenate.gov/legislation/bills/2019/a6787.
[8] Biometric identifying technology is "any tool" that uses "an automated or semi-automated process that assists in verifying a person's identity based on a person's biometric information." N.Y. Tech Law §106-b(1)(a).
[9] N.Y. Tech Law §§106-b(2)(a), (3)(a).
[10] *Governor Cuomo Announces $59.9 Million For School Technology Upgrades Through the Smart Schools Bond Act*, February 24, 2021, https://www.wnypapers.com/news/article/current/2021/02/24/145481/59.9-million-for-school-technology-upgrades-through-smart-schools-bond-act.
[11] *See, e.g.*, Otselic Valley Central School District (requesting funding for, among other things, a license for Avigilon ACC7 software which explicitly includes "facial recognition technology") http://p1232.nysed.gov/mgtserv/documents/Georgetown-SouthOtselicCSD-Application1.pdf; *see also*, proposals from Binghamton, Canaseraga, Carmel, East Syracuse Minoa, Stillwater, and Sullivan West.

analytics" and biometric identifying capabilities.[12] These projects include camera, software, and analytics products from a vendor called Avigilon, including systems known as Avigilon Control Center ("ACC") 6 and 7.[13] ACC 7 explicitly includes "facial recognition technology" to "identify[] people of interest based on secure watch list(s)."[14] ACC 6 includes an "Appearance Search" feature which is described as "a sophisticated deep learning AI search engine for video" that uses "face analytics" including "the unique characteristics of a person's face… to understand that it is searching for the same person, even if items such as their clothing change over time."[15,16] Fulfillment of these proposals is a clear violation of New York law.[17]

1.1 Implications of Facial Recognition Technology in School Settings

Lockport is one of the first public school districts in the country to implement biometric identifying technology in a school setting[18] and, after wasting years of taxpayer money and human capital on a system it cannot use, it should be a cautionary tale for other districts intent on using similar technologies. The use of facial recognition and other biometric surveillance technologies in schools presents a number of potential harms to students and we urge OSTP to consider these carefully in its review of biometric surveillance.

First, there are well-documented issues with the accuracy and bias of facial recognition technology, particularly when used to identify women and people of color.[19]

[12] Brighton Central School District (requesting funding for a license for Avigilon ACC6 software and "self-learning video analytics."), http://p1232.nysed.gov/mgtserv/documents/BrightonCSDCouncilRock.pdf.
[13] Avigilon Control Center 6 (ACC 6) software "combines an intuitive interface with advanced search functions called Avigilon Appearance Search." Appearance Search technology "is a sophisticated AI search engine for video data that incorporates the characteristics of a person's face." Avigilon describes their ACC 6 software as "self-learning video analytics." Avigilon Control Center 7 (ACC 7) incorporates "AI-powered facial recognition technology to detect people of interest based on one or more secure watch lists" and has "next-generation analytics and self-learning video analytics," https://www.avigilon.com/support/software/acc7/avigilon-acc7-datasheet-en.pdf.
[14] *See Avigilon Control Center 7 Software*, https://www.avigilon.com/products/acc/7.
[15] https://www.avigilon.com/products/ai-video-analytics/appearance-search.
[16] It also appears that ACC 6 will be discontinued so these Districts may need to update to ACC 7 which explicitly includes facial recognition technology, https://assets.avigilon.com/file_library/pdf/acc6/ACC_6_EOL_Notice.pdf.
[17] In addition to biometric identifying technology, the NYCLU is also concerned about the use of online surveillance systems for school-issued devices. As you may know, GoGuardian and other similar products purport to monitor all online student activity "under the guise of student safety" yet these products raise concerns regarding student and family privacy and racial bias inherent in such surveillance programs. *See* letter from Senators Elizabeth Warren, Edward J. Markey, and Richard Blumenthal, Sept. 29, 2021, https://www.warren.senate.gov/imo/media/doc/2021.09.29%20Shinde%20-%20EdTech%20letter.pdf.
[18] Davey Alba, *Facial Recognition Moves Into a New Front: Schools*, THE NEW YORK TIMES, Feb. 6, 2020, https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html.
[19] *See, e.g.,* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face recognition vendor test part 3: demographic effects* NIST IR 8280 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; and Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven*

As with any artificial intelligence, biometric surveillance carries the biases of the people who design it and the information used to train it. In the system purchased by Lockport, for example, Black women are 16 times more likely to be misidentified than white men.[20]

In all facial recognition systems, the databases to which the images are paired can be unreliable—they are not required to be vetted for quality and they are not created with any requirement of due process—and because they are provided by law enforcement, often disproportionately include young men of color.[21] This creates an unfair and undue risk of false identification for students of color, who are already more likely to be unfairly targeted by the criminal justice and school discipline systems, fueling the school-to-prison pipeline.

Second, these systems infringe on the privacy rights of students, parents, and staff. Student images are a protected part of a student's biometric record, included in the definition of "personally identifiable information" under the Family Educational Rights and Privacy Act and New York's student data privacy law, Education Law §2-d.[22] Once an individual's photo is uploaded to a school facial recognition system, the system will track that person's movements around the school and with whom they interacted. These systems can turn students' and staff members' every step into evidence of an infraction or crime, can trace a student's use of sensitive services such as the nurse's or counselor's office, and can be used to criminalize ordinary child behavior and personal interactions, potentially violating the First Amendment right to association. These systems can even be used with immigration enforcement databases, meaning students could be targeted by immigration authorities simply for coming to school—putting themselves and their families at risk of deportation.

Third, the use of this technology raises concerns about data maintenance and retention. For example, how long the associated data will be retained, how securely it will be stored, who will pay for the upkeep of additional data storage, who will have access to it and how it may be shared, including any connection to law enforcement databases. While there is good reason to maintain most education records for the student's entire school career, surveillance records should be retained for the shortest possible time.

Fourth, these systems, like all databases, are vulnerable to hacking.[23] But unlike passwords or credit card numbers, a person's biometric information is highly sensitive and

Commercial Systems, 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE 32–41 (2019).

[20] *Shultz v. NYSED*, Index No. 904134-20, New York Supreme Court, Albany County, Schwarz Aff. Ex. 12, https://www.nyclu.org/sites/default/files/field_documents/schwarz_affidavit.pdf.

[21] Sidney Fussell, *School Districts can Hardly Wait to Start Tracking Kids with Police State-Style Face Recognition*, Gizmodo, May 21, 2018, https://gizmodo.com/school-districts-can-hardly-wait-to-start-tracking-kids-1826197713.

[22] "Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting." 34 C.F.R. § 99.3.

[23] In February 2018, CCTV systems were hacked at four schools in the UK and aired online in real time. ACLU of Arkansas Warns Schools of Privacy Risks of Biometric Surveillance Systems, Mar. 16, 2018, https://www.acluarkansas.org/en/press-releases/aclu-arkansas-warns-schools-privacy-risks-biometric-surveillance-systems.

cannot be changed if there is a security breach. Storing massive amounts of this data collected from children, parents, and school employees raises the risk that personally identifiable information may be hacked, stolen, or sold.[24]

Fifth, these systems can cost millions of dollars, taking vital funding away from instruction. "Ed Tech," including school surveillance, has become a lucrative industry for private vendors and security consultants who see the deep pockets of public funding and may take advantage of schools' well-intended efforts to protect students.

Sixth, these systems negatively impact school climate. Students should feel welcomed and supported in schools—not made to feel like suspects who must be surveilled throughout the school building.

Finally, these systems, particularly Lockport's, have been implemented without full transparency and input from critical stakeholders. Private vendors are incentivized to conceal system information to protect proprietary interests. Students, families, teachers, and other community members must be consulted as to whether the use of biometric identifying technology should be used in a school and should be engaged in a frank discussion of the potential harms and benefits.

1.2 Recommendations Concerning Biometric Technologies in School Settings

Lockport's use of facial recognition technology highlights the immediate need for protections at the federal level. There is currently no federal guidance or restrictions on the use of facial recognition and other biometric surveillance technologies in schools. As highlighted above, these systems pose real risks to students and are inappropriate for use in an educational context. The OSTP should work with the United States Department of Education to issue guidance advising schools that facial recognition and other biometric identifying technologies should not be utilized in school settings and that no federal education funding should be utilized for purchasing such systems. Above all, the OSTP should emphasize that schools and districts have an obligation to protect student privacy and ensure that schools are welcoming places for all children to learn and thrive, not for them to be surveilled.

2. Biometric Surveillance by Law Enforcement

In the absence of federal- or state-mandated guidelines or restrictions on the acquisition and use of biometric surveillance technologies, law enforcement agencies throughout New York have been free to set their own rules. Because these departments so frequently attempt to evade public demands for greater transparency and oversight, the full reach of the surveillance state is unknown. What we do know, however, is that the biometric surveillance systems currently being used by law enforcement agencies make countless people, particularly people of color, less safe. As mentioned above, facial recognition technology is notoriously inaccurate, failing to correctly match faces to a

[24] Matthew Gault, *DHS Admits Facial Recognition Photos Were Hacked, Released on Dark Web*, Vice, Sept. 24, 2020, https://www.vice.com/en/article/m7jzbb/dhs-admits-facial-recognition-photos-were-hacked-released-on-dark-web.

comparison database, especially when it comes to identifying women and people of color.[25] When these systems are used by law enforcement, the risks of misidentification cannot be overstated, especially considering the potential for lifelong consequences that can result from even a single encounter with law enforcement.[26]

Even if the accuracy of the technologies were to improve, biometric surveillance systems would continue to operate with built-in bias. This is because the databases that the technologies rely on for comparators are, themselves, typically generated by law enforcement. For example, facial recognition systems may depend on mugshot databases, which—reflecting the disproportionate rate at which communities of color are policed—have many more faces of people of color in them. The biased policing practices that continue to disproportionately target and criminalize people of color[27] will mean that these technologies will end up being used disproportionately against people of color.

While the risks of misidentification are obvious, the potential for these technologies to produce accurate identifications should also raise serious concerns in the law enforcement context. The widespread deployment of biometric surveillance systems – especially when coupled with existing surveillance infrastructures – would give law enforcement the ability to easily identify and track a person's every movement: where they go to school, which doctors they visit, which places of worship they attend, and which protests and demonstrations they decide to attend. The New York Police Department ("NYPD" or the "Department") already has more than 20,000 cameras integrated into its Domain Awareness System[28] and plans to increase that number to a staggering 50,000 cameras.[29] And the Department continues to introduce even more cameras in the form of officer body-worn cameras and unmanned drones. It also makes use of social media photographs; in August of 2020, the NYPD used facial recognition software to identify a Black Lives Matter activist during a protest against police brutality through a photo from his Instagram account.[30]

Given the NYPD's long and troubling history of engaging in surveillance tactics that have targeted political dissent, criminalized communities of color, and singled out Muslim New Yorkers for suspicionless surveillance solely on the basis of their religion,

[25] *Supra,* note 19.
[26] *See, e.g.,* Kashmir Hill, *Wrongfully Accused by an Algorithm*, THE NEW YORK TIMES, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, THE NEW YORK TIMES, Dec. 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
[27] *See, e.g.*, Annual Stop-and-Frisk Numbers, NYCLU, https://www.nyclu.org/en/stop-and-frisk-data (demonstrating that police stop, detain, frisk, and arrest Black and brown people at disproportionate rates).
[28] A Conversation with Jessica Tisch '08, HARVARD LAW TODAY (2019), https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/.
[29] Preparedness Grant Effectiveness Case Study: New York City, 27 (2021), https://www.fema.gov/sites/default/files/documents/fema_nyc-case-study_2019.pdf.
[30] George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, GOTHAMIST, Aug. 14, 2020, https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

the dangers that hypothetically accurate biometric surveillance technologies would pose to our most fundamental rights and liberties would be no less concerning.[31]

Through litigation, the public has learned of the highly flawed, unscientific, and even unlawful practices that pervade the NYPD's facial recognition program since its inception over ten years ago. A 2019 report from the Georgetown Law Center on Privacy and Technology revealed that the NYPD engaged in such dubious tactics as uploading photographs of celebrity lookalikes in lieu of actual suspect photos, editing suspect photographs (including through effects that substantially alter the suspect's actual appearance) in order to generate a potential match, and apprehending suspects "almost entirely on the basis of face recognition 'possible matches'" without taking additional investigative steps to establish probable cause.[32]

NYCLU
ACLU of New York

Investigative reporters have uncovered even more failures by the NYPD to safeguard sensitive information and ensure officer adherence to even minimal standards on the use of biometric surveillance systems. It was revealed that the NYPD was including mugshots of juveniles and other sealed arrest records in its facial recognition database.[33] And despite the NYPD's explicit rejection, citing concerns about security and the potential for abuse, of software developed by Clearview AI that scrapes billions of photographs from social media platforms and other public sources, it has been reported that dozens of "rogue" officers have continued to use the software in more than 11,000 searches.[34] The reporting noted that "[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,"[35] raising doubts about the willingness of the Department to enforce even its own rules and raising concerns about their ability to safeguard sensitive biometric information going forward. The NYPD is far from the only agency deserving of closer scrutiny; at least 61 law enforcement agencies across New York State (*see figure 1*) have secretly used Clearview AI's software, which includes biometric data on virtually everyone who has ever uploaded photos to Facebook, Instagram, Twitter, Venmo, or other social media platforms.[36]

[31] A few examples of the many cases the NYCLU has litigated involving NYPD surveillance abuses include *Handschu v. Special Services Division* (challenging surveillance of political activists), *Raza v. City of New York* (challenging the NYPD's Muslim Surveillance Program), and *Millions March NYC v. NYPD* (challenging the NYPD's refusal to respond to a Freedom of Information Law request seeking information about whether the NYPD is using invasive technology to infringe on the protest rights of Black Lives Matter advocates).

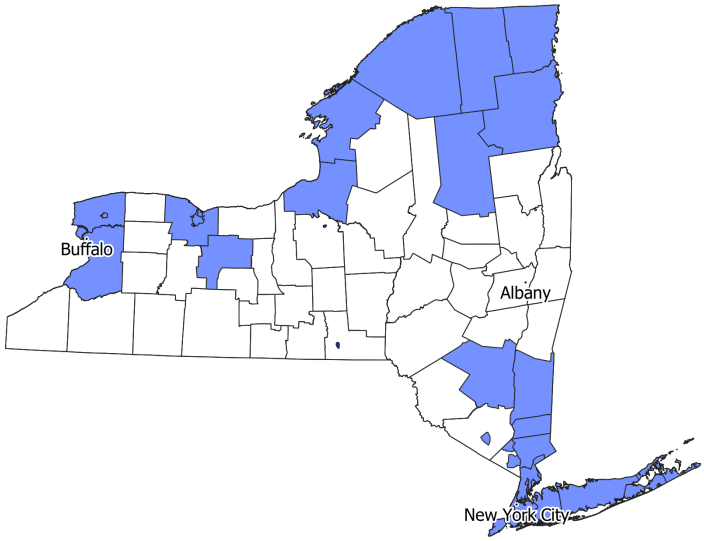
[32] Clare Garvie, Georgetown Law Center on Privacy & Technology, Garbage In, Garbage Out: Face Recognition on Flawed Data, (2019), https://www.flawedfacedata.com/.

[33] Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, THE NEW YORK TIMES, Aug. 1, 2019, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[34] *See, e.g.,* Craig McCarthy, *Rogue NYPD Cops are Using Facial Recognition App Clearview*, N.Y. POST, Jan. 23, 2020, https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/; Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, Feb. 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[35] *Id.*

[36] *See, e.g.,* Ryan Mac et al., *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, BuzzFeed News, April 6, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition; and Kashmir



NYCLU
ACLU of New York

Fig 1: New York law enforcement agencies that have used Clearview AI.

The widespread availability of biometric technologies has led to deployments across agencies and industries, which law enforcement has attempted to exploit. In one particularly alarming example, the Metropolitan Transportation Authority and the NYPD partnered with IBM to develop software to search for people by their skin color in the transit system.[37] And Amazon Ring has partnered with hundreds of law enforcement agencies, including on Long Island, to facilitate data sharing from privately installed devices to the police.[38] Some of these systems offer or plan to offer other forms of biometric recognition such as affect recognition and aggressive or suspicious behavior detection, whose outcomes are severely inaccurate and plagued by disparate impacts for Black people.[39]

Correctional facilities have also become a testing ground for biometric surveillance technologies. The New York Department of Corrections and Community Supervision

Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[37] George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color*, THE INTERCEPT, Sept. 6, 2018, https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

[38] Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns*, WASHINGTON POST, Aug. 28, 2019, https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach; Catherine Thorbecke, *Long Island Police Partner with Amazon's Ring to Crack Down on Porch Pirates*, ABC NEWS, Dec. 4, 2019, https://abcnews.go.com/Technology/long-island-police-crack-porch-pirates-amazon-ring/story?id=67489715.

[39] *See* Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements:*, PSYCHOLOGICAL SCIENCE IN THE PUBLIC INTEREST (2019), https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full; LAUREN RHUE, *Racial Influence on Automated Perceptions of Emotions* (2018), https://doi.org/10.2139/ssrn.3281765.

("DOCCS") uses facial recognition for "visitation processing," deploying it to deny visitation to family members, friends, and other loved ones who wish to visit people in DOCCS's custody.[40] DOCCS has not released any information about its utilization of facial recognition for "visitation processing," and its use has not been subject to any public oversight. Additionally, DOCCS deploys a telephone system with voice recognition technology to collect and analyze voiceprints of not only the person who is incarcerated, but other parties on the call. The vendor offers investigative support, identification capabilities, call monitoring, behavioral analysis, suspicious keyword notification, pattern analysis, and even location tracking of the called party. Yet voice recognition tools have similar racial bias as other biometric technologies; studies have shown error rates for Black speakers are twice as high compared to white speakers.[41] In March 2021, it was revealed that a vendor recorded confidential attorney-client calls and provided them to New York City district attorneys.[42] A recent audit disclosed that nearly 2,300 calls to attorneys were recorded.[43]

NYCLU
ACLU of New York

Law enforcement use of biometric surveillance technologies will only continue to expand absent federal oversight. The OSTP should work with the United States Department of Justice to issue clear guidance advising law enforcement agencies against the continued use of biometric surveillance technologies given the grave risks that they pose to privacy, civil liberties, and racial justice.

3. Conclusion

The ever-expanding deployments of biometric surveillance and the immense risks associated underscore the immediate need for a ban on biometric surveillance by government, in particular in schools, by law enforcement, and in other areas where our fundamental rights are at stake.

Sincerely,

[redacted]

Stefanie D. Coyle
Deputy Director
Education Policy Center

[redacted]

Daniel Schwarz
Privacy & Technology Strategist
Policy Department

[40] Beth Haroules & Lisa LaPlace, *NYCLU v. DOCCS*, New York Civil Liberties Union (2021), https://www.nyclu.org/en/cases/nyclu-v-doccs.
[41] *See e.g.*, *Voicing Erasure*, ALGORITHMIC JUSTICE LEAGUE (2020), https://www.ajl.org/voicing-erasure; Allison Koenecke et al., *Racial disparities in automated speech recognition*, 117 PNAS 7684–7689 (2020).
[42] Chelsia Rose Marcius, *NYC's 5 DA offices wound up with recordings of confidential jailhouse calls between inmates and lawyers*, NYDAILYNEWS.COM, (2021) https://www.nydailynews.com/new-york/ny-jails-recordings-attorney-client-privilege-calls-20210321-tzbyxwnle5dc5jgvi5cona6wry-story.html.
[43] Noah Goldberg & John Annese, *NYC Correction contractor recorded thousands more lawyer-client jail phone calls than first reported; could jeopardize court cases*, NYDAILYNEWS.COM, (2021), https://www.nydailynews.com/new-york/nyc-crime/ny-audit-shows-doc-listened-in-on-even-more-lawyer-inmate-calls-20211230-zni5qacdhjaozok7rdmwyg2wsm-story.html.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

No Name Provided

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] < RFI Response: Biometric Technologies >
Date: Saturday, January 15, 2022 11:02:04 AM

This comment regards the past and present use, and misuse, of facial recognition technology by Customs and Border Protection (CBP), and the impact and harm of such misuse on members of the public. This comment is submitted by a member of the public and addresses topic numbers 1, 3, 4, and 6.

Background information on CBP's use of facial recognition is widely available. The agency directs members of the public passing through its checkpoints to have pictures of their faces taken by automated kiosks, or by cameras mounted to the booths at which their agents interact with members of the public.

The agency consistently represents, in posted signage and in sworn testimony to Congress (for example, to the Committee on Homeland Security on July 10, 2019 >https://www.youtube.com/watch?v=JFnGJjva8aU<), that for US citizens participation in these facial recognition programs is voluntary. Yet repeated experience across several airports and several years time shows that individuals declining to take part are harassed, intimidated, subject to selective profiling, or even told that they have no choice.

I travel extensively both for business and for personal reasons, thus I frequently pass through CBP checkpoints. I consistently decline to have my picture taken. My reasons for doing so are several fold.

I do not trust any assurances regarding retention or non retention of photographs taken. Numerous historical examples (e.g. the illegal use of census data for Japanese internment during the second world war) demonstrate the general fact that assurances from government agencies regarding the retention and use of data cannot be relied upon.

I do not trust that such photographs will not fall into the hands of third parties. Countless mass data breaches, including several stunning losses by government agencies of their most closely guarded secrets (for example, loss by the Office of Personnel Management (OPM) of more than 22 million records about government employees and job applicants, including highly sensitive information about holders of security clearances, and the loss by the National Security Agency (NSA) of possibly their entire arsenal of computer exploits to a group known as the Shadow Brokers) demonstrate that no institution inside or outside of government is currently capable of adequately securing its data.

I value the privacy of images of my face inherently. I am most especially concerned about possible future use of these photographs, whether retained by CBP or by a third party, to aid in facial recognition identifying myself in large databases of photos such as those available online, or in feeds from surveillance cameras, thus compromising the privacy of my movements and other important privacies of life.

I submit these reasons for the benefit of OSTP, however I should not need to explain these reasons to CBP. If they intend to maintain, including in sworn testimony to Congress, that participation in their facial recognition programs is "voluntary", then an individual choosing not to participate should not be interrogated regarding his reasons for making that choice. Yet this has been my lived experience.

I have encountered the booth mounted cameras three times, once in ATL in 2019, and twice in IAH in 2021. All three times the CBP agent repeatedly and aggressively questioned my reasons for declining to have my picture taken and impugned this choice.

The most recent time, the agent stated explicitly that I would be sent to "secondary" if I made this choice. When I politely indicated that my decision was to opt out of having my photo taken, the agent followed through with this threat. I was detained for approximately one hour and a half (making me late for my connecting flight), my bags were searched, and I was subjected to further and lengthy interrogation, including as to my reasons for not wanting my picture taken. As the first agent made quite explicit, none of this would have happened had I relented and allowed my photo to be taken.

In addition to the booth mounted cameras, I have encountered the kiosks dozens of times. In nearly every case, travelers were being directed to use the kiosks with no indication given that there existed an option not to use them, other than in fine print on a notice on the screen of the kiosks themselves. In each case, I would indicate that I choose not to use the kiosks.

In about half of these instances, I was told that use of the kiosks were mandatory. In such cases, I pointed out that a notice presented on the screen of the kiosks explicitly states that their use is voluntary.

In some cases the person directing me to the kiosk and informing me that their use is mandatory would read the statement from the screen or consult a supervisor or coworker before allowing me to proceed. In several cases I was detained for several minutes as a result of choosing not to use the kiosk, and in several cases I was subjected to an aggressive and sometimes lengthy interrogation regarding my reason for declining to use the kiosk.

This experience highlights an obvious best practice procedure relating to the use of facial recognition technology, which has not been and is not being adhered to by CBP: where participation in a facial recognition program is supposed to be voluntary, individuals choosing not to participate should not be harassed, intimidated, subject to selective profiling, punished, or told that participation is mandatory.

Claims from parties using facial recognition technology that participation in such use is voluntary should be closely scrutinized. Statistics regarding number of people choosing to opt-out should be viewed skeptically and with an eye to the possibility that many people do not know that they have this option, and that many other people may realize or suspect that they will be harassed or intimidated if they choose to exercise such option.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Notre Dame Technology Ethics Center

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 4, 2022

To: Office of Science and Technology Policy
Executive Office of the President

Via electronic mail

From: Elizabeth M. Renieris, *Professor of the Practice, Director of Policy, Notre Dame Technology Ethics Center* and Yong Suk Lee, *Assistant Professor of Technology, Economy and Global Affairs, Faculty Affiliate, Notre Dame Technology Ethics Center*[*]

Re: *RFI Response: Biometric Technologies*

We are colleagues at the University of Notre Dame's Technology Ethics Center, which develops and supports multi- and interdisciplinary research on questions related to the impact of technology on humanity. We are writing in response to the White House Office of Science and Technology Policy's request for information on "Public and Private Sector Uses of Biometric Technologies" as part of its broader efforts to develop a Bill of Rights for an Automated Society. In summary, the already widespread and rapidly proliferating use of biometric technologies across the public and private sectors raises a wide array of ethical concerns and challenges. As such, we are encouraged by the OSTP's efforts to consider policies that can equitably harness the benefits of these technologies while providing effective and iterative safeguards against their anticipated abuses and harms.

Our response is focused on use cases (topic 1) and harms (topic 4), as set out below:

1. Descriptions of use of biometric information for recognition and inference: Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

UNITED STATES

- *Biometric IDV*
  One of the most common uses of biometric technologies at present is in the context of digital identity and access management (IAM), including for identity verification

[*] We would also like to acknowledge Benjamin Larsen, a PhD Fellow at the Copenhagen Business School and The Chinese Academy of Sciences (CAS) in Beijing, for his significant research contributions on use cases.

(IDV) and authentication. Verification is typically a one-time process used to onboard a customer or create an account for an individual by linking a unique individual to an identity document or other identity information. Authentication is typically a recurring process by which to determine that a previously verified individual is who they say they are on the basis of one or more factors of authentication. Low assurance environments (e.g., social media accounts) may require simple login credentials such as a username and password, while higher assurance ones (e.g., a benefits portal) may require two or more factors such as login credentials and a code sent to a verified phone number associated with the account. Even higher assurance environments (e.g., bank accounts) increasingly require physical biometrics, such as fingerprints, faceprints, voiceprints, iris or retina scans, and behavioral biometrics, such as keystroke dynamics, eye-tracking, and gait recognition, among other modalities.

Emerging technologies such as artificial intelligence (AI) and machine learning are increasingly used to process biometrics for IAM purposes. For example, remote, AI-powered IDV through the use of biometric facial verification allows individuals to prove their identity by providing an image of an identity document (e.g., a driver's license) and a live picture or video of their face. Machine learning models are then used to determine the likelihood that the document is authentic by extracting data from it and attempting to detect any manipulations. If the document is deemed authentic, the model is used to perform a biometric-based facial similarity check to determine whether the image on the document matches the face in the selfie or live video of the individual presenting it. If the faces match, the person passes the IDV check.

Beyond AI-powered IDV, here are other examples of private sector use cases in the U.S.:

- *Contactless Payments/Checkout*
  Biometrics are increasingly embedded into "contactless" payment and checkout solutions. For example, restaurants are beginning to use facial recognition technologies (FRT) for contactless drive-thru orders and payments through companies such as PopPay. While there has been significant emphasis on the use of FRT, a wide array of other physical and behavioral biometrics is also increasingly being used by the private sector for payments. For example, Amazon One uses vein scanning technology to turn an individual's palm into a physical biometric that can be used for contactless checkout in its Amazon Go grocery stores. Payment providers like Mastercard and Visa are also beginning to embed vein scanning and fingerprint recognition technologies into their payment solutions. Proponents argue these biometric-enabled tools make these processes more efficient, convenient, and secure, and uptake has been boosted in part by pandemic-induced germaphobia.

- *Exam Proctoring/Remote Learning*
  As many educational activities have shifted online during the pandemic, there has been a considerable increase in the use of remote learning software and remote proctoring tools to administer exams. Companies like Proctorio, ProctorU, and Honorlock purport to use a variety of behavioral biometrics, such as gaze-detection and eye-monitoring, face-detection and head movement tracking, and mouse clicks and scrolling patterns, among other behaviors, to detect cheating or other abnormalities during exams. These tools presume there are "normal" behaviors or patterns and that deviations or "abnormal" movements indicate cheating or fraud.

- *Security/Loss Prevention*
  The use of FRT among U.S. retailers for purposes of security, theft or loss prevention is already a widespread practice and includes household names such as Apple, Lowe's, and Macy's, among others. Going beyond facial recognition technologies, retailers are increasingly adopting invasive biometric methods and modalities, many of which were initially developed by the Pentagon, that purport to use things like heart rate (or "cardiatric signature"), body odor and other chemical indicators, gait analysis, and more to predict theft or other criminal activity in stores.

- *Employee Monitoring/Tracking*
  Employers are increasingly using AI-powered biometric systems to monitor, track, and nudge employees into certain activities or behaviors. For example, Amazon delivery drivers have to sign "biometric consent" forms to allow biometric sensors to collect facial images and other biometric information in the name of driver "safety." Wearables and biometric-enabled sensors are increasingly being considered to monitor and surveil employees for social distancing and other pandemic-related protocols.

Biometrics are also increasingly part of public sector use cases, such as the following:

- *Policing/Law Enforcement*
  Police and law enforcement agencies frequently use a variety of facial recognition software tools in their efforts to identify both suspects and victims, otherwise solve crimes, and, increasingly, to police certain neighborhoods. Some uses are less targeted and involve more pervasive surveillance and monitoring of specific communities (typically lower income and minority communities). Often, these tools are provided by private sector firms, such as the controversial Clearview AI whose database allegedly contains nearly 3 billion facial images.

- *Education/Schools*

In addition to remote learning tools, public schools and universities are increasingly adopting technologies that incorporate an array of physical and behavioral biometrics for various purposes on school premises. For example, during the pandemic a number of schools and universities began using fingerprint readers for contactless ordering and payments in dining halls and cafeterias. Facial recognition systems and behavioral biometric-based systems are also being explored for school safety and security purposes, including, in some cases, to replace metal detectors.

- *Security/Access Control*
  Public sector entities were early adopters of the use of fingerprints and other physical biometrics for purposes of security and access control. In part due to the pandemic, DHS and the TSA are increasing their investment in facial recognition systems, including iris scanners and other biometric-enabled technologies to automate a variety of processes in airports and other travel hubs, from security and passenger screening to check-in, health checks and other COVID-19 related protocols. Here, it is important to reiterate the public sector's increasing dependence on private sector provided tools. For example, DHS has moved its biometrics database to Amazon's cloud service.

CHINA

While the use of biometric technologies in the United States is widespread and rapidly accelerating, in large part due to the COVID-19 pandemic, these technologies are also ubiquitous in other countries, where certain use cases may foreshadow what is to come. For example, China has been aggressively using biometric technologies for purposes of convenience, safety, and surveillance in both public and private sector contexts. New wearable devices such as "smart" helmets, "smart" bands, and "smart" uniforms are increasingly being used by organizations in an attempt to detect individuals' movements and whereabouts, as well as changes in their emotional states. The wireless sensors of "smart" helmets, for instance, constantly monitor the wearer's brainwaves and stream the data to computers that use AI algorithms to purportedly detect emotions such as depression, anxiety, or rage, as well as other mental activities, which, can purportedly be monitored or used to prevent accidents or increase safety or efficiency in an organization.

Here are some more specific examples of private sector applications in China:

- *Helmets – Manufacturing Company*
  Manufacturing firms are outfitting their workers to wear caps that can monitor their brainwaves. Management seeks to use this data to adjust the pace of production and redesign workflows. For example, Hangzhou Zhongheng Electric believes it could increase the overall efficiency of the workers by manipulating the frequency and length of break times to reduce the mental stress of workers.

- *Cushions –Tech Company*
  Hebo Technology, a private firm in Hangzhou, developed and gave smart cushions to its employees. The smart cushions alert managers when employees appear to be away from their desks, or when an employee appears to get emotional or stressed. Smart cushions are additionally being used to monitor an employee's vital signs, which also informs workers when to get up and stretch. Companies can use this collection of data to cross-reference it with an employee's general performance at work.

- *Bands/Uniforms - Service Company*
  A sanitation company use smart bands to keep track of idle workers, and send out alerts saying "please continue working, add oil!" if there has been no movement from the wearer for more than 20 minutes. Smart bands and smart uniforms embedded with ID chips and GPS function are being used to monitor location and to keep track an employee's whereabouts. The devices are also used as a way for workers to clock in, and ensure they remain in their designated work areas, which management uses to potentially increase efficiency and lay off lazy workers.

And here are some more specific examples of public sector applications in China:

- *Helmets – Hospitals*
  Hospitals use smart helmets to allegedly monitor patients' emotions and prevent violent incidents. In addition to the helmet, a special camera captures a patient's facial expression and body temperature, while pressure sensors under the bed monitor shifts in body movement. Together, it is believed that the collected information can give a more precise estimate of the patient's mental status. Patients are informed if their brain activities are monitored, and the hospital does not activate the devices without the patient's "consent" (the sufficiency of which is another matter).

- *Helmets - High-speed Trains*
  Brain monitoring devices are worn regularly by train drivers working on the Beijing-Shanghai high-speed rail line. The sensors, built in the brim of the driver's hat, are purportedly used to measure various types of brain activities, including fatigue and attention loss with an accuracy of more than 90 percent, according to the company's website (e.g., if a driver dozed off the cap could trigger a cabin alarm to wake him up).

- *Headsets – Public Schools*
  Some schools have made students wear brain-wave sensing gadgets that can purportedly help track their attention and concentration-levels during class. The idea is that teachers can access this data to track who is paying attention or not, and that parents can also track their kids' attention levels and compare them with the scores

and grades of other kids in class. Teachers say the students pay better attention after wearing the devices, which makes them more likely to study harder and obtain better scores. Data collected can also be repurposed for government-sponsored research.

- *Bands/Uniforms - Public Schools*
  A secondary school in Guangdong uses Tencent's smart campus platform and smart bands to monitor the location of students, the number of people in the area, class arrivals, and campus entry and exit information, which can be paired with FRT to monitor students, staff or unwanted individuals around campus. Tencent's smart campus platform has already been deployed at more than 300 schools and universities and is alleged to give school management, teachers, and parents a way to obtain more information about the students and their activities.

4. Exhibited and potential harms of a particular biometric technology: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

These use cases present a wide array of known and potential harms and ethical concerns.

1. Ethics of Biometric IDV Systems

To be reliable and accurate, biometric digital ID solutions require a lot of data—typically sensitive, personal data such as facial images and other biometrics. For example, a training set of millions of faces is required for AI facial similarity checks, which are only as good as the training data and require continuous monitoring and correction of the model. Mistakes in AI used for biometric IDV can lead to significant consequences, such as the denial of access to services, especially when there is no analog or physical alternative, which is increasingly the case. This challenges traditional data protection and privacy principles such as data minimization, purpose and use limitations, storage limitations, transparency and accountability requirements, and data integrity and quality principles, among others, while introducing new risks of bias, discrimination, and exclusion.

While we tend to focus on the data privacy and security features of a specific AI-powered biometric technologies, we typically ignore the privacy and security implications for people whose personal data, faces, and other biometrics are used to build and train those tools and models in the first place. As a result, there is an asymmetry between the privacy of individuals used to build and train the AI and the beneficiaries of any tools ultimately built and deployed from those data sets. Moreover, as a result of complex supply chains of personal data use, the entities designing and building AI-based identity solutions are often not the ones using or deploying them. Without a direct relationship to the companies designing and building these tools, the chain of responsibility and accountability for privacy and security often breaks down, leaving individuals with limited visibility, control, or recourse over how their information is used.

2. Shaky Scientific Foundations

Many of the use cases for physical and behavioral biometrics described herein are based on controversial or shaky scientific foundations. It is widely recognized that general FRT systems are prone to bias based on gender, race, ethnicity, age, and other characteristics. Other physical biometric modalities such as voice recognition have been shown to exhibit similar biases. Many tools and technologies that incorporate physical and behavioral biometrics assume that it is possible to automatically and systematically infer certain emotions or other internal states or proclivities of human beings from outwardly observable features, expressions, movements, or behaviors, without a solid scientific basis. For example, as FRT is increasingly used for emotion detection or to predict certain behaviors or traits, we must recognize that things like facial expressions vary widely across cultures and contexts, making such systems inherently suspect.

Similarly, other physical and behavioral biometrics, such as gesture recognition or gait analysis, presume some kind of “normal” from which deviations are deemed “abnormal” and indicative of certain traits of proclivities. These systems are inherently discriminatory against individuals with differences in body shape, posture, mobility, or certain disabilities, and can exacerbate the risks of inequitable treatment and exclusion.

3. Data Privacy Concerns

In the United States, the lack of comprehensive federal privacy legislation means that many uses of data implicated in these biometric technologies remains largely unregulated. While some states have passed privacy legislation, these laws often fail to adequately address the kinds of biometrics implicated in many of these systems. Even Illinois’ Biometric Information Privacy Act, which regulates the collection, use, and handling of biometric identifiers by private entities, and is arguably the most stringent biometrics law in the country, narrowly defines “biometrics” such that it would not cover a wide array of new modalities of behavioral biometrics and is easily bypassed by “consent.”

Over-collection of data as well as predatory data-gathering practices is also very common in China, since regulation on the areas has historically been laxer, trailing behind the EU, for example. New regulation such as the incoming Personal Information Protection Law (PIPL) is changing this, however, and large companies have already altered and strengthened their data gathering and data privacy practices considerably. With respect to over-collection of data, it is not clear whether people are genuinely appeased by stronger measures taken with regards to China's private sector enterprises, whereas extensive collection of data by the state, is simply an area to be accepted and respected, similarly to the legitimacy of the CCP.

The Chinese government has directed large Chinese companies such as Alibaba, Baidu, ByteDance, Xiaomi, Pinduoduo and Meituan, to rectify a number of issues on their apps, such as mishandling of personal data, frequent harassment of users, and deceiving consumers to give up more of their data including through the use of "dark patterns." Smaller companies have also been directed to rectify a number of similar issues on their apps. Companies use personal data for consumer profiling, which allows for more targeted commercials and advertisements. Data may also be sold in markets for data, which makes small companies engage in predatory practices to collect large swaths of individual data, and generally more data than the company needs for its app itself. Large companies can benefit considerably as they have access to big swaths of individual data.

Chinese citizens are increasingly becoming aware and concerned of data privacy issues. Baidu has, for example, been brought to court in the city of Nanjing by a government-controlled consumers' group. The group claims that a Baidu app illegally monitors users' phone calls without telling them. Ant Financial, which is the financial arm of Alibaba, the country's largest e-commerce group, has also made a public apology for a default setting on its mobile-money app, which automatically enrolled customers in a credit-scoring scheme, called Sesame Credit, without their active consent. If companies are able to monetize consumers' private data, they have an incentive to over-collect personal data and thereby infringe on user privacy.

4. Data Security/Cybersecurity Concerns

While data leaks and cybersecurity issues are as common and concerning in China as they are in the U.S., Europe, and elsewhere, China's strong emphasis on rapid technological implementation and experimentation means that many technologies may overlook or neglect security aspects, particularly as fines for security breaches remain insignificant. New and incoming laws are changing this, however. It is unclear whether people care more about data leaks by public sector agencies (e.g., FRT, school-platforms and wearables) or by private sector entities, which could reveal relative attitudes towards public versus private sector technological implementation and measures of surveillance.

FRT in Residential Neighborhoods & Schools. Residential neighborhoods and apartment complexes across China are rapidly adopting FRT, accelerated by Covid-19. However, incorrectly configured databases remain a widespread security problem in China, as tech companies and workers implement certain technologies too quickly without taking the necessary data security or cybersecurity precautions. As a result, personal data is often insecure and easily leaked. Similar problems are arising in schools. For example, a middle school database in China full of photos of students' faces, ID and student numbers, and GPS locations, was recently left open to the internet without any encryption or other protections. It contained records of 1.3 million people, including students, teachers, cleaners and security personnel, with great risk that individuals' data will be misused.

5. Government Surveillance

As noted above, FRT systems have garnered significant attention and controversy, largely due to concerns about pervasive and expanding government surveillance. Cities and municipalities across the U.S. are imposing limits on the use of FRT, going so far as to ban the technology outright through statewide moratoria in Vermont and Virginia, and in cities including Berkeley, Oakland, and San Francisco in California; Portland, Oregon and Portland, Maine; Boston, Cambridge, Somerville, and other cities in Massachusetts; Minneapolis, Minnesota, and more. But just as these bans were gaining momentum, the shift to a more digital existence during the COVID-19 pandemic, including the proliferation of digital contact tracing, exposure notification, proof of vaccination and health status, and other apps has accelerated and normalized the presentment of biometrics.

In China, the government supports a range of new data-gathering technologies to improve public goods such as safety and health. This includes FRT, which gather individuals' biometric information through surveillance of public spaces. For example, when buying a sim-card, individuals are also required to give up their biometric facial data, which is gathered in order to purportedly combat fraud or abuse. Many public schools are being surveilled, and it is believed that tracking students is a measure to increase safety. Along with the construction of the social credit system which can allegedly help to reduce fraud and criminal behavior, the government is able to keep track of individuals. However, the boundary between public good purposes and government surveillance remains murky.

6. Perverse Incentives

Digital identity is big business and growing bigger each day. The global market for IAM is expected to reach $29.79 billion by 2027, while the global IDV market is expected to reach $17.8 billion by 2026. Cloud-based authentication or identity-as-a-service based on AI/ML is one of the fastest growing market segments. ID products and services are typically either enterprise grade (B2B) or consumer grade (B2C). For example, the entity building a remote, AI-based IDV tool is typically a vendor to another company providing a product

or service to end users. A common business model in B2B arrangements is a *pay-per-verification* scheme, whereby the AI vendor is compensated per verification check (per query or API call) or per user in a given time frame (e.g., one month). Alternative subscriptions, volume-based pricing models, and hybrid arrangements also exist.

When we move through the physical world, we are rarely asked to identify ourselves. Presenting a government-issued ID is the exception, reserved for high-risk situations like boarding an international flight. But as the market for digital ID systems and solutions grows larger, and as everything from online to in-person services increasingly has a digital component, we are at risk of flipping that paradigm and of requiring people to identify themselves in every setting. Increasingly cheap, efficient, and "seamless" forms of biometric-enabled ID, such as contactless payments and palm scanning technologies, could create a fictious need for individuals to identify themselves in contexts where such a need did not exist before. We risk going from ID as the *exception* to ID as the *rule,* especially if we fail to address the nature of the business models of these schemes.

There are few commercial incentives around the use of your physical, government-issued ID documents. In general, no one gets notified or paid when you use them (e.g., the DMV isn't typically notified or paid when you use your license to purchase alcohol). In contrast, digital ID schemes have commercial and technical incentives that are very different from in-person, manual processes. Commercial arrangements such as *pay-per-verification* schemes could incentivize the overuse of ID tools and further normalize the presentment of biometrics. Additionally, the use of AI and ML in combination with biometrics for digital ID management risks transforming identity from something *relational* (established in the context of government to citizen, or business to customer) into something *transactional.*

CONCLUSION

In sum, biometric technologies are already widespread in both the public and private sectors throughout the United States, as they are in other countries, such as China. While FRT has been a primary focal point of the conversation, a wide array of other physical and behavioral biometric modalities present similar concerns with respect to ethics, shaky scientific foundations, data privacy and security, the risks of government surveillance, and perverse business models that risk commercializing all of our interactions, whether as citizens, employees, or consumers. We hope the use cases and harms outlined above help to inform the OSTP as you develop a Bill of Rights for an Automated Society. Should you have any additional questions or concerns about our response to this RFI, please do not hesitate to contact us via email at [redacted] or [redacted].

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Office of the Ohio Public Defender

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Via Email: BiometricRFI@ostp.eop.gov

January 6, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Request for Information on Public and Private Sector Uses of Biometric Technologies, Doc. No. 2021-21975, 86 FR 56,300

The Office of the Ohio Public Defender ("OPD") submits this response to the Office of Science and Technology Policy's request for information about public and private sector uses of biometric technologies. The OPD is the Ohio government agency "responsible for providing legal representation and other services to people accused or convicted of a crime who cannot afford to hire an attorney."[1] Our clients and the communities from which they come are disproportionately impacted by biometric surveillance, giving OPD a vantage point to address the efficacy of various regulatory efforts. The comments below largely stem from the OPD's participation in the Ohio Attorney General's Facial Recognition Task Force ("Task Force") that was formed in 2019.

I. Introduction.

The government's use of facial recognition software and other biometric technology to surveil people is a topic that generated intense debate in the state of Ohio. In 2019, the Columbus Dispatch reported that Ohio's facial recognition dataset—containing 24 million driver license photos that are searchable by law enforcement[2]—may be accessible to local, state, and federal officials.[3] These officials face a very low

[1] Office of Ohio Public Defender, *About OPD*, https://opd.ohio.gov/wps/portal/gov/opd/about-opd (last visited Dec. 28, 2021).

[2] Ohio's state-run facial recognition database is hosted on the Ohio Law Enforcement Gateway ("OHLEG"), which is maintained by the Ohio Bureau of Criminal Investigation. In 2019, the OHLEG database contained 24 million images. Ohio Att'y Gen., *Facial-Recognition Inquiries: A Special Report* 1 (Aug. 2019), https://www.ohioattorneygeneral.gov/FacialRecognitionInquiriesReport.

[3] *See* Randy Ludlow, *Feds Used Ohio Licenses for Facial Recognition*, Columbus Dispatch (July 8, 2019), https://www.dispatch.com/story/news/columns/the-daily-briefing/2019/07/08/feds-used-ohio-licenses-for/4728829007/.

[redacted]

burden before being authorized to conduct a search; they must simply claim a reasonable belief, based upon the totality of circumstances, that the search may result in an investigative lead.[4]

The outcry generated by this news led Ohio Attorney General Dave Yost to temporarily suspend access to the dataset and he established a Task Force responsible for recommending regulatory measures for facial recognition use.[5] The OPD was given one of two public defender seats on this 29-member Task Force. In January 2020, the task force sent 13 recommendations to Attorney General Yost with the goal of balancing "people's privacy interests with the need for public safety while providing scrutiny and increased oversight."[6] To date, none of these recommendations have been acted upon.

Ohio's failure to institute reforms to its biometric surveillance system, even when under intense media scrutiny, demonstrates one problem with allowing law enforcement agencies to self-regulate their access to databases of information. Either they don't do it or they do so in ways that do not factor in other stakeholders' perspectives.

But there are more profound problems than that: local and state actors are only able to regulate the datasets of facial images that they control. Even if the Ohio Attorney General placed stringent regulations on access to its own data, local and federal officers could create or access other datasets without similar guardrails. When considering the federal role in regulating public use of biometric technologies, the Office of Science and Technology Policy should bear in mind the complicated and overlapping patchwork created by the reality that facial recognition datasets are controlled at the local, state, federal, and tribal levels, and not every dataset is subject to the sort of self-regulation on which the Task Force was commenting.

As members of both the Task Force and the indigent defense community, we write to relay the need for a more comprehensive regulation of facial recognition technology by agencies and offices at all levels of government. Below, we address the following questions for which comment was requested:

- #1 Descriptions of use of biometric information for recognition and inference;
- #4 Exhibited and potential harms of a particular biometric technology; and
- #6 Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use.

[4] Ohio Att'y Gen., Bureau of Crim. Invest., *Rules & Regulations* 18 (Feb. 22, 2017), https://files.ohleg.org/general/OHLEG_Rules_Regulations.pdf [hereinafter OHLEG Rules].

[5] *See* Jeremy Pelzer, *AG Dave Yost Suspends But Defends Ohio's Facial-Recognition Software: Capitol Letter*, Cleveland.com (Aug. 15, 2019), https://www.cleveland.com/open/2019/08/ag-dave-yost-suspends-but-defends-ohios-facial-recognition-software-capitol-letter.html.

[6] Ohio Att'y Gen. Facial Recog. Task Force, *Report & Recommendations* 8 (Jan. 26, 2020) [hereinafter Task Force Report], https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/AG-Facial-Recognition-Task-Force-Report-FINAL.aspx.

[redacted]

II. Unregulated facial recognition can produce harm to individuals and communities.

The Task Force recognized that the government's use of facial recognition technology can pose significant risks to civil liberties.[7] These risks have been well documented by others[8] so this letter will only briefly summarize them.

A. Issues with validity systemically impact accuracy of identifications.

A facial recognition search is a "two-part machine-human process" involving facial recognition (which is software-based) and facial comparison (which is human-based).[9] Both software issues and human factors can negatively affect the accuracy of a facial recognition search.

- **Software and algorithmic concerns:** The facial recognition software used in Ohio, NEC-3, has one of the most accurate algorithms on the market, as tested by the National Institute of Standards and Technology ("NIST").[10] This means that the software is relatively better than its competitors at correctly pairing a photo in a dataset of known faces with a photo of an unknown person (also known as a "probe photo"). However, despite these high marks, facial recognition software generates both false negatives and false positives. False negatives—when the software fails to recognize a face—can range from 0.5% to over 10% depending on the software.[11] Similarly, false positives—when the software incorrectly associates two different faces—exist at rates two-to-five times higher for women than men. False positives and negatives increase when probe photos have bad lighting, uneven angles, and when subjects are not directly facing the camera.[12]
- **Human errors:** Humans impact a facial recognition search at multiple points in the process. First, humans choose the probe photo to run through a facial recognition dataset. Later, humans compare the probe photo to the database photo to confirm a putative match. Errors can exist at every point of human intervention. Law enforcement may manipulate probe photos before running a facial recognition search—in fact, officers have photoshopped out tattoos[13] and even replaced a suspect's photo with that of a celebrity lookalike.[14] These manipulations may

[7] Task Force Report, *supra* note 6, at 7 (Recommendation 1).

[8] *See, e.g.*, Clare Garvie et al., *The Perpetual Line-Up* (2016), https://www.perpetuallineup.org.

[9] U.S. Dep't of Justice, *Face Recognition Policy Development Template for Use in Criminal Intelligence and Investigative Activities* 3 (2017), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf.

[10] Nat'l Inst. of Stds. & Tech., NISTIR 8280, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 8 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[11] *Id.* at 7.

[12] Garvie et al., *supra* note 8, at 47.

[13] Nicholas Bogel-Burroughs, *The Police Photoshopped His Mug Shot for a Lineup. He's Not the Only One.*, N.Y. Times (Aug. 24, 2019), https://www.nytimes.com/2019/08/24/us/police-photoshop-tattoos.html.

[14] Drew Harwell, *Police Have Used Celebrity Look-Alikes, Distorted Images to Boost Facial-Recognition Results, Research Finds*, Wash. Post (May 16, 2019), https://www.washingtonpost.com/technology/2019/05/16/police-have-used-celebrity-lookalikes-distorted-images-boost-facial-recognition-results-research-finds/.

[redacted]

exacerbate algorithmic error. But this does not end the impact of human error. Humans must evaluate a probe photo against a menu of database photos of known people that are algorithmically generated as potential matches. Even with training in facial comparison, humans perform poorly at the task.[15]

B. The burdens of inaccuracy rest disproportionately on marginalized populations.

The accuracy problems described above do not have equally distributed effects. The accuracy of facial recognition varies depending on sex, age, race, and skin color.[16] If the software was not trained on diverse enough faces, the technology can struggle to identify a wide array of faces. For example, false positives are highest when analyzing Black and East Asian faces.[17] False positives also tend to be higher for younger and older faces.[18] False negative rates tend to be higher for Asian and Native American people, women, and younger people.[19] False negatives are also generally higher for Black faces when the probe photo is low quality.[20] Issues with the accuracy of facial recognition software compound the disproportionate and racialized impact of other policing practices.

C. The speed at which facial recognition technology expands creates risks of additional unregulated surveillance in real time.

Currently, facial recognition use in Ohio is limited to investigating events that happened in the past. But live, real-time facial recognition tools have emerged and are in use around the country.[21] Use of real-time biometric technology amplifies accuracy concerns because of the risk that identification errors will be accompanied by split-second thought-processes on decisions including the choice to use lethal force. Additionally, the use of real-time facial recognition software has profound chilling effects on core constitutional rights including the right to assemble and protest.[22]

III. Our current patchwork system of regulating facial recognition is inadequate to protect against these harms.

The OPD appreciated the opportunity to raise some of the harms articulated above as a member of the Task Force. But, in a regulatory space that has not yet been shaped by constitutional guardrails, even

[15] Alice Towler et. al, *Do Professional Facial Image Comparison Training Courses Work?*, PLoS One 14(2) (2019), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0211037.

[16] *See, e.g.*, Nat'l Inst. of Stds. & Tech., *supra* note 10, at 2.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] Antonaneta Roussi, *Resisting the Rise of Facial Recognition: Growing Use of Surveillance Technology Has Prompted Calls for Bans and Stricter Regulations*, Nature (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03188-2.

[22] Task Force Report, *supra* note 6, at 8.

[redacted]

rigorous gatekeeping for access to a single state-run dataset of facial images will not materially shape law enforcement use of biometric surveillance in Ohio. And that has profound consequences for our clients, who are indigent, disproportionately people of color, more likely to live in communities subject to significant government surveillance, and at greater risk of suffering the harms generated by unregulated facial recognition use. Federal guidance can limit state overreach.

A. There is a lack of currently articulated constitutional guardrails in this space.

There is a nascent recognition in Fourth Amendment doctrine that digital surveillance is different from other government action, and that it requires more robust regulation. Most recently, the United States Supreme Court held that the government must obtain a warrant to obtain more than seven days of cell site location information ("CLSI").[23] This holding acknowledged the "deeply revealing nature of CLSI" and the "depth, breadth, and comprehensive reach" it provides into a person's life.[24] There are undoubted similarities between CLSI and facial recognition searches: both are deeply revealing about people's whereabouts and are only possible because of the digital world in which we live. But Fourth Amendment jurisprudence has not yet reached biometric surveillance, and there is no guarantee that it will, let alone that it will do so in a way that considers the needs, rights, and civil liberties of people like the OPD's clients.[25]

B. In this constitutional murkiness, self-regulation is inadequate.

If the Constitution and courts are unable to effectively constrain use of biometric surveillance, self-regulation by executive agencies at local and state levels is equally unlikely to be effective. This is true for two major reasons. First, self-regulation is a wholly voluntary act. Second, even rigorous self-regulation by some executive actors is an ineffective way to regulate the law enforcement community.

1. Voluntary self-regulation is not an adequate check on executive power.

The Ohio Attorney General's Task Force made consensus-driven recommendations after a deliberative process that included law enforcement officials, legislators, judges, professors, community stakeholders, and defense attorneys.[26] One example of how compromise and consensus were reached is the Task Force's recommendation regarding the amount of cause needed to authorize a facial recognition search. The existing standard requires only a reasonable belief that the search will lead to an investigative lead.[27] The OPD argued for adoption of Michigan's standard, which requires a showing of probable

[23] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[24] *Id.* at 2223.

[25] *See, e.g.*, *United States v. Tuggle*, 4 F.4th 505 (7th Cir 2021); Andrew Gutherie Ferguson, *Facial Recognition and the Fourth Amendment,* 105 Minn. L. Rev. 1105 (2021).

[26] Task Force Report, *supra* note 6, at 6.

[27] OHLEG Rules, *supra* note 3.

cause before a facial recognition search.[28] The Task Force ultimately recommended that facial recognition searches be authorized upon a showing of reasonable suspicion that the person to be identified has committed a crime."[29]

Because of the compromise-driven nature of the recommendations, significant gaps in the Task Force's regulatory framework remain. The OPD has identified three fundamental concerns with the Task Force's recommendations:

- The Task Force's recommendations fail to require training for law enforcement users of facial recognition on cognitive biases. Such training should recognize that feature comparison methods that partially rely on human judgment remain vulnerable to the similar reliability concerns found in traditional eyewitness identification.[30] Training alone will not render facial comparisons completely accurate, but these training efforts are consistent with current best practices for mitigating human errors during facial recognition processes.[31]
- The Task Force's recommendations do not provide strategies for mitigating the higher rates of mistaken matches among the young, women, and people of color.[32]
- The Task Force's recommendations do not propose an appropriate legal framework for facial recognition use that adequately respects the privacy interests of Ohioans, particularly given the sheer number of Ohioans whose photos are being searched. The modest limit proposed still permit law enforcement to run facial recognition searches for misdemeanors.[33]

Highlighting the relatively lax guidelines proposed by the Task Force identifies part of the problem with self-regulation. The other reality is that these recommendations are unenforceable. The Ohio Attorney General published the Task Force's recommendations nearly two years ago but has not acted on them. And even if the recommendations were adopted, they remain wholly voluntary. Absent legislative action

[28] Task Force Report, *supra* note 6, at 31.

[29] Task Force Report, *supra* note 6, at 4.

[30] *See* President's Council of Advisors on Sci. & Tech. (PCAST), *Report to the President on Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* 5, 31–32 (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf; *see also In Focus: Eyewitness Misidentification*, Innocence Project (Oct. 21, 2018), https://innocenceproject.org/in-focus-eyewitness-misidentification/.

[31] *See* Facial Identification Sci. Working Grp. (FISWG), *Guidelines and Recommendations for Facial Comparison Training to Competency Version 2.0*, at 2–3 (2019), https://fiswg.org/fiswg_fr_systems_guidelines_v2.0_20191025.pdf; *see also* Office of Cmty. Oriented Policing, *President's Task Force on 21st Century Policing Implementation Guide: Moving from Recommendations to Action* 20, 30 (2015), https://cops.usdoj.gov/RIC/Publications/cops-p341-pub.pdf (recommending incorporating explicit and implicit bias into the police training regime).

[32] *See* Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, N.Y. Times (Aug. 2, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html; Garvie et. al., *supra* note 8, at 53–55.

[33] Task Force Report, *supra* note 6, at 14.

[redacted]

or other checks and balances, even adopted recommendations could be rescinded administratively after a single high-profile crime.

2. In a world where facial recognition searches can be done by using multiple private and government-owned data sets, regulation by data set is inadequate.

Even if self-regulation had teeth, it would not meaningfully limit the impact of facial recognition on our clients' lives. We represent clients all over the state of Ohio, in all stages of criminal cases. Our clients' cases can involve state, local, and federal law enforcement, across several jurisdictions in a single case. The Ohio Attorney General's regulations place limits only on how the OHLEG facial recognition dataset can be used. There are countless other databases of facial images that can be purchased or created by local law enforcement or used by federal law enforcement.[34] State-level regulation may effectively articulate a set of political values, but it will have little impact on the use of facial recognition software on the ground in our clients' cases.

A hypothetical can clarify this point further. Imagine that the Columbus Police Department, the Ohio Bureau of Criminal Investigation, and federal agents from the FBI and ATF work together in a multi-jurisdiction guns-and-drugs task force.[35] Imagine further that agents who work for the state government are bound by regulations that limit use of the OHLEG system to circumstances where there is reasonable suspicion that an unidentified, but photographed, person engaged in a gun or drug crime. Finally, imagine that the Columbus Police Department has no internal regulations and its own contract with a company, such as Clearview AI, that has access to private photo databases and an algorithm capable of searching those databases. Under these circumstances, the task force does not need reasonable suspicion to run a facial recognition search. It can simply use Clearview AI via the Columbus Police Department rather than the OHLEG database.

This holds true even outside multi-jurisdiction law enforcement teams. Even when the Columbus Police Department or federal agencies are working alone within the state of Ohio, they may access any database that is not controlled by the Attorney General without complying with OHLEG regulations. Any limitations imposed by a single jurisdiction can be easily circumvented.

IV. Conclusion.

It is an unqualified good thing that state government actors, including the Ohio Attorney General, are considering regulation of biometric technology such as facial recognition. Further, the inclusion of stakeholders like public defenders—whose clients are directly and harmfully impacted by this technology—should be applauded. But executive agency self-regulation in a space that includes private

[34] GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies* (Aug. 24, 2021), https://www.gao.gov/products/gao-21-526.

[35] Multi-jurisdiction task forces are very common in police work today. *See* David Hayeslip & Malcolm Russel-Enhorni, *Evaluation of Multi-Jurisdictional Task Forces Project* (Sept. 27, 2002), https://www.ojp.gov/pdffiles1/nij/grants/200904.pdf.

databases, public databases, and multiple overlapping jurisdictions will have limited impact on the practical use of the technology. We write this comment to ensure this office has the perspective of public defenders and the clients we represent on this critical issue.

Sincerely,

Timothy Young

Ohio Public Defender

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Onfido

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

onfido

Comments to the White House Office of Science and Technology Policy

RFI on Public and Private Sector Uses of Biometric Technologies

January 2022

Respondent: Onfido, Inc.
Respondent Type: Industry
Point of Contact: Amy Shuart, Head of US Government Affairs

Establishing real identity is essential to unlocking financial services and other opportunities for underserved communities in the United States, while also protecting all consumers from the harmful impacts of identity fraud. In the US, losses from identity fraud increased 42% in 2020, costing businesses $712 billion.[1] Biometrics and the power of artificial intelligence (AI) are essential components to verifying and protecting an identity.

Onfido is excited for the opportunity to share our expertise and experience to help develop regulatory reforms to foster innovation, accessibility and financial inclusion for all across national borders.

Our response provides a general overview of our company and how we use biometric technology, and our responses to RFI Topics 1, 2, 5, and 6.

Introduction to Onfido

Onfido, founded in 2012, is a global remote identity verification provider that partners with 1,600 organizations worldwide, including many US companies. Our leading biometric and artificial intelligence technology enables clients to prove that their customers are who they claim to be, enabling them to comply with regulatory obligations. We use a hybrid model that combines machine learning with human expert oversight, which delivers best-in-class speed, consistency and accuracy.

Onfido is a leader in security, privacy, and ethics while combating AI bias and fraud. Winners of the 2020 CogX Award for "Best Innovation in Algorithmic Bias Mitigation" and "Outstanding Leader in Accessibility" and awarded "Highly Commended" in the SC Europe Awards 2020 for "Best Use of Machine Learning"—our talented team of experts is recognized as top in their field.[2] Our team has published various academic papers on AI including the performance of facial recognition algorithms.[3] We also work with Interpol to share best practices in fraud prevention and publish an annual Fraud Report to share our data with the global community.[4] Onfido is a founding member of the Better Identity Coalition, a Board member of the FIDO Alliance, and a member of TechNet.

Onfido is a market leader in establishing real identity, helping to combat identity fraud and document forgery. Our AI based technology verifies whether a government-issued ID is genuine or fraudulent. It then compares the document against an individual's facial biometrics to determine if they are the genuine owner of the ID. Many of our customers are

[1] https://aite-novarica.com/report/us-identity-theft-stark-reality

[2] https://onfido.com/resources/blog/onfido-wins-best-innovation-in-algorithmic-bias-mitigation-outstanding-leader-in-accessibility-at-cogx-2020

[3] https://openaccess.thecvf.com/content_WACVW_2020/papers/w1/Bruveris_Reducing_Geographic_Performance_Differentials_for_Face_Recognition_WACVW_2020_paper.pdf

[4] https://onfido.com/resources/insights/identity-fraud-report-2022

in the financial services sector, and the quality of our service allows them to use it to comply with anti-money laundering and "know your customer" regulatory obligations across the globe.

Use of biometric information for identity verification and to prevent identity fraud

As more activity is conducted online, it is critical to be confident that a person is who they claim to be online. In light of numerous data breaches, knowledge based authentication is no longer a viable way to confirm a person's identity.

The pandemic drove people to use digital services more than they ever did before. This, combined with the speed of technological innovation, means the number of fraud attempts and sophistication of fraudster tactics has only grown. The data in Onfido's latest Identity Fraud Report 2022[5] shows the growing amount of time spent online has created more opportunities for fraudsters.

While fraud attempts continue at high levels, the type of attacks continue to evolve. We are seeing a lot more 'medium' sophisticated fraud, meaning attacks with less obvious errors such as incorrect fonts or imitated security features. Passports have overtaken National Identity Cards as the most frequently attacked form of identification, which indicates a shift in fraudsters' methods as they choose to target the one-sided passport page, rather than a two-sided ID card. By choosing to target the most high-assurance document, they are hoping that a passport's reputation will help the fake go undetected.[6]

As fraudsters evolve their techniques, so must the detection and prevention methods. It is no longer enough to simply look at a document to determine if it is real, it is essential to check all its security features and ensure that the person presenting the ID is the true owner.

Our AI is able to validate IDs quickly and accurately, and the biometric technology identifies a person based on unique traits such as their face. This ensures that the user is who they say they are, and their ID is genuine. This not only helps to tackle fraud, it provides a fantastic user experience. The whole process is quick, intuitive and can be done whenever and wherever the user chooses.

Procedures for and results of data-driven and scientific validation of biometric technologies

Even in high-risk areas, we need to ensure that we are fostering innovation and promoting the responsible use of AI. To that end we strongly support regulatory sandboxes as a means

---

[5] https://onfido.com/landing/identity-fraud-report/?utm_source=organic&utm_medium=linkedin&utm_campaign=Identity+Fraud+Report+2022

[6] For more details, see Identity Fraud Report 2022 https://onfido.com/landing/identity-fraud-report/?utm_source=organic&utm_medium=linkedin&utm_campaign=Identity+Fraud+Report+2022

to experiment in a safe environment. Greater use of sandboxes need to be more than just a token gesture. It needs to be part of a wider push to stimulate dynamic innovative firms and encourage investors to back them. Industry standards are a key way to independently validate the performance of a technology and efforts are underway to establish an internationally recognized standard for identity verification.

Onfido has extensive experience of working in sandbox environments, which has proven extremely valuable for us, the sponsoring agency and ultimately our customers. Most recently Onfido partnered with the UK Information Commissioner's Office to conduct research on measuring and mitigating algorithmic bias in our facial recognition technology. The research included best practice in data labelling, performance measurement and optimum bias mitigation techniques, all in the wider context of ensuring protection of personal data. This extensive exercise yielded extremely valuable results, which can be found in the public report.[7]

Onfido strives to continually improve the performance of our models but recognize it is difficult to validate our efforts due to a lack of industry standards to assess the accuracy and equitable performance of our product. As result, we have championed the creation of an independent certification and testing program by the FIDO Alliance. Onfido is a Board Member of the FIDO Alliance, an identity standards and certification body with both industry and government participation, and has been participating in this initiative, along with other FIDO Alliance members, to create a new testing and certification program for remote ID proofing tools. When complete, this will create a way to independently validate the claims made by vendors and also determine whether there are any specific biases in a product or algorithm that may need to be addressed.[8]

Exhibited and potential benefits of biometric technology in identity verification

In addition to protecting against identity fraud as discussed above, using biometric technology to verify individuals increases access to services. The world is changing and individuals no longer want to do everything in person. Digital identity verification using biometrics and AI technology enables businesses to give people access to all the services they need, when they need them, while improving equity and inclusion. For example, in the financial services sector, biometric based identity verification can help individuals with a thin credit file (often young people, immigrants, and historically marginalized groups) be approved at a higher rate.

Governance programs, practices, or procedures applicable to the context, scope, and data of a specific use case

Industry and governments must work together to ensure that fraud-fighting technologies can be deployed successfully to identify and stop criminals. With the need for AI becoming

[7] https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf
[8] See https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/

ever clearer, policymakers around the world are looking at what sort of frameworks should be implemented to make sure that this powerful technology is used responsibly. As policy and laws develop to meet the evolving technological landscape, it is crucial that new laws recognize the positive benefits that AI can offer, ensuring fraudsters do not gain an advantage, while also ensuring those utilizing the technology are governed by procedures and practices that are protective of public privacy and protect against bias.

Human oversight

Onfido adopts a hybrid approach that involves both machine-learning and humans in decision-making. However, we only use human oversight when it makes sense to do so. Involving humans in every decision would be disproportionately burdensome and remove all of the efficiencies that AI brings. Indeed it would render many AI use cases redundant.

Further, it might reduce the accuracy of decisions that are made. Studies have shown that humans make mistakes in verifying the authenticity of documents[9] raising doubts about the effectiveness of introducing human oversight to improve the performance of AI systems. Moreover, obliging human oversight implies that humans are better in solving certain imperfections presented by AI systems, which is not necessarily the case.

Discussion on regulating the use of human oversight should be focused on sectors and use cases where it is really needed, i.e. where high-risk decisions are being made and human oversight can be evidenced to show it will improve the outcome (e.g. law enforcement) .

Measures to encourage innovation

It is vital that AI regulation is balanced in terms of protecting users and encouraging trust on the one hand, and promoting innovation and investment on the other. To that end regulations should promote the use of industry-driven standards which are flexible and outcomes-based.

We appreciate OSTP's willingness to consider our comments and suggestions and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact Amy Shuart, Head of US Government Affairs, at [redacted].

[9] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0103510

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Oosto

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

TO: Dr. Eric Lander
Director
THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)
Via email: BiometricRFI@ostp.eop.gov

FROM: Mr. Avi Golan
Chief Executive Officer
OOSTO
152 Madison Avenue, 20th Floor
New York, NY 10016

RE: **RFI Response: Biometric Technologies**

Dear Dr. Lander,

Thank you very much for the opportunity to respond to your Request for Information regarding public and private sector uses of biometric technologies. We have a unique value proposition in this space and are pleased to present six common use cases that facial recognition technology is utilized for purposes of verification and identification (in real-time and post-facto) in various environments, as well as the potential benefits and risks of each case.

We admire and support your organization's mission to implement responsible and meaningful science and technology policies, and we are most appreciative of the opportunity to provide your team with our point of view on the benefits and best practices of biometric technology as it relates to our specific area of expertise - facial recognition.

Introduction

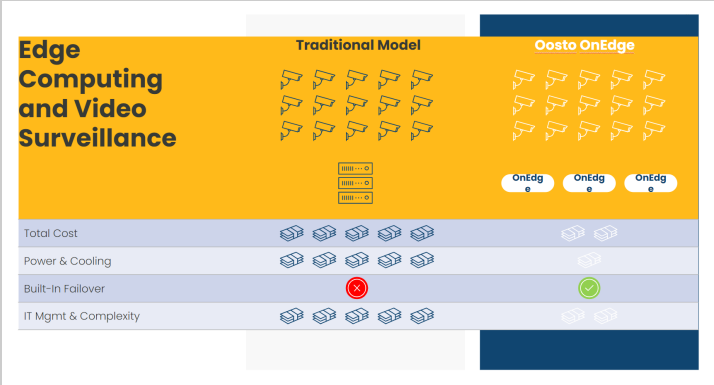
Oosto is a world-leading visual artificial intelligence platform company that organizations across the globe partner with to create secure, seamless experiences in their physical spaces. Since our founding in 2015, Oosto's technology has been proven to operate with the highest levels of identification accuracy in real-time and real-world scenarios while achieving top rankings across all five categories in the Face Recognition Vendor Test (FRVT) conducted by the National Institute of Standards and Technology (NIST), including 1:1 verification. As a result, Oosto has been rated as one of the best facial recognition solutions in the Western hemisphere. This distinction has been achieved through years of world-class AI research, ethical rigor, and proven artificial intelligence technology.

Oosto's data scientists are pioneers in Visual AI research - offering extensive experience in the field with real-world challenges, and expertise with state-of-the-art technologies, applications, and best practices. This research will be accelerated by our recently announced collaboration with Carnegie Mellon University's CyLab Biometrics Center which will focus on advanced object classification and behavior recognition algorithms for commercial use cases.

This collaboration will help Oosto address a broad range of safety-related use cases, including object detection (e.g., weapons on school grounds) and behavioral analysis (e.g., when someone falls down).
Ultimately, our mission is to enable a safer, better protected, and more connected world for the benefit of society.

To date, Oosto has developed, deployed, and continuously improved our facial recognition technology in four primary product offerings:

- **OnAccess** frictionless access control;
- **OnWatch** watchlist alerting;
- **OnPatrol** real-time, in-the-field identification for law enforcement and military personnel; and the
- **OnEdge** appliance, a complete system on module (SOM) that enables facial recognition on video processing to take place on near-edge compute appliances. This completely alleviates the need for cloud-based solutions that need high bandwidth data lines to the cloud and enormous monthly cloud computing costs. In fact, Oosto's OnEdge solution also effectively shifts the GPU-heavy compute load from expensive on-premise servers to small, dedicated power-efficient modules. Oosto OnEdge is our latest offering (available in Q1-2022) and costs a fraction of a traditional on-premise server – typically one-third the cost per video channel – and is capable of processing video from existing security cameras. Also unlike traditional on-premise servers, Oosto OnEdge requires a small amount of power and cooling and doesn't take up space in a rack - which helps to further reduce TCO and is the only feasible way to accommodate large-scale deployment that can handle a large number of video feeds.



Deployment benefits

It is clear that physical safety in the workplace is a prerequisite for operational excellence. To that end, facial recognition technology offers unparalleled threat detection capacity as it can considerably improve workplace safety without inundating security teams with additional responsibilities.

When visual AI takes on repetitive or dangerous tasks, it frees up human labor to carry out work that we are better equipped for — tasks involving aspects of creativity and empathy.

Visual AI also provides organizations with a tool that can process big data quickly and identify anomalies that may compromise or threaten facility security.

Oosto's customer base covers both public and private sector entities, including governmental agencies, and leading companies in financial services, manufacturing, transportation, retail, health and fitness, professional sports, and gaming sectors, among others.

Our customers are using Oosto's leading visual AI platform to positively impact safety and security, productivity, and customer experience. Oosto's facial recognition technology enables enterprises to better protect their customers, guests, and employees by identifying security and safety threats in real-time without compromising on fair and ethical use.

Please note that Oosto operates in the physical security space, and not in the digital space (i.e., cybersecurity). Therefore, all of the aforementioned refers to only biometric-related identification - and specifically ethical facial recognition - in physical spaces.

How it works

Facial recognition technology allows matching between a person's image (video or stills) and a tagged image of that person in the database, which includes his or her name and other identifying features. The list of people in a database is called a "watchlist;" there are also "safelists" to segment persons with authorized access, versus "blocklists" which identify those whose entry is prohibited in a specific space.

How we lead

Today, the success of an organization lies in its ability to quickly adapt, evolve, and respond to change.

Many public- and private-sector entities are looking to adopt new technologies that make life easier, safer, and more intuitive for employees, visitors and customers while optimizing existing resources, increasing productivity, and reducing operational risk. Artificial intelligence provides significant benefits to this effort, including improved speed, accuracy, cost savings, fraud detection, medical diagnoses, and customer experience, for example.

Our mission is to provide the public and private sectors with more efficient, accurate, and reliable tools in which to keep their people, properties, and assets safe and secure. Our technology is powerful and we consider its potential use in a variety of contexts very seriously when presented with new opportunities for its deployment.

> **Ethics review board.** For example, Oosto employs an internal Ethics Board which reviews every potential sales opportunity to ensure that our technology is being used for ethical purposes. The Ethics Board also considers the regional differences and compliance mandates to ensure that our technology falls within those designated guard rails. If the prospective customer is a government or law enforcement agency, we carefully review each use case to ensure it meets our strict guidelines for ethical use.

Terms of use. Secondly, in Oosto's end-user license agreements, all customers are prohibited from using the technology for inappropriate, improper, or unlawful purposes. We are committed to doing what's right, and building technology that protects our identities and biometric data while simultaneously protecting places, people, and profits from bad actors and security threats.

Advanced privacy settings. As there currently exists no federal regulation on visual artificial intelligence (AI) and face recognition technology, Oosto takes a strict, market-leading approach to ensure that we meet a high standard of maintaining user privacy and fair and ethical use of the technology in both private and public use cases.

This includes our offering advanced privacy settings, including Face Blur and Discard Detections options, designed to protect the identities of innocent individuals not on watchlists. Our **Face Blur option** effectively blurs all faces of people not explicitly listed on an organization's watchlist. When this feature is activated, only individuals identified on the watchlist are visible — all other people in the field of view of the camera are blurred. Our **Discard Detections mode** goes a step further, as it discards

all face detections of non-enrolled individuals (and doesn't retain any of their biographic data).

The power of Oosto's AI lies in our platform's ability to provide highly accurate results, generate fewer false positives, and leverage clients' existing hardware to deploy our technology as rapidly as possible.

Nature and source of data used

A key differentiator of ours as a facial recognition provider is that **Oosto starts with an empty watchlist,** and we build datasets from scratch, rather than scraping images from publicly-available sources on the Internet (e.g., including news media, public social media). Unfortunately, this method of facial recognition has justifiably angered privacy groups and data protection agencies around the globe and damaged public trust in the accuracy and reliability of facial recognition systems**.** The watchlist should be narrowly defined based on known security threats or other classes of persons of interest (e.g., VIPs or employees).

Also, **we use real-world production data.** Whereas many facial recognition technologies struggle to correctly identify people under challenging conditions, such as bad lighting or when individuals are not looking directly at the camera, Oosto's technology consistently outperforms expectations in terms of speed and accuracy. This is due to our AI models having been built with real-world imperfections which make them more robust and more accurate in recognizing persons of interest even in suboptimal environments.

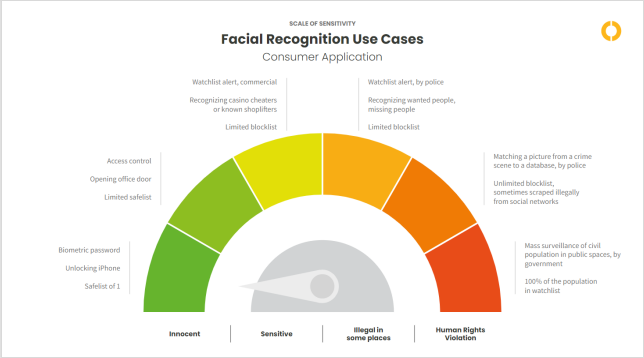
Moreover, our training models are built on representative, balanced data sets. Neural networks - built with diverse skin tones, facial poses, genders, ages, and ethnicities - perform better in the wild and minimize demographic bias.

Notably, when our solution runs on-premise, no data is passed over the Internet from our commercial customers to Oosto, which effectively makes it a closed network. Oosto does not

store any images of faces or bodies, just mathematical vectors. Any watchlist photos in use are uploaded and managed by our commercial customers based on their unique security needs.

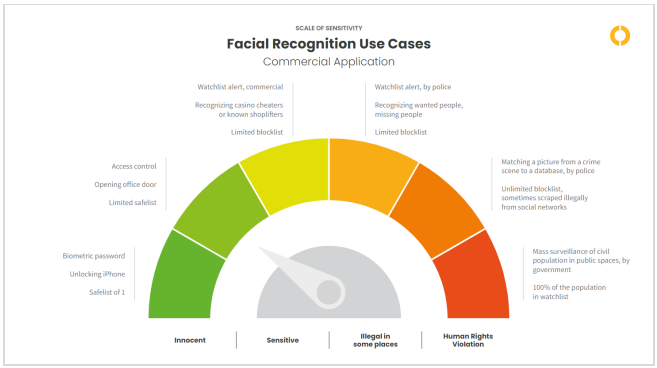
In this summary, we will detail the different types of popular use cases of facial recognition according to the degree of sensitivity and risk.

1. **CONSUMER APPLICATION**
    - **Facial recognition as a password.**
    - **Oosto offering in this use case: None.**
    - **A safelist of one person.**



This is a very popular use case example in which facial recognition technology unlocks a mobile phone or a car. Facial recognition replaces the use of a key or password and is reliable and convenient to use. The technology also provides socially acceptable security and privacy risks. The critical thing to mention in this use case is that **the user voluntarily *opts-in* to provide their face** as the unlocking biometric mechanism in these environments, and the algorithmic data created to recognize the unique attributes of a person's face is performed at the user's request.

2. **COMMERCIAL APPLICATION**
    - **Frictionless access control.**
    - **Oosto offering in this use case: OnAccess.**
    - **A safelist of a small group of people.**



A physical access control solution based on facial recognition is commonly found in locations such as corporate office buildings, residential buildings, manufacturing facilities, transportation hubs, commercial areas, and the like. These facial recognition systems allow access to a predefined group of authorized people who have only safelisted access. The

system will allow automatic, frictionless and very rapid opening of access doors to authorized personnel; it will also prompt immediate alerts in order to identify and locate unauthorized persons in a restricted area.

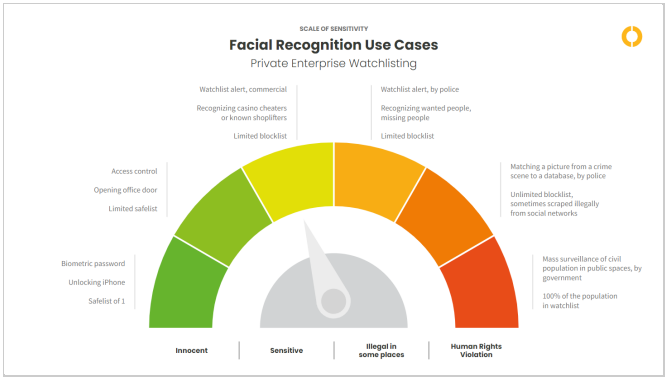
Moreover, Oosto's visual AI-driven platform protects users against sophisticated spoofing attempts as our solution has liveness detection technology to ensure every detected face is a real person vs. a spoof (e.g., a picture displayed on a phone). A good solution can identify spatial inconsistency in real-time by using an array of sensors that create a 3D map of a person's face to effectively eliminate spoofing threats.

This set of use cases has traditionally been used for security purposes, but has recently expanded into areas of safety, efficiency, hygiene, and improving the customer experience.

In one customer use case, a logistics center uses Oosto's solution to streamline and improve the process of releasing containers to truck drivers. In another, a professional football team uses Oosto's technology to allow professional athletes entry into private practice facilities and restricted areas of a stadium including training and locker rooms.

3. PRIVATE ENTERPRISE WATCHLISTING

- **Watchlist alerting**
- **Oosto offering in this use case: OnWatch**
- **A limited blocklist**



Security-enabled CCTV systems are commonly used in private spaces open to the public, such as retail chains or casinos. These types of commercial clients maintain a limited list of individuals who either are identified as VIPs for whom an establishment would like to provide a special level of customer service or a person of interest (POI) who poses a threat to the business because they are convicted criminals, or have a history of violence or theft.

Casinos

In casinos, Oosto's identity alerting solution adds another layer of safety and experience to the casino and gaming environment by enabling operators to keep a watchlist of persons of interest (POIs) and alert upon any unauthorized individual or VIP as soon as they enter the premises. Oosto's neural network uses both face and body recognition to detect POIs on a watchlist. This technology allows security teams to meet banned players (which could also

include self-excluders or advantage players) before they reach the gaming floor - and enables a hospitality team to greet VIPs as soon as they enter the lobby.

Oosto's OnWatch solution also allows operators to use historic footage from already-installed cameras to trace a POI and understand in real-time who they've come in contact with (and for how long). As soon as a patron or employee is identified, our software can search backward and determine everyone who may have interacted with him or her.

Retail

According to a recent report from Retail Industry Leaders Association and Buy Safe America Coalition, as much as $68.9 billion worth of products were stolen from retailers in 2019 (pre-Covid). In addition to the adverse economic impact that shoplifting has on small and large businesses, more brazen and violent theft in stores is also having a negative psychological impact on employees.

As detailed in the report, nearly 67% of asset protection managers at leading retailers surveyed report a moderate to a considerable increase in organized retail crime, while more than 86% said that an organized retail criminal has verbally threatened an associate with bodily harm.

Oosto helps retailers identify known shoplifters, identify employee theft, and reduce shrinkage with real-time video surveillance and forensics which allows operators the ability to quickly search weeks of video footage to identify suspects and streamline their investigations.

Oosto's facial recognition technology is both immediate and highly accurate (0.1% false alarms coupled with 0.2ms detection speed), and serves to protect law-abiding shoppers while identifying security risks that may pose a threat to employees, customers, and profitability.

Much like the casino scenario, operators are empowered to protect their people, properties, and assets by keeping a watchlist of persons of interest (POIs) that alert upon any unauthorized individual, known shoplifter, or VIP as soon as they enter the store.

One Oosto retail customer realized 77% more apprehensions in shoplifting suspects in one month's time and a 25% ROI on total company-wide project cost during the first three months of deploying our watchlisting solution.

PUBLIC SECTOR USE CASES

Facial recognition technology offers a number of benefits to law enforcement and other government agencies and can be used as a force for good.

There are two fundamental use cases for law enforcement -- real-time alerting and post-event/forensic investigations. Oosto's solutions can help in both use cases. Much of the public backlash is associated with real-time video surveillance in public places.

oosto

Oosto helps protect law enforcement and military personnel by connecting to existing body cameras and analyzing video streams in real-time using on-the-go Vision AI technology to identify persons of interest such as criminals, dangerous individuals, or missing children.

To the detriment of local communities and citizenry, police use of facial recognition technology is currently prohibited in several U.S. cities and states. Unfortunately, this effectively handicaps law enforcement agencies from successfully serving the best interests of their communities. In many cases, time is of the essence and mere seconds could mean the difference between life and death. ***Visual artificial intelligence can help save lives.*** Thus, it is short-sighted to prohibit the use of such a powerful tool that can lead to more favorable outcomes for law-abiding citizens.

Claims about demographic bias in facial recognition technology are overblown. For example, an FBI study from 2012 showed a "5 to 10 percent differential in biometric performance for matching photos of Black people," but the Security Industry Association (SIA) notes that in the intervening time, industry accuracy measurements have changed from errors per *thousand* candidates to errors per *million*, showing the study to no longer be relevant."

As the SIA pointed out in July 2021, in another study often quoted by opponents of the technology, "The results are also based on algorithms which are now considered obsolete and were challenged immediately by IBM, but the study is often the main point in support of the contention that face biometrics do not work for women or people with dark skin."

Moreover, the U.S. National Institute of Standards and Technology (NIST) further investigated the issue and reported that "the results were being overgeneralized and misinterpreted by some in the media." In fact, what differences found were largely due to passport fraud identified among samples from Somalia and that ongoing NIST testing has revealed that "among the top 20 performing facial recognition algorithms, the worst demographic for performance is still 99.7 to 99.8 percent as accurate as the best, and white males are the demographic with the lowest match rates."

Notably, public sentiment is evolving on the use of facial recognition technology. While privacy concerns drive some of the skepticism on the technology, in a recent Australian study, it was noted that 61% of those surveyed were "supportive of police using facial recognition technology after a crime has occurred" and that, "Overall, the discourse was mostly positive for the use of FRT (facial recognition technology) by police."

Moreover, in a recent survey conducted by an advocacy group opposed to facial recognition, only 19 of 53 retailers said they would shun the technology.

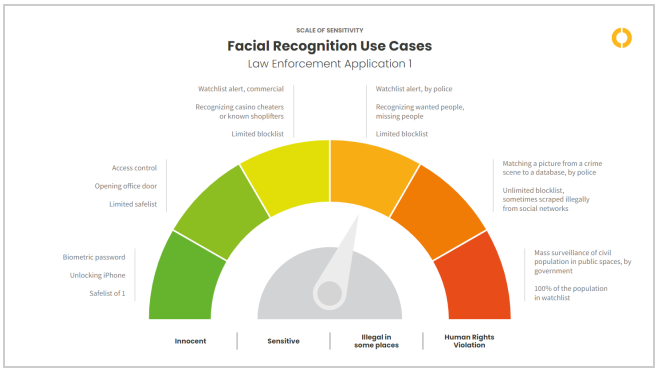
The following two use cases relate to police use but differ in the purpose and manner of use, as well as in the scope of watchlist data being utilized. These examples also differ as it relates

to the general public's perception of personal privacy and the potentially invasive, but widely misunderstood, use of facial images without consent.

oosto

4. LAW ENFORCEMENT APPLICATION 1

- **OnPatrol.**
- **Real-time monitoring of public spaces for locating missing people and identifying wanted criminals.**
- **Limited watchlists.**

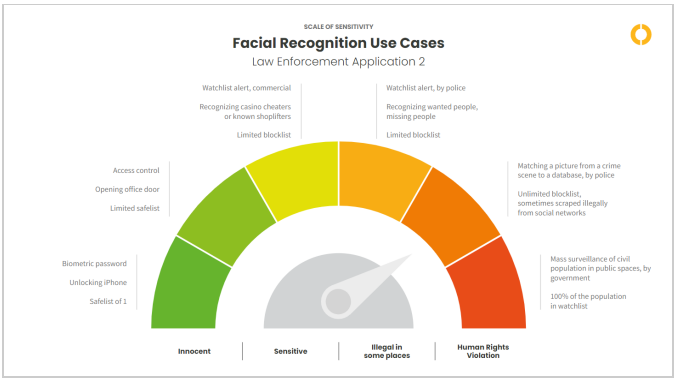


Oosto's OnPatrol solution works before a crime happens, and locates missing people and wanted criminals after a crime has occurred.

OnPatrol's functionality excels in both its flexibility and diverse abilities in being able to spot a wanted individual in a large, real-world environment of many people in real-time - while using the officer's body camera or a mobile phone. The OnPatrol app is provided to police with an empty database. The database is populated directly by law enforcement personnel due to justifiable reasons for watchlisting specific security threats.

5. LAW ENFORCEMENT APPLICATION 2

- **Post-facto identification for forensic investigation.**
- **Oosto offerings in this use case: OnPatrol and OnWatch.**
- **Unlimited watchlists.**

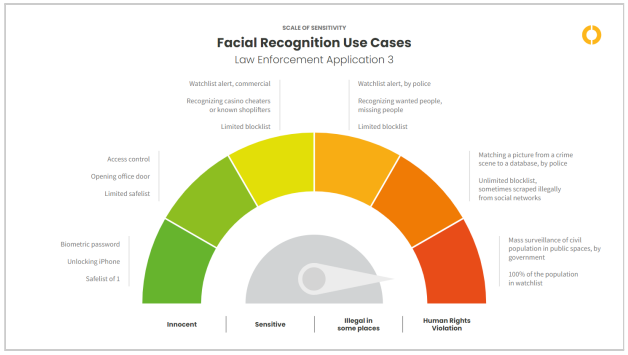


The police obtain a picture of a suspect from a crime scene and want to find out, "Who is the person in the picture?" That requires as wide a database as possible. Optimally - photos and identities of all the people in the world.

In order to accumulate a database of billions of images and identities, there are facial recognition companies that have scraped images from social networks. (Oosto is *not* one of them.) This method has been used by hundreds of U.S. police and other law enforcement agencies in the pursuit of solving crimes.

However, this method has been declared illegal in Canada, Australia, the UK, and France, with all of these countries ordering the deletion of photos of their citizens from face recognition apps used by law enforcement agencies.

6. **LAW ENFORCEMENT APPLICATION 3**
    - **Mass surveillance of the civilian population in public spaces.**
    - **Oosto offerings in this use case: None.**
    - **Unlimited watchlists.**



The practice of using facial recognition for purposes of mass surveillance of civilian populations has been reported in the Western press as a concerning method of conduct by non-Western governments. To the best of our knowledge, this is not occurring in the U.S. today. Surveillance for monitoring and controlling the civilian population has been deemed as a violation of human rights by the United Nations, while video surveillance equipment and VMS manufactured by Chinese companies such as Dahua, Huawei, and Hikvision have been banned for use by the U.S. government. It has been reported that the technology has the potential for unethical practices such as social scoring and the suppression of ethnic minorities. A Beijing News survey showed that nearly 90% of respondents in China stated they do not want facial recognition used in commercial areas.

As UN High Commissioner for Human Rights (OHCHR) Michelle Bachelet recently stated, appropriate safeguards need to be put into place and due diligence must be conducted in order to protect and uphold human liberties so that biometrics technology benefits, rather than threatens, society: *"The higher the risk for human rights, the stricter the legal requirements for the use of AI technology should be…the power of AI to serve people is undeniable, but so is AI's ability to feed human rights violations at an enormous scale with virtually no visibility. Action is needed now to put human rights guardrails on the use of AI, for the good of all of us."*

…

In conclusion, as a worldwide operating company in ongoing dialogue with governments and global corporations, we strongly recommend that regulatory guidance be developed in the field of artificial intelligence and specifically facial biometrics in an effort to better protect civil liberties and human rights while supporting businesses and government agencies with a safe path to gain from the many benefits that facial recognition technology offers.

As we previously demonstrated on our Sensitivity Scale examples, facial recognition involves many different use cases, ranging from innocuous activities such as unlocking a mobile phone, to government video surveillance in public settings. There is a significant chasm of use cases falling in the "gray" zone that requires careful consideration of balancing the need for security and public safety with an individual's right to privacy.

Oosto is willing to share our industry insights and best practices from our vast experience gained from independent research, collaborations with some of the leading universities in the world, and from having deployed this technology in real-world conditions for thousands of institutions. We continue working diligently on ways to enhance Visual AI technology for the benefit of society as a whole.

Again, thank you for the opportunity to contribute our voice to helping shape our nation’s technological priorities. Please do not hesitate to contact us directly with any questions you may have about Oosto, our facial recognition technology, or our practices.

Sincerely,

[redacted]

Avi Golan
Chief Executive Officer
OOSTO
www.oosto.com

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Orissa Rose

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 14, 2022

Via Electronic Submission to [redacted]

Office of Science and Technology Policy (OSTP)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: RFI Response: Biometric Technologies

Dear Members of the Office of Science and Technology Policy:

I, Orissa Rose, graduate student at University of California, Berkeley am pleased to submit the following comments on Public and Private Sector Uses of Biometric Technologies. As a candidate for a Masters of Information Management and Systems from Berkeley's School of Information, my work focuses on expanding access to data and improving its usability, reliability, and credibility while preserving human rights, security and privacy. My research on information policy investigates the role public institutions like you play in mitigating algorithmic harms and establishing data standards that protect citizens, especially the most marginalized by rapid technology developments. These comments do not address the entirety of RFI sections available, but rather, focus on Section 6 of the RFI: Governance programs, practices or procedures.

I welcome any opportunity to continue this conversation, provide future resources or answer questions. Although the undersigned is a member of UC Berkeley, I am signing as an individual and do not represent this organization.

In appreciation,

[redacted]

Orissa Rose
Masters Student and Technology Consultant
[redacted]

Section reference:
General comments on data collection ethics.

Recommendation:
Prioritize investigation into disparate impacts on the most vulnerable communities throughout your investigations of biometric data use. These communities are most likely to be negatively impacted by discriminatory algorthmis and data treatments, and least likley to have their interests advocated for and funded.

Comment:
A common mistake of our times is the assumption that when we hand activities off from human actors onto technical systems, things will go smoothly so long as the components we swap are modular in their functional scope, and we have accounted for errors with math.[1] The growing popularity of using AI built on biometric data to identify people, surveil activity, or assess human emotion and health has gained momentum on the notion that employing technical systems to do this work will generally leave ethical and political dimensions intact. We rationalize that these tools and uses of data don't cause more harm than good, and we believe these narratives because the system developers claim to have attended to bias in their models, or because we are aware of error rates in human computing, or because we do not yet have evidence to counter the claims.

Recent literature on the failings of pretrial risk assessment tools like COMPAS[2] can be a useful and cautionary resource to your team about the pitfalls of reliance on subjective datasets to make serious determinations about a person's future. Legal experts and technology scholars have consistently demonstrated how risk assessment tools -- which purport to leverage data to predict a criminal's pretrial custody options, appropriate length of parole, and more -- are more truly tools to predict and map trends in policing behavior. The use of biometric technologies to monitor behavior and predict emotional state or physical health is not too dissimilar. Just as risk recidivism tools use partial datasets to advance prejudice and racialized decisions, biometric technologies that are not built with the explicit intention to mitigate known and unknown harms could result in worsening occurrences of undue prosecution, misidentification of innocent people, and entrenchment of medical racism and elderly abuse.

The FTC's 2016 report on data collection abetted by IoT devices details the disparate impact these technologies have on disadvantaged communities. Inaccurate or biased analyses of biometric data collected by a range of IoT devices can lead to consumers being denied opportunities for education, employment, healthcare or credit.[3] The imperative of our federal agencies to protect equal opportunity and fair treatment compel OSTP to prioritize these most vulnerable communities in your investigations of biometric data collection and standards.

[1] (Nissenbaum & Mulligan, 2020)
[2] See Megan Stevenson's *Assessing Risk Assessment in Action*, and Alicia Solow-Niederman's *The Institutional Life of Algorithmic Risk Assessment*.
[3] (Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning, 2016)

Section Reference:
6a) Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies.

Recommendation:
Resist the urge to convey the use of biometric data for healthcare and social welfare programs as a panacea to industry bias and inefficiency. Advocate for biometric data collection standards that are based on human rights principles. Additionally, evaluating proposed biometric technologies against the five "abstraction traps" could help OSTP and your partners prioritize technologies that place human rights over profit incentives.

Comment:

The language in OSTP's RFI demonstrates your optimism that biometric technologies can solve many societal and institutional shortcomings. While I acknowledge and celebrate the important ways technological developments have contributed to incredible achievements in medicine, education and social connection, I am also compelled to warn OSTP against the five common traps that indiscriminate support of AI can create. Machine learning scholars from Microsoft, Princeton, and the Data and Society Research Institute identified five "'Abstraction Traps' that result from failing to properly account for or understand the interactions between technical systems and social worlds". This framing can support policymakers' and technology professionals' essential considerations before proceeding with adoption and implementation of new machine learning systems".[4]

1. Framing Trap - Failure to model the entire system over which a social criterion, such as fairness, will be enforced.
2. Portability Trap - Failure to understand how repurposing algorithmic solutions designed for one social context may be misleading, inaccurate, or otherwise do harm when applied to a different context.
3. Formalism Trap - Failure to account for the full meaning of social concepts such as fairness, which can be procedural, contextual, and contestable, and cannot be resolved through mathematical formalisms.
4. Ripple Effect Trap - Failure to understand how the insertion of technology into an existing social system changes the behaviors and embedded values of the pre-existing system.
5. Solutionism Trap- Failure to recognize the possibility that the best solution to a problem may not involve technology.

Analyses of marketing trends amongst leading biometric technology companies found that the arguments they put forward skillfully position the deregulation of biometric data as essential to the advancement of medical science. Many of these parties "assumed that patients want 'their' data to be used and prioritized long-term use of patient data above actual patient expectations or consent.[5] In practice, and as evidenced by the lawsuits, recent media firestorms, and "levels of indignation [from newly informed citizens] about perfectly lawful data practices", we know that

[4] (Selbst, Boyd, Friedler, Venkatasubramanian, & Vertesi, 2019)
[5] (Felt & Starkbaum, 2019)

that status quo needs to change.[6] A recent investigation into facial recognition programs at large tech companies revealed how the lack of public knowledge about biometric data collection and use has “allowed technology companies to create a climate favorable to their use of customers' biometric data, largely without their knowledge or consent.”[7] To support data collection standards that prioritize the data subjects and are especially sensitive to vulnerable communities, these principles of designing for social justice will be useful to incorporate in your investigation:

- Design for Transformation - A long-term approach focusing on the role of structural inequalities; designing for the evolving, emergent social, economic, and political relations that produce inequalities and perpetuate social injustices.
- Design for recognition - Focuses on identifying unjust practices, policies, laws, and other phenomena that create data realities , as well as identifying those people who are most negatively impacted by such phenomenon.
- Design for Reciprocity - Focuses on relationships and the ways in which those relationships may need to change to become more equitable for all stakeholders; the relationship between those who are owed justice and what needs to occur for the obligations of justice to be fulfilled.
- Design for Enablement - a multi-level focus on developing opportunities for change, including scaffolding individual behavior change as well as the practices and policies related to fostering structural change.
- Design for Ethics - Contending with the individual’s immediate needs, and attempts to address the larger context and imbalanced power relations that produce the potential for and actual oppression

Section Reference

6c) Practices regarding data collection, review, management, storage, and monitoring practices.

Recommendation:

Leverage the maturity and effectiveness of existing data collection and storage standards from GDPR, CCPA and existing state biometric legislation (Illinois, Oregon, Texas, Washington, City of New York) to advance proven practices whose path to compliance is already known.

Comment:

The benefit of OSTP supporting data collection articles similar to the GDPR, CCPA and other existing biometric policies[8] is that many large companies and international researchers have already had to build out their systems to achieve compliance with those standards, and they are proven effective. The GDPR articles most apt for consideration in OSTP’s biometric data collection investigations are:

[6] (Nissenbaum, 2015)
[7] (Pope, 2018 discussing April Glaser’s investigation into Facebook’s collection of the facial data of millions of its users and is now the biggest lobbying force against biometric data privacy laws).
[8] Including: Illinois’ Biometric Information Privacy Act (BIPA); City of New York Administrative Code, Title 22, Chapter 12; Portland City Code, Title 34- Digital Justice, Washington Rev. Code §§ 19.375.010 et seq

- **Responsibility of the controller (**Article 24**):** Controller (data collector) shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that data processing and protection is performed in accordance with all regulations.
- **Data minimization** (Article 25): Defaults data collection to only the data "which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility".
- **Data protection** (Article 25): Data controllers must employ practices like pseudonymization (replacing identifiable fields within a data record with pseudonyms or dummy values), to protect personal data, (and sensitive data categories) and must certify compliance with this requirement.

Section Reference

6c) Practices regarding data collection, review, management, storage, and monitoring practices.

Recommendation:

Standardize compliance with conscientious data collection tools to help biometric data companies examine their positionality and the ethical implications of their methods and findings. Develop sensitivity ratings for different types of biometric data. In an effort to minimize paperwork, focus dataset evaluations on biometric metadata that is most sensitive and influential to care, treatment or sentencing decisions. Consider an online survey or form like HEVAC[9] that requires participation in 70% of recommended activities when handling these highly sensitive data categories to receive a passing mark. Use this as a gatekeeping mechanism for any program seeking federal funding, partnership or approvals.

Comment:

Reflexivity is a practice of critically assessing "the significance of environment, power, and context as well as subjectivity in the delineation and construction of knowledge".[10] Without reflexivity, biometric data researchers, private companies and public agencies may unwittingly impose the values, prejudices and practices of their specific culture onto the data and people their tools are working on. Prominent technology scholars and data ethicists have developed tools that data collectors, engineers, and cross-disciplinary teams can use to get clear on the history, context, limitations and ethical implications of the datasets they're working with.

- *Datasheets for Datasets:* Require development of datasheets for any public agency or private partner working with biometric data. In 2018, researchers from Microsoft, Georgia Institute of Technology, Cornell University, University of Maryland, and the Now Institute

[9] Developed by the Higher Education Information Security Council, the HECVAT is a questionnaire specifically designed to measure vendor risk. Before institutions partner with third-parties, the partner must complete a HECVAT tool to confirm that information, data, and cybersecurity policies are in place to protect sensitive information and constituents' PII.

[10] (Ryan & Walsh, 2018)

introduced the idea of a narrative “datasheet” to accompany any dataset. Recognizing that “the risk of unintentional misuse of datasets increases when developers are not domain experts”, or are using data collected by third parties, and hoping to “initiate a broader conversation about data provenance, ethics, privacy, and documentation”, the team developed questions that prompt users to describe dataset’s creation, their strengths, and their limitations. Sections of the Datasheet tool prompt reflection on: motivation for dataset creation; dataset composition; data collection processes; data preprocessing; dataset distribution; dataset maintenance; and legal and ethical considerations. The outcome of datasheet creation is better and more appropriate use of data, and the intentional consideration of the implications and logic models the dataset embodies. Datasheet questions that are particularly important to the ethical collection and use of biometric data, plus my commentary, are as follows:

- What preprocessing/cleaning was done? (e.g., discretization or bucketing, tokenization, part-of-speech tagging, SIFT feature extraction, removal of instances, processing of missing values, etc.) *Judicious and non-discriminatory data cleaning is an essential step in making sure models working off these datasets do not compound discriminatory or sensitive characterizations of people.*
- Were there any ethical review applications/ reviews/approvals? (e.g. Institutional Review Board applications) *Beyond protecting citizens, obtaining ethical review approvals helps mitigate legal fillings.*
- Were data subjects told what the dataset would be used for and did they consent? What community norms exist for data collected from human communications? *Understanding and respecting community norms protects against skewed data resulting from collection under duress or discomfort.*
- Could this dataset expose people to harm or legal action? (e.g., financial, social or otherwise)? What was done to mitigate or reduce the potential for harm?
- Does it unfairly advantage or disadvantage a particular social group? In what ways? How was this mitigated? *Explore what funding resources could be made available to subsidize harm mitigation efforts for qualifying partners.*

- *Data User Guides* are another useful tool whose utilization OSTP would be wise to promote across public and private biometric technology organizations.[11] Similar to Datasheets for Datasets, a Data User Guide is a narrative document prepared by data controllers and engineers that addresses key issues anyone working with the data should be aware of.

[11] (Data User Guides, 2015)

Bibliography of References & Recommended Reading

Business for Social Responsibility. (2013). *Conducting an effective human rights impact assessment.* (). Retrieved from https://www.bsr.org/reports/BSR_Human_Rights_Impact_Assessments.pdf

California Consumer Privacy Act of 2018, (2018). TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100

Coglianese, C., & Lehr, D. (2017). Regulating by robot: Administrative decision making in the machine-learning era. *The Georgetown Law Journal, 105*(5), 1147-1223. Retrieved from https://search.informit.org/documentSummary;res=agispt;dn=20191011018318

Contreras, J. L. (2019). Technical standards, standards-setting organizations, and intellectual property: A survey of the literature (with an emphasis on empirical approaches). *Research handbook on the economics of intellectual property law* (pp. 185-235) Edward Elgar Publishing. doi:10.4337/9781789903997.00051 Retrieved from https://www.elgaronline.com/view/edcoll/9781848445369/9781848445369.00051.xml

Data user guides. (2015). Data-User-Guides/README.md

Dombrowski, L., Harmon, E., & Fox, S. (Jun 4, 2016). Social justice-oriented interaction design. Paper presented at the 656-671. doi:10.1145/2901790.2901861 Retrieved from http://dl.acm.org/citation.cfm?id=2901861

General data protection regulation (GDPR), (2018). https://gdpr.eu/

Feathers, T. (2021). Facial recognition is racist. Why aren't more cities banning it? Retrieved: https://www.vice.com/en/article/4avx3m/facial-recognition-is-racist-why-arent-more-cities-banning-it

Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning. (2016). *In the matter of the benefits, challenges, and potential roles for the government in fostering the advancement of the internet of things - docket no. 160331306-6306-01* .

Higher Education Information Security Council. (2021). Higher education community vendor assessment toolkit. Retrieved from https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

Mulligan, D. K., & Bamberger, K. A. (2019). Procurement as policy: Administrative process for machine learning. *SSRN Electronic Journal,* doi:10.2139/ssrn.3464203

Najibi, A. (2020). Racial discrimination in face recognition technology . Retrieved from https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Nissenbaum, H. (2015). Respect for context as a benchmark for privacy online: What it is and isn't. *Social dimensions of privacy* (pp. 278-302) Cambridge University Press. doi:10.1017/CBO9781107280557.016 Retrieved from http://dx.doi.org/10.1017/CBO9781107280557.016

Pope, C. (2018). Biometric data collection in an unprotected world: Exploring the need for federal legislation protecting biometric data. *Journal of Law and Policy, 26*(2), 769.

Ryan, A., & Walsh, T. (2018). *Reflexivity and critical pedagogy*. Boston: BRILL. Retrieved from https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=5570490

S.1214 - 116th Congress (2019-2020): Privacy Bill of Rights Act. (2019, April 11). https://www.congress.gov/bill/116th-congress/senate-bill/1214

Schoechle, T. (2009). *Standardization and digital enclosure*. Hershey: IGI Global. Retrieved from https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=3309560

Selbst, A., Boyd, D., Friedler, S., Venkatasubramanian, S., & Vertesi, J. (Jan 29, 2019). Fairness and abstraction in sociotechnical systems. Paper presented at the 59-68. doi:10.1145/3287560.3287598 Retrieved from http://dl.acm.org/citation.cfm?id=3287598

Solow-Niederman, Alicia & Choi, YooJung Choi & Van den Broeck, Guy “The Institutional Life of Algorithmic Risk Assessment,” 34 BERKELEY TECH. L.J. 705 (2019)

Stevenson, M. (2018). Assessing risk assessment in action. Minnesota Law Review, 103(1), 303.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Palantir

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Suresh Venkatasubramanian
Office of Science and Technology Policy

November 17, 2021

Dear Suresh Venkatasubramanian,

Thank you for the opportunity to respond to the "Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies." Our comments are primarily focused on "(6) *Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case"* from the federal register posting, although we may touch on several points related to other areas of comment.

Palantir Technologies, Inc. ("Palantir") is a U.S.-headquartered software company. We provide enterprise data platforms that enable public and private institutions to integrate, analyze, collaborate, and take action based on their data in a privacy-protective way. We have over 15 years' experience working with governments and commercial organizations on sensitive problems including in areas relevant for this RFI. Our technology is meant to reconcile the need for security with the value of privacy and we reject the notion that there is an inherent tradeoff between security and privacy. Our goal in responding to this RFI is to share best practices we have developed to inform future regulation.

Unlike many tech companies, we do not collect, store, disseminate, sell, or otherwise monetize customer data. We make software to help some of the most critical organizations around the world to make better use of the data they already lawfully possess or access.

Palantir operates on the conviction that it is essential to preserve fundamental principles of privacy and civil liberties while using data. We believe that well-designed technologies can dramatically enhance security without undermining the rights and freedoms of individuals. Our work strengthens national security while supporting constitutional privacy protections.

Upholding these principles means integrating new technologies for processing data responsibly. Our experience working with a broad range of public and private sector organizations has continually reinforced our position that there are both responsible and irresponsible ways of using sensitive data and algorithms. This insight applies as well to biometrics and facial recognition.

To be clear, Palantir does not collect or hold facial recognition data, it does not build facial recognition algorithms, nor does it hold any direct stake in the adoption of this technology. To the contrary, we believe that there should be limits placed on the use of such powerful technologies, including restrictions on their use for programs that could be construed as mass surveillance. Narrowly circumscribed applications based on appropriate legal authorities and integrating critical privacy-preserving safeguards may present more defensible use cases. As a company that provides data integration platforms, we view facial recognition data as one of several sensitive classes of biometrics data that may — under the right conditions and with appropriate controls— be used in direct, stand-alone form or as integrated into a more

generalized information or analytics environment. In either case, we believe technological capabilities coupled with procedural controls show that a more prescriptive approach to facial recognition regulation can achieve both security and privacy goals. We believe that sharing these principles and best practices will help empower organizations and regulators to effectively regulate facial recognition technologies.

The suggestions included in this document are primarily intended to apply to the use of facial recognition systems for specific security applications, but many of the same ideas may apply to other potential uses of facial recognition and even other biometric technology applications. That said, a critical consideration to call attention to up front is that determining the appropriateness of facial recognition use is indeed a context-dependent exercise and requires a concrete outline of the conditions of use in order to make a clearer assessment of the attendant privacy and civil liberties risks, as well as adequacy of mitigating measures.

Recommendations

Limiting Facial Recognition Technologies

This submission proposes principles that impose technological limitations for facial recognition systems used for security provision. We believe that policies can direct the intelligent design and application of these systems to capture the essential security utility of facial recognition technologies whilst achieving what we term *engineered ephemerality*. That is the notion that non-suspect individuals should be able to pass by facial recognition systems with minimal consequence or no trace at all.

By ‘facial recognition technologies’ we refer to those systems that attempt to *a)* detect human faces that appear in still imagery and video footage and *b)* attempt to derive the unique geometry of detected faces and *c)* match derived facial geometric data against previously obtained target data held within databases. Though there may be other operational definitions of facial recognition technologies, we believe this definition will cover the majority of applications in the security context.

Technical measures alone are insufficient to ensure the safe use of facial recognition technologies. The measures suggested here are intended to compliment, not replace, governance mechanisms such as limiting the purposes for which such technologies can be employed, establishing oversight bodies, and acting transparently to ensure that the affected public is informed about programs and environments using facial recognition systems.

We are primarily responding to the use of Facial Recognition for use in the physical security of a sensitive facility or at an international border crossing. By contrast, we do not believe that indiscriminate use in contexts that could construed as mass surveillance, even if all these guidelines are followed, would be justifiable or warranted.

In addition, we advise heavy skepticism with regards to the use of biometric technology, including processing of facial features, in systems that purport to identify a person’s interior

states, such as their emotions, thoughts, or intentions, as well as its use in job hiring or other social recommendation scenarios.

Obfuscation By Default

Facial recognition technologies present a challenge to 'practical obscurity' as a traditional privacy protection. In the absence of machine-assistance, facial detections are the product of human observations and cognitive faculties with all the benefits and limitations of vision, memory, attention, etc. Facial recognition technologies enable augmented or fully automated detection and identification of faces. While for certain institutions, the prospect of more expansive surveillance can foster valuable security protections, an uninhibited approach can lead to significant and alarming privacy intrusions.

Facial recognition systems can, however, be engineered and configured to mitigate privacy concerns by using the same technology that enables facial detection to automatically obfuscate or blur detected faces to system users.

We propose that facial recognition systems should implement an 'obfuscation by default' paradigm that obfuscates (blurs) imagery exposed to end users for both unidentified faces and known faces that do not trigger an alert or other appropriate viewing threshold. In other words, unless there is a reason, faces should not be visible to system users. When there is a reason to allow viewing of faces, authorized users should operate under proportionately granted, auditable access controls that limit viewing of faces in an appropriate way.

Obfuscation by default ensures that any imposition on privacy is appropriately proportionate with the end-users' authorized objectives while minimizing casual browsing of imagery and potential privacy intrusions. Faces that require identification as a legitimate part of a security investigation or other appropriate use case could be unmasked by an explicit user action with associated reason justification recorded (more on this below).

Limiting data collection

In one of the most common applications, facial recognition systems attempt to match the facial geometry of newly encountered individuals against previously collected facial geometry data stored within databases. We term the list of individuals whose facial geometry data populates these databases *seed lists*. Management of seed lists must be robust. That is, the objective should be to keep these lists as short, current, and reliable as possible, proportionate to legitimate security needs.

The addition of data to, or the removal of data from, seed lists should require and document explicit justifications. Seed list alterations and their associated justifications should follow an established policy and be subject to oversight.

Seed lists should be subject to mandatory review and reconfirmation of their 'membership' at reasonable and regular intervals. We suggest that every six-months is a reasonable schedule for these reviews (though alternative retention periods may apply, depending on the context). The

default assumption for these reviews should be that, unless specific evidence justifies the continuing inclusion of an individual on a seed list, the individual should be removed.

Limiting Data Retention

Ensuring that data generated by facial recognition systems is deleted after an appropriate period of time is essential to achieving 'engineered ephemerality'.

If a facial recognition system encounters an unknown face (a face that does not match any of those in relevant seed lists), then biometric data concerning this unknown face should be subject to limited retention or immediate deletion. This prevents unnecessary data aggregation on non-suspect individuals, allowing them to pass by facial recognition systems leaving minimal or no trace.

If a facial recognition system returns a match against an individual on a seed list, then a record of this match (including metadata such as time and location) should be made and stored for a moderate period. We suggest that one month would be a reasonable default retention period for this set of records. During this period, human analysts can review the possible match to determine if it was accurate and significant.

If a match passes these checks, then it can be elevated to a third, longer retention category. The retention period of this category should not be unlimited but should be calibrated with reference to the laws and best practices relevant to the defined mission that the data is intended to serve.

Limiting System and Data Access

Access to the processes and data of facial recognition systems should be governed by granular *access controls*. This means that users should be able to discover, view, process, edit, and delete sensitive data only to the extent that their responsibilities and roles demand. Data from video capture and facial recognition technologies should not be available indiscriminately across an organization.

Granular permissions preventing unauthorized access should be applied to all levels of system interaction, including but not limited to:

- Viewing the imagery that facial recognition systems analyze (e.g., CCTV feeds)
- Viewing seed lists
- Editing seed lists
- Viewing facial recognition matches
- Viewing maps and schematics identifying location of facial recognition capture devices
- Deleting system data
- Escalating retention periods
- Viewing audit logs

Selective Revelation with Purpose Justifications

Facial recognition systems should include mandatory documentation of user justifications for key actions undertaken, including but not necessarily limited to:

- De-obfuscating an obfuscated (i.e., blurred) facial image or detection
- Adding data to a seed list
- Removing data from a seed list
- Extending retention periods for data within a seed list
- Ad-hoc searches against a facial geometry database
- Exporting data

Justifications provided by users can take multiple forms, but we recommend pre-determined justification categories formulated with the support and review of appropriate oversight authorities and codified in system usage policies and guidelines. In other applications, it may be appropriate for users to provide case number or other critical reference details in addition to or in lieu of category or free-form text justifications.

Facilitating Oversight

A thorough audit log of all significant user actions within the system should be maintained. This allows those responsible for system oversight to detect and investigate illegitimate user behavior and to hold users accountable for actions undertaken within the system.

Audit logging capabilities should be sufficiently detailed and accessible to determine whether individuals are misusing data by inappropriately accessing information, conducting overly-broad searches, deliberately or inadvertently entering erroneous information, sharing or exporting information without authorization, or engaging in other activities that could lead to serious violations of privacy and civil liberties.

At a minimum, audit logs should include details regarding the specific user, user action in the system, corresponding metadata (e.g., date/time), data elements the user action exposes or interacts with, and (where appropriate) justifications provided by users to carry out specific actions.

Audit log analysis applications for the facial recognition system used in this example physical security context should be developed and made available to oversight bodies that allow these bodies to identify inappropriate use, analyze audit logs at scale, and highlight anomalous or concerning behavior. Raw and uninterpretable logs will not allow oversight bodies to protect civil liberties in the proper context.

Data and Algorithmic Quality

The history of facial recognition systems is rife with examples of applications beset by poor accuracy and systemic unfairness. These outcomes are unacceptable. Proper control over facial

recognition use is not sufficient if the facial recognition systems themselves have or propagate unwanted biases.

Evaluations of algorithmic performance across a range of different identity groups, demographic backgrounds, dress conditions, disabilities, and other physical variations must be conducted before a facial recognition system goes live, as well as continuously throughout the lifecycle of the system. Test images should be representative of actual deployment scenarios including lighting, camera placement, and image quality. Minimum acceptable standards should be established in advance, and these standards should accord with the potential for harm resulting from false-positives in any given use case.

When a system returns a match, it should also return a well-specified 'confidence score' assessment that conveys the confidence the system has that this match is not a false-positive.[1] This match should be visually apparent and prominently displayed to the end-user. If the confidence score does not meet a defined threshold, then the image match should not be displayed to end-users.

Systems should have an embedded capacity for manual correction and improvement. When an end-user identifies a false-positive or a false-negative, the system should allow the end-user to correct such high-impact errors. In the case of a false-positive, the correction should remove the association between the falsely matched person (or object, if the system has identified a non-human entity as a face) and the video footage. All corrections should be clearly recorded in the audit log. Corrections may also feed back into the underlying facial recognition software to improve training and reduce error rates over time as well as flag disparate impact on an impacted population.

Training data oversight

Data used to train facial recognition algorithms, as well as data used to test those algorithms' efficacy in potential application scenarios, should be collected according to principles of transparency and explicit consent of the individuals represented by the data. More directly, implied or non-explicit consent (e.g., opt-out requests buried deep in the bowels of Terms and Conditions should not be allowed). Similarly, images captured and tagged for one consented use should not be freely repurposed for the development or training of facial recognition algorithms or systems without additional explicit consent from subjects of the images.

---

[1] Confidence Score' is intentionally under-defined. We leave it as a matter for later, context-specific determinations about the question of how confidence scores are designated, recognizing that there are a plethora of facial recognition evaluation metrics and algorithm evaluation standards that have been elsewhere articulated and that can be used individually or in composite form for "confidence" representations along the above lines. The critical points here are that a) confidence scores should be defined and agreed upon by appropriate oversight authorities, b) how those scores are defined and were determined as the appropriate metrics should be plainly documented, c) scores should be evaluated and consistently displayed in practice and in regular system use.

Preserving the Role of Human Judgement

Finally, decisions that can impact an individual's freedom should not be left to exclusively to software. Facial recognition systems and processes should be designed to augment rather than replace the decision-making capability of human analysts. A human capable of spotting false-positive matches should be the decision-making endpoint in any facial recognition-facilitated operation. Analysts should undergo training to allow them to better understand the weaknesses of automated systems (as well as their own inherent biases) to identify errors, the role of both human and system bias, and to interact with the system in a responsible way.

Conclusion

Facial recognition has great potential for enabling meaningful and constructive security outcomes but must be evaluated against privacy and other social costs attendant to its use. We firmly believe that better security that leverages facial recognition and other biometric technologies need not come at the expense of privacy and civil liberties. This submission proposes several technical and administrative limits on facial recognition systems used for security. We assert that these limits are feasible and should be considered as part of future regulation. We welcome further discussion with OSTP on this proposal.

Sincerely,

Anthony Bak, Head of AI Implementation, Palantir Technologies
Courtney Bowman, Global Privacy and Civil Liberties Lead, Palantir Technologies

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Pangiam

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500
BiometricRFI@ostp.eop.gov

RE: RFI Response: Public and Private Sector Use of Biometric Technologies

Pangiam offers the following response to the Office of Science and Technology Policy's (OSTP) request for information, "Public and Private Sector Uses of Biometric Technologies" (Biometrics RFI).[1] Pangiam is a national security software and technology company applying computer vision to define the future of trusted movement and security. We are revolutionizing the future of operations, security, and safety at airports, seaports, and land crossings using emerging technologies. Our technology and expertise in computer vision and artificial intelligence (AI) is world leading, as recognized by organizations like the National Institute of Standards and Technology (NIST). Our facial recognition algorithm recently achieved a top three ranking in the NIST Face Recognition Vendor Test 1:N Identification and was ranked the fastest in the world by NIST's most recent 1:1 test.

We are also experts at deploying biometric technology for identity verification in a variety of trade and travel use cases, working in partnership with both other private sector entities and government. In the private sector, Pangiam's technology is

[1] OSTP, Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 FR 56300 (October 8, 2021) (hereinafter, "Biometrics RFI").

trusted and used by 42 airlines. For government, Pangiam developed the U.S. Customs and Border Patrol's cloud-based facial biometric matching service, known as the Traveler Verification Service. In a collaborative effort, Pangiam is providing the biometric technology that enables a partnership between Delta Airlines and the U.S. Transportation Security Administration for bag drops and security checks at Delta stations across the U.S. We are, therefore, uniquely positioned to respond to the Biometrics RFI on the real benefits and potential harms of biometric technology for identity verification.

Pangiam employs an industry-leading rigorous governance program to ensure the accuracy, efficiency, and security of our technology and build trust with clients and the users of our technology. Our company, like many others, has expended private resources to develop artificial algorithms with the highest ethical standards. As federal entities like OSTP and the National Artificial Intelligence Initiative consider policies to ensure U.S. leadership in AI, we propose two key recommendations to ensure the ethical advancement of biometric technology and keep the U.S. competitive with international competitors. Our first recommendation is to provide private companies access to government datasets to train their algorithms and, second, for the U.S. government to leverage technical safeguards and policy incentives to ensure ethical AI development by the private sector.

Benefits and Harms

The use of biometrics in the trade and travel domain offers several key benefits to create operational efficiencies, increase the security and safety of air travel, and

improve the traveler experience. First, biometric identity verification automates manual human processes which reduces labor costs and errors caused by fatigue. This automation verifies passenger identity more quickly than manual processes, cutting time for processes like boarding almost in half, reducing potentially costly late departures and allowing for growth of aviation operations within existing infrastructure constraints.[2]

Second, identity verification in travel is the cornerstone of aviation security. Using biometric technology to verify a passenger's identity increases the security of travel as algorithms outperform humans in identifying imposters.[3] From a safety perspective, at several points in a passenger journey the passenger physically exchanges documents to verify their identity. Biometric identity verification is contactless, reducing the potential points of transmission for viruses and enabling physical distancing at otherwise crowded chokepoints.

Beyond these benefits, travelers are open to using biometric technology to reduce the time they spend being "processed" during travel. The International Air Transport Association's 2021 Global Passenger Survey, found that passengers want to use biometric identification if it expedites travel processes, with 86% of passengers

[2] https://www.flydulles.com/news/emirates-deploys-one-step-biometric-boarding-dulles-international-airport-veriscan-1

[3]https://www.nist.gov/system/files/documents/2021/05/12/frgc_face_recognition_algorithms_surpasshumans.pdf

that had experienced biometric technology during their journey satisfied with the technology.[4]

The trade and travel use case for facial recognition is often confused with ubiquitous surveillance and law enforcement use cases. Our use case is narrow, explicitly used to facilitate the movement of people and goods. Despite this narrow application, there are still instances in which the companies developing this technology could cause harm. First, is in the development of algorithms. The size and quality of datasets used to train algorithms could cause disparity in performance across different demographics. Without high performance across all demographics, the facilitation and efficiency benefits for large, diverse populations such as the traveling public are lost.

Second, it is costly and time consuming to acquire large and diverse datasets, which has led some organizations to blur ethical and legal lines in acquiring them. Additionally, poor data security and data protection practices can leave biometric information vulnerable to nation-states, hackers, or even the highest bidder through third party sales. In a recent example, one company improperly harvested customer data through deceptive methods, training its algorithm on a consumer-facing application designed to acquire dataset images without informing the consumer. Further, consumer data was retained indefinitely even after accounts were

[4] IATA - Global Passenger Survey (GPS), 2021.

deactivated. This is just one example, but many more exist and will continue to so long as these datasets remain a barrier to development.

Maintaining the U.S. Lead in Trustworthy Algorithms

Pangiam has proactively adopted its own Biometrics Principles in order to fully realize the benefits and neutralize the potential harms of this rapidly advancing technology. From data sourcing and acquisition to deployment, Pangiam's industry-leading principles protect the integrity of the technology and process against malfeasance and abuse. While our company has adopted this policy voluntarily, if not properly regulated, biometric technology has, like all technologies, the potential to be misused. If the U.S. is to maintain its lead in trustworthy artificial intelligence research and development, it must promote the adoption of rigorous ethical behavior for biometric technology in the private sector.

U.S. federal initiatives and policymaking to promote this ethical behavior must start with how algorithms are developed. In this first stage, private companies must acquire or create datasets for algorithms to be trained on. This is a costly, time-consuming step that has already led to many examples of unethical shortcuts in the industry, breaching legal agreements and eroding the confidence of the American public in AI. Access to government biometric datasets would speed the development of trustworthy U.S. algorithms, leapfrogging U.S. companies past this initial barrier to development.

Internationally, governments are already sharing their datasets with their private sector to help advance AI performance. In our closest competitors, this

sharing is a key reason for the rapid advancement of their capabilities, but few, if any, ethical guardrails are required for companies to access to billions of images. In the U.S., access to government datasets can be done in an ethical fashion with technical safeguards and policy incentives. Technical safeguards, such as training algorithms behind a firewall, can ensure companies only have access to results rather than the underlying data. Policy incentives, such as requiring ethical corporate behavior either by audit, pledge, or other disclosure, can ensure that only responsible companies that abide by an ethical code of conduct can take advantage of this resource.

The U.S. government is already sharing data with the private sector for AI development. The National Geospatial-Intelligence Agency (NGA) shares geospatial data with the private sector to help the agency solve some of its current AI challenges and employing advanced algorithms. NGA takes its engagement with the private sector a step further and runs an accelerator to grow the number of advanced solutions available to NGA. The Pentagon's Joint Artificial Intelligence Center uses the Joint Common Foundation, a cloud-based platform that enables users to access Defense Department data and develop AI solutions in a secure environment. These are just two examples, but there are more that could be leveraged as a model for sharing datasets with the private sector for training facial recognition algorithms.

The U.S. government has a responsibility to its citizens to ensure the ethical development and use of AI. Federal agencies have their own requirements for data access, but facial recognition requires the highest ethical corporate behavior.

Pangiam offers the following principles for consideration as ethical requirements for U.S. companies to access federal datasets for training facial recognition algorithms.

- **Data Transparency**. Regularly and publicly communicate how information is stored, transmitted, and accessed, and the privacy policies governing biometrics use simplified, easy to understand language;
- **Opt-In Databases**. Travelers to affirmatively opt-in to biometric collection;
- **Opt-Out Operations**. Areas where biometrics are captured are clear and obvious and an operational policy for those who opt-out is deployed;
- **Privacy-by-Design**. Systems are designed and implemented that protect the privacy of the traveler;
- **Security Safeguards**. Use encryption and biometric algorithms whose face templates cannot be reverse-engineered to identify a traveler;
- **Performance and Accuracy**. Use only biometric algorithms that have the highest rates of accuracy and precision as determined by The National Institute of Standards and Technology;
- **Domestic Development**. Algorithms are developed in the U.S.;
- **Ethically-sourced Datasets**. Datasets are ethically and legally sourced and contain a wide range of demographics to reduce bias;
- **No Third-Party Sales**. Prohibit the sale of biometric and biographic information to third parties; and

- **A Track Record of Trust**. Organizations that are known or found to have abused customer privacy, misled consumers, or insufficiently protected data are excluded from accessing government datasets.

While ethical behavior by the private sector is paramount to developing trustworthy AI in the U.S., any federal effort to verify the desired corporate behavior must keep in mind the speed at which biometric technology is being developed worldwide. In order to maintain a competitive edge against global competitors, this ethical verification effort cannot be so cumbersome for the private sector as to inhibit innovation and therefore counterproductive to the U.S.'s overall aim at leading AI research and development. In the same vein, any technical safeguards must not be so complex as to prohibit the ability of an ethically-verified company to use the dataset.

Beyond incentivizing ethical behavior, access to government datasets would address a key cause of inconsistent performance across different demographic groups or "algorithmic bias." There is an overrepresentation of Caucasian images in many public and private datasets and, when algorithms are trained on datasets that lack diversity, it leads to bias in facial matching of underrepresented groups. Pangiam is committed to eliminating bias in its facial recognition models and we already strive to train our models on datasets that have equal representation across gender and ethnicity. We do this because of our strong ethical principles, and this diligence results in better parity of performance across demographic groups. The U.S.

government can help the private sector writ large produce higher performing models with access to diverse government datasets.

Ultimately, we believe this Biometrics RFI is the beginning of an important dialogue between the private sector and OSTP. Pangiam welcomes the opportunity to participate in further policy discussions to ensure that biometric technology in the U.S. is developed ethically and enables the U.S. to maintain its global competitive advantage.

Respectfully submitted,

Shaun Moore
Chief Artificial Intelligence Officer
Pangiam
[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Parity Technologies

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: Liz O'Sullivan
Chief Executive Officer
Parity Technologies, Inc.
[redacted]

January 15, 2022

To whom it may concern,

Response to White House Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies - 86 FR 56300

The team at Parity welcome this opportunity to share our years of experience working with and within enterprise AI teams to mitigate AI-driven risk factors across multiple industries.

While it's certainly true that the use of biometrics has expanded dramatically alongside the growth of AI in the last few decades, concern about biometric data abuse is by no means a new phenomenon. These concerns are easy to understand, given the nature of the technology itself. Biometric measurements are all but useless if they are mutable, meaning that the collection and retention of this data grants often irrevocable power to the collector over the subject.[1] In modern times, many of our most sensitive, immutable characteristics are up for grabs, including our very DNA[2].

DNA provides a perfect example of how biometric data can be abused during the gaps between technological progress and appropriate regulation. In 2017, in order to investigate a murder, NYPD officers set up a "stop-and frisk" DNA dragnet in Howard Beach, targeting Black and Latinx people exclusively.[3] In New York, the police operate a DNA database with no oversight, which has been ruled illegal, and yet it continues to operate in obscurity[4]. DNA is particularly problematic because there is absolutely no way to change its nature in our bodies, no way to avoid collection, and its collection implicates your family relations for identification in addition to your own.

But other technologies, mostly powered by AI, have had the spotlight for the last few years. This should also not be surprising, given the implications of horrific privacy abuses

[1] AI Now Institute, "Regulating Biometrics: Global Approaches and Urgent Questions", Sep 1 2020, <https://ainowinstitute.org/regulatingbiometrics.pdf>.
[2] Federal Bureau of Investigation, "Frequently Asked Questions on CODIS and NDIS", <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet>
[3] Ransom, M., Southall, A. "Race-Biased Dragnet': DNA From 360 Black Men Was Collected to Solve Vetrano Murder, Defense Lawyers Say", *New York Times*, March 31 2019.
[4] Durkin, E., "New York City said it would purge its DNA database. A year later, it's expanded.", *Politico*, 23 Feb 2021.

that allow brute force identification of anyone with a social media profile, as is the case with Clearview AI, from a distance, adding further fuel to the privacy debate[5].

If you find yourself in a state-run database today, there is no recourse. No notification of your enhanced exposure to investigative risk. No way to remove yourself from the database. And no way to know that the reason police regularly stop by your home is, in fact, due to a case of mistaken identity that may or may not show up in court should this charge ever come to trial.

The White House effort to create a bill of rights on this topic is salient here, where the basic right of presumption of innocence have been transformed in this data-driven age. There are many such basics which have been largely ignored by the Silicon Valley pursuit of "disrupting" our justice system[6]. Given our existing legal framework, it can be clearly argued that people have a basic human right to know whether they are in such databases, have the right to correct that information or be removed, and to know whether technologically-driven identification played a role in their charges. We hope that the forthcoming bill of rights will sufficiently address these "table stakes" necessities as a starting point for regulating this technology.

Question 1:

Unfortunately for civil liberties around the world, one of the best places to assess the current state of biometrics technology is by way of our own Department of Defense. Their laundry list of RFIs and research on the topic range from facial recognition[7] to heart-rate identification by long distance laser[8]. Many investments cover biometric technologies, which are fundamentally flawed from scientific and human rights perspectives.

One recurring and contentious example is emotion recognition. The likelihood of a person experiencing certain families of emotions may only be weakly estimated, even under highly invasive conditions where many simultaneous biometrics are measured.[9] However, these conditions do not translate to real world use cases, can be gamed by

[5] Hill, K. "Unmasking a Company that Wants to Unmask Us All", *New York Times,* Jan 20 2020.
[6] For instance, consider predictive policing products which assign different likelihood of criminal guilt based on an individual's location.
[7] Department of Defence, *Advanced Tactical Facial Recognition at a Distance Technology*, <https://www.sbir.gov/node/1188789>.
[8] Hambling, D, "The Pentagon has a laser that can identify people from a distance—by their heartbeat", *MIT Technology Review,* June 27 2019.
[9] Shu L, Xie J, Yang M, Li Z, Li Z, Liao D, Xu X, Yang X. "A Review of Emotion Recognition Using Physiological Signals" *Sensors*. 2018; 18(7):2074.

humans[10], and are subject to enormous diversity of emotional expression across cultures and backgrounds.

This failure persists in spite of enormous advancements in signal and image processing, which suggests that useful forms of this technology are unlikely to ever work. Investment in unreliable emotion recognition technologies is investment in scientifically flawed decision making, but this fallibility has done little to dissuade Silicon Valley from pressing forward with funding for startups[11]. Should it ever arise that a technology can reliably infer emotional state from a video feed, many would argue that the implications of this technology are themselves far too dangerous for their potential impact on freedom of thought to ever be responsibly deployed. These implications are hardly hypothetical, given the history of technology companies eager to commercialize bleeding edge technology, well in advance of its scientific vetting.

Modern biometrics as a field has undergone significant scope creep from its early goal of fighting crime[12]. Currently, biometrics data can be clandestinely used in consumer applications, including advertising use cases, snapping photos to classify subjects into categories based in part on their protected classes to personalize web experiences, or as is also proposed, dynamic ads along a smart city street[13].

This scope creep neglects entirely the preferences of people for whom their demographic identity poses active risk. Those from the transgender and disability community may not feel at ease when this information lives on a corporate server, outside of their control. Moreover, this information can pose such individuals true and pressing risks, like being outed to a family member or employer.[14] A world with ubiquitous, persistent, and obscured demographic identification is one full of danger for marginalized communities—lest we forget that in our not-too-distant past, queerness was considered being ill, and continues to be prohibited by law in many places around the globe.

As experts in AI, we can categorically state that many of the technological approaches to inferring demographics are riddled with stereotypes. Training data for a model concept called “female” is likely scraped from social media, where femininity is often performed as

[10] Pokrovskii, V, Polischuk, L. “On the conscious control of the human heart” *Journal of integrative neuroscience*. (2012); 11:213.
[11] For instance, Affectiva’s acquisition for 73.5M
[12] “One of the earliest attempts to use biometric data for identification dates back to the 1880s when the French criminologist Alphonse Bertillon proposed a method based on anthropometric measurements.” - Arbab-Zavar, B., Wei, X., Bustard, J., Li, C. “On Forensic Use of Biometrics”, in *IEEE Handbook of Digital Forensics of Multimedia Data and Devices*, 2015, pp.270-304.
[13] Alfi, “Facial Recognition Advertising: The Future Is Here”, <https://www.getalfi.com/advertising/facial-recognition-advertising-future-is-here/> July 23 2021.
[14] Scheuerman, M., Paul, J., Brubaker, J. “How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services”, *Proceedings of the ACM on Human-Computer Interaction*. 2019. 3. 1-33. See, especially, section 6.1.4.

fashion and makeup, and this stereotype trickles down into the models themselves.[15] Most of these models fail entirely to attempt to infer gender identities outside of the traditional gender binary, thereby erasing a growing cohort of Americans along the gender spectrum entirely.

In the "move fast, break things" modality of Silicon Valley, far too often products are designed only for the mean/majority and released without testing on our nation's most vulnerable. In particular, there is a vast lack of thoughtful research on how biometrics models function on those with visible disabilities (such as the blind and autistic communities)[16]. Unilaterally exposing these people to enhanced risk of false arrest stands at odds with our claimed moral high ground of judicial objectivity, and is decidedly un-American.

Question 2:

Because the Parity platform enables multi-stakeholder design and evaluation of proposed artificial intelligence models across multiple industries, we are empowered to speak comprehensively about the challenges in validating such activities. We emphatically state that validation methods must differ among applications of the technology, rather than the simple design choices inherent in the technology itself.

The rationale is simple – the acceptable error rate for a law enforcement application must substantially differ from that of an advertising use case, and our current anti-discrimination laws make virtually no mention of acceptable rates of variance among protected classes. In its current form, the NIST facial recognition benchmark demonstrates some of the most egregious problems in existing test methodologies – neglecting the context and application of the technology for a "lab-conditions" test that involves facial photos of prisoners in their mugshots.[17] Whether these accuracy rates transfer to real world applications is debatable. In artificial intelligence, we call this the problem of "domain adaptation", wherein a model is trained for one thing and applied to another.[18] Put simply, NIST's lab conditions accuracy rates may not at all translate into applications in the real world. When applying this problem to a use case that involves someone's access to freedom, this nuance must be taken into account. Important to note here is that NIST's evaluation tactics model entirely the kind of data stewardship this bill

[15] Steed, R., Caliskan, A., "Image Representations Learned With Unsupervised Pre-Training Contain Human-like Biases", *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. 2021. 701-703.
[16] For instance, the facial expressions of autistic people may be less expressive in general than non-autistic people
Trevisan, D., Hoskyn, M., Birmingham, E. "Facial Expression Production in Autism: A Meta-Analysis: Facial Expression Production in Autism". *Autism Research*, 2018, 11.
[17] Here, we are referring to the NIST Mugshot Identification Database (MID)
[18] Mei W., Weihong D. "Deep visual domain adaptation: A survey", *Neurocomputing*, 2018, 32.

of rights should strive to prevent, by collecting and exploiting prisoner mugshot data, devoid of any meaningful consent.

Moreover, NIST's assertion that a "one and done" analysis of accuracy should suffice is worryingly naive. Seasoned data scientists understand that even if your model is static, the world can change around you, resulting in a phenomenon known as "concept drift"[19]. If makeup fashions change, or monocles become in vogue, facial recognition would have a much harder time identifying these individuals. A world with algorithmic rights requires a commitment to continuous testing and reduction of bias among intersectional protected classes. Testing data must be appropriately curated in order to surface the nuances of minority populations[20]. The current status quo is one of randomized testing, which ignores that resulting harms most often disproportionately fall on insufficiently represented communities. People should have the right to know that any justice-related product in use, or even one whose data may show up as evidence in response to a subpoena, has been vetted against their individual demographics, or should not be used at all.

Questions 4 & 5

All too often, when discussing biometrics, the public is presented with a misleading black or white choice: expose yourself to the risk of crime or loss of liberty, with no mention of the grey scale in between. In attempting to regulate biometrics effectively, careful attention must be paid not to blind ideology, but instead to the pragmatic trade-offs inherent in the application.

To claim that biometrics usage fails to mount a persuasive application is to ignore the usefulness of the technology in identifying lost children, mentally ill patients, and missing persons. This very same technology is undoubtedly at work incarcerating innocent people of color, without their knowledge or ability to appeal[21]. Many have claimed that the fault lies not in the technology itself, but in the overwhelmingly insufficient legal frameworks to prohibit one and allow the other. This should not be taken as an argument against forms of abolition, but instead an opportunity to locate the source of harms and restrict those effectively.

---

[19] Leslie, David. Understanding artificial intelligence ethics and safety, 2019. <https://www.turing.ac.uk/sites/default/files/2019-08/understanding_artificial_intelligence_ethics_and_safety.pdf>.

[20] Kearns, M., Roth, A. "Ethical algorithm design should guide technology regulation", *Brookings Institute,* Jan 13 2020, <https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation/>.

[21] Angwin, J., Larson, J., Mattu, S., Kirchner, L. "Machine Bias - There's software used across the country to predict future criminals. And it's biased against blacks.", *ProPublica,* May 23 2016.

Some members of Parity's staff have been involved in local efforts to abolish facial recognition as a law enforcement tool, but they may also enjoy the hands-free benefits of iPhone face unlock. If the United States conferred sufficient protections against data abuse, her residents may be able to enjoy these benefits without worry. As it stands, however, the people deciding when and how this technology is used are the billionaire technology CEOs and their VC backers, whose primary responsibilities are to their shareholders, often at the expense of our Constitutional rights.

Without this profit-driven, ideological risk, we may still find that there are spectra of benefits and costs to this emerging technology. In the not-too-distant past, many forget that even our most basic ability to browse the internet today is one that frustrated 90's kids to no end – the vastness of available content on the internet created a wild west experience, where undesirable content could easily find itself in front of children's eyes. Many of the positive applications of biometric data invoke child predation as a crime worthy of any and all interventions that might bring about justice. Indeed, a world where every uploaded photo is scanned for known criminals may seem appealing to a mourning parent. But we cannot ignore that this benefit comes at an unacceptable cost, namely the installation of an easily-abused national surveillance network of all our private communications. Nor can we ignore that computer vision technology, a main offender in biometric privacy, is inherently ineffective on categories it hasn't been trained to identify. This leaves anyone in a minority identity group at the mercy of high error rates that could rob them of their freedom.

Similarly, we can not ignore the clear benefits of wearable health devices such as fitbit or Apple Watch, whose "Fall Detection" features enable great freedom for people suffering from epilepsy or heart conditions[22]. Unfortunately, this same technology has also been quietly patented by Apple for identifications of an individual[23], yielding yet another "accidental" national surveillance network, just a subpoena away. In recent years, other forms of biometric identification that involve walking patterns and digital behaviors have been claimed effective at identifying pre-crime mental states. That there is no evidence to support this claim will do little to deter the influx of Silicon Valley money to build it. It is only with greater legal protections that divide and exclude our health and biometric data from police intrusion entirely that we can safely enjoy these benefits.

Question 6:

The Parity platform offers enterprises a modern format for multi-stakeholder design of algorithms, powered by multiobjective optimization. Our platform is tailored to specific

[22] For instance, see the FallCall Detect app, available on the Apple Store
[23] Apple's patent application can be found here. See the following for a breakdown
Zibreg, C. "New Patent Details "Wrist ID" Authentication for Apple Watch", *MakeUseOf,* Jan 12 2021. <https://www.makeuseof.com/apple-watch-wrist-id-patent/>

use cases in healthcare, employment, insurance, and finance. And while we will largely decline to work with vendors engaged in biometric surveillance on principle, we would be happy to engage with the White House in a less-public venue to discuss the existing shortcomings of validation techniques in desperate need of modernization. For years, the industry has cried out for a lack of standardization and best practices for AI validation, but this period of maximal uncertainty is drawing to a close, where the ability to predict failure modes of algorithms becomes more stable every day. It is long past time that we agreed as a society that "the algorithm did it and we don't know why" ceases to be an acceptable excuse for quantifiable harm.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Patrick A. Stewart, Jeffrey K. Mullins, and Thomas J. Greitens

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

To: Office of Science and Technology Policy (OSTP)
Re: OSTP Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.
Date submitted: January 5, 2022

Comments on use of biometric technologies for inference of individual mental and emotional states: Facial Expression Analysis (FEA)

As Artificial Intelligence (AI) increasingly becomes part of everyday life, the opportunities and potential perils posed by using these new technologies are most elevated during the early stages of adoption and implementation. Because the critical decisions concerning how a technology is used affects its development and application, and occur during the early stages of scientific discovery, we welcome the OSTP's efforts to create a "Bill of Rights for an Automated Society." More specifically, we embrace the invitation to comment focusing on the opportunities and threats posed by Facial Expression Analysis (FEA).

FEA technology offers to revolutionize the study of human behavior and is thus an exciting tool for social and psychological scientists to add to their toolbox. However, there are multiple evidentiary reasons to proceed with caution, and to consider regulating the use of FEA in hiring, workplace, and education practices; perhaps more importantly, we advise careful consideration of FEA use in the criminal justice system where the powerless have little recourse when technology is misused. The primary point of this comment is that the theory driving how FEA is used and marketed is flawed and threatens to exacerbate current societal inequities. This is especially the case with videoconferencing becoming a ubiquitous part of everyday life and providing digital intimacy via a mediated face-to-face setting (*1*). In what follows, we provide information requested regarding: *RFI-4.* Exhibited and potential harms of a particular biometric technology, focusing on *4.a.* harms due to questions about the validity of the science used in the system, specifically questions regarding the inference process, and *4.b.* harms due to disparities in the effectiveness of the system for different demographic groups. We then discuss policy implications in light of historic management practices and privacy concerns.

Potential harms from Facial Expression Analysis due to validity of inference process

The societal threat posed by the unquestioning acceptance of FEA may be seen as similar to one experienced with the now century-old polygraph. These so called "lie detectors" entered into the popular culture with the expectation that deception could be unerringly identified based upon psycho-physiological indicators being measured and analyzed during questioning. More specifically, respiration, heart rate, blood pressure, and galvanic skin response (GSR - electrodermal response [EDR] in which sweat on the skin's surface is measured) are used to compare physiological indicators in responses to control and the relevant questions (*2*). Claims regarding the "truth telling abilities" of 90% or better for polygraph lie detection continue to be made regardless of a report by the National Research Council (NRC) in 2003 (*2*) and an update in 2019 by Iacono and Ben-Shakhar (*3*) that this assertion greatly overstates its efficacy. To quote the NRC regarding the persistence of the myth of polygraph accuracy "… practitioners have always claimed extremely high levels of accuracy, and these claims have rarely been reflected in empirical

research" (2003, p. 107) with Iacono and Ben-Shakhar concluding: "Fifteen years later, the landscape has not changed: The panel's conclusions still stand" (2019, p. 96).

With the polygraph still being used in the criminal justice system by state and local law enforcement agencies, in the court system, and by private businesses in the interview process, as well as its continuing cachet as proof of guilt or innocence for political and public figures, the persistent myth of its infallibility is instructive for FEA. While coherence of a person's narrative with their physiology and resultant nonverbal behavior is instructive in understanding interpersonal trust (*4-8*), the ability to correlate nonverbal behavior with deceptive statements is weak at best (*9*). Despite there being a greater connection between truth telling and nonverbal behavior, especially during stressful events (*10, 11*), many facial behaviors can be controlled (*12*). This leads to multiple critiques regarding the use of FEA in employment, education, governance, and criminal justice decision making. We organize these critiques based upon three distinct concerns regarding how FEA is used, and subsequently consider how FEA use may negatively affect different populations.

First, the term "Facial Expression Analysis" is a misnomer. The face does not "express" emotions, with internal physiology and possible behavior represented in the face on a one-to-one ratio (*13*). A meta-analysis by Durán and Fernández-Dols (*14*) of studies over the past 50 years on coherence of facial behavior with self-reported emotion suggests "that between 6% and 27% of the participants who reported one of the six emotions produced the whole predicted facial expression" (p. 15), with lower estimates for co-occurrence during "an actual emotional situation" (p. 14). In other words, facial behaviors do not occur as predicted; i.e., facial expressions do not consistently express internal physiological states. Likewise, while there is a relationship between facial behavior and emotional experience via facial feedback, a meta-analysis shows this relationship is small and variable (*15*), potentially due to a range of contextual and individual causes. In sum, a growing corpus of scientific findings have built and elaborated upon the groundbreaking work of emotion science pioneers to provide for a re-examination of "folk" psychological understandings; this has led to a much more nuanced and complex appreciation of facial behavior.

Second, FEA is biased. The major means by which FEA is applied in both academia and the private sector is through the lens of the Basic Emotion Theory which posits six fundamental emotions of happiness, anger, fear, sadness, disgust, and surprise (*16*). Here, there is a negative bias with four of the six emotions being negative and only one positive (*13*). Surprise, for its part, is not so much an emotion as a transitory state of orienting oneself to address stimuli having negative or positive implications. Consequently, such diverse and important positive emotions as interest, pride, pleasure, joy (*17*), and contentment (amongst others) are either bundled into one undifferentiated emotion of happiness or are misidentified. A recent performance comparison of eight commercially available FEA programs by Dupré and colleagues suggests that even with faces posing the six basic emotions, these programs significantly and substantially underperform human observers, with the performance suffering further when considering spontaneous facial behavior (*18*). The focus on identifying negative emotions in the face encourages regulatory and social strategies involving control and coercion, rather than cooperation and coordination that may result from positive emotions (*19*).

Third, FEA's use of Basic Emotion Theory is overly simplistic. Facial behavior itself is highly complex with 44 unique Action Units (AUs) identified by the Facial Action Coding System (FACS) and corresponding with facial musculature, albeit not on a 1:1 ratio. Another 18 Action Descriptors (ADs) describe behaviors that might have several muscles involved with movement; the combination of these AUs and ADs, along with the timing of their appearance, and their comparative intensity influences interpretation (*20*). For example, the smile serves multiple discrete social purposes, including reflecting amusement, communicating affinity, and asserting dominance (*21-24*); while all these smiles involve the pulling up of the lip corners using the zygomaticus muscle (AU 12), the involvement of other facial muscles, as well as their movement in terms of intensity and timing, affects how these different smiles are received and responded to. As pointed out by Dupré and colleagues (*18*) "(B)y extending the number of emotion categories, automated methods might overcome their current limitation of classifying a small set of emotion labels that are insufficient to describe the complexity of human expressive behaviors" (p. 11). Echoing these concerns, modern neurocomputing research remains in the early stages of applying FEA in a natural environment and identifying finer-grained emotional states (*25, 26*).

In summary, the face may best be seen as a communication tool with which humans influence others both consciously and subconsciously (*27-29*). It does so through signals that are more-or-less reliable depending on how they reflect internal physiology of an individual (*30, 31*), with greater reliability through multimodal coherence of verbal utterances and other body signals. For instance, the emotion of amusement may be seen as extremely reliable due to the coherence of multimodal signals beyond the face, with the amusement smile including the zygomaticus muscle being contracted, the jaw dropped, and the eyes closed, to include the vocalics of laughter, and the body movement including shaking in the torso (*32*). Furthermore, the use of these subtle signals in the face (as well as other nonverbal signals) are affected by contextual elements, including the person with whom the individual interacts. Attempts to simplify and explain behavior, especially for the purpose of gain and/or social control, without accounting for the complexity and variation in human experiences will likely lead to misuse and potentially to exploitation – especially of those social groups with little to no recourse.

Potential harms from Facial Expression Analysis due to demographic group disparities

A major critique beyond the application of simplistic models of emotion, as is currently the case with FEA, is that it simplifies the complexity of human emotional experience both across and within individuals. Such factors as development, gender, and societal context, amongst others, play a role in the display and interpretation of facial behaviors. The simplistic "one size fits all" approach currently in use with FEA technologies for employment, education, service provision, and governance – including criminal justice – may in many cases fail to adequately support local norms and individual freedoms.

Life history influences emotional experiences and the resultant facial behaviors. Research shows that infants develop the ability to process the faces of those around them and appreciate their social context as they grow older, and consequently develop different strategies to influence others (*33, 34*). This awareness and the deployment of facial behaviors becomes more varied and resonant throughout an individual's lifespan. This occurs through introspection and interoception, the knowing of one's own mind and body

states respectively (*35*) and may even be seen with differences in individual facial behavior repertoires (*36*).

More broadly, influences at the intersection of biological sex and socially constructed gender affect facial behaviors, with biases being introduced early in life. Gender biases with FEA might occur due to females being more nonverbally communicative than males, and when males are more expressive, having a tendency towards anger and fear (*37-39*). Tellingly, Woodzicka found that during mock interviews females smiled between half as much to twice as long as males after controlling for time, based upon the type of smile measured (*40*). Mehu and Dunbar found that gender and power interacted asymmetrically, with younger males deliberately posing smiles to older individuals with (presumed) greater status within a hierarchy. For women the relationship was not as clear. Older women posed more deliberate smiles, while younger women laughed and displayed amusement smiles to a greater extent, suggesting a power dynamic other than hierarchy at work (*41*). Thus, while men might smile as often, if not more than women do, in more fluid social circumstances (*41-43*) context and age jointly affect facial behavior in men and women differentially in terms of both types and amount.

FEA might likewise introduce biases against rural citizens due to their being less facially animated and less likely to display positive emotions than those living in more heterogenous urban areas. Cross-cultural research of thirty-two countries shows that greater historical heterogeneity of a culture, i.e., the extent to which numerous source countries contributed that that country's present day population, and residential mobility – the increased likelihood of moving away from one's current home – was positively related to the willingness to openly show emotions (study 1), as well as rationale for smiling (*44*). This research was followed up with a more extensive world nation-level and state-level polling data (*45*) finding that "[i]ndividuals from historically heterogenous cultures smile more and display facial expressions that are more accurately recognized across cultures" (p.13).

Policy Implications

In the modern era, the application of new technologies within organizations has largely outpaced the ability of the nation's policymaking system to protect employees – and the general public – from adverse outcomes. Starting in the early 1900s, the "time and motion studies" used by organizations implementing "scientific management" provided managerial tools that relied on the then-new technologies of photography and videography to increase productivity. While such studies allowed for the systematic and scientific discovery of the "one best way" within organizations to accomplish a task, thus maximizing labor efficiency, it also implemented a style of performance management that pressured employees to meet often-unattainable efficiency goals. It also reinforced discriminatory managerial decisions while relying on conceptualizations of organizational behaviors that were often misguided and, at their worst, led to inhumane work conditions and labor strife (*46-48*). Arguably, negative long-term effects of "scientific management" approaches can be seen in the many organizations that now use monitoring software on a variety of employee behaviors (*49*).

Given such history and the above risks and limitations of FEA, new concerns will emerge as monitoring software evolves to integrate FEA data and organizations generate inaccurate inferences of individual behaviors and emotions. For instance, organizations

could mis-identify emotional states with FEA and then use that data in subsequent managerial decisions. In such a scenario, FEA software might identify an employee with facial displays commonly associated with anger during a meeting. Retrospectively analyzing FEA data from the meeting, a manager may infer the employee's emotional state is negative and react with punitive or restrictive measures to control the employee's behavior in ways that reinforce existing biases and stereotypes, *even though FEA software cannot accurately predict an individual's emotional state*. When extended to the criminal justice system, which now depends on evidence-based therapeutic "behavioral change" models to control recidivism, the extension of such FEA-aided decisions into the public sector can have severe consequences and disrupt the intent of many existing public policies and priorities.

While many public policies designed to maintain privacy and mitigate discriminatory administrative practices were passed in the 1960s and 1970s, advances in computing and the widespread storage of private data have compromised the goals of such policies. Public and private firms began to search for relationships in data to aid operational decisions with a focus on enhancing efficiency, often at the expense of other indicators of organizational well-being. For their part, public policymakers increasingly passed laws to leverage such data for policies like crime control (*50-52*). Concerns raised over the accessibility of such data led to new privacy laws in the 1970s and 1980s, the discussion of a "right to information privacy," and how such rights could be protected within organizations via a "zone of privacy" for individuals and their data (*53*). However, privacy is a loosely defined concept that requires deeper consideration of cultural and temporal context (*50*), and discussions do not easily translate into law; currently we face significant concerns over information privacy and the control of data collected by private organizations and governments. With FEA-based data, such concerns only intensify.

To date, information privacy research and policy have focused on records of knowingly expressed or recorded behaviors; however, advances in AI and personal data digitalization promise to increasingly enable identification of physiological states and, by their extrapolation, internal cognitions and behavioral intent (*54, 55*). In short, FEA threatens to permeate a sacred boundary by imputing one's *internal thoughts or feelings* based upon the often pre-cognitive or involuntary physiological responses individuals have to stimuli (*56*). Warren and Brandeis foreshadowed these concerns in their seminal work that established the basis for modern U.S. privacy legislation (*57*).

> "The circumstance that a thought or emotion has been recorded in a permanent form renders its identification easier, and hence may be important from the point of view of evidence, but it has no significance as a matter of substantive right. If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in *facial expression*." (p. 206, emphasis added)

Much like the implementation of time-and-motion studies in the early 1900s that enabled scientific management, the use of digital databases since the 1960s that store and analyze personal information, and the "big data" revolution of the past two decades that enables both hyper-personalization and mass surveillance, FEA has the potential to influence the management of organizations and governing of society in ways that could

harm employees and the public. As evidenced by the continued use of the polygraph as a "lie detector" in employment, legal, and political domains, potentially life changing decisions are made despite low levels of confidence in a technology's efficacy. Likewise, there will be a temptation to use FEA in a variety of big data applications that record facial behavior and then extrapolate FEA data to provide predictive analytics that impact employment decisions – or worse.

The simplified analysis offered by FEA may be seen as a strength by those who would use this tool in public, non-profit, and private sector decision making. However, the large-scale uses of such a technology would introduce and perpetuate biases if used to inform decisions without proper skepticism and regulation to consider context and other influences. For instance, a hostile off-camera interrogator will influence facial response behavior with implications for personnel decisions in organizations, and importantly, prosecution, judgment, and sentencing decisions in the criminal justice system. FEA might likewise exacerbate pre-existing biases against rural residents and lower-status individuals due to variations in facial behavior, resulting in long term societal impacts. Perhaps the greatest cause for concern with this (and other) new biometric technologies is an emerging threat to the boundary between what we make visible to an observer and the thoughts and feelings we keep to ourselves.

Patrick A. Stewart, Ph.D.
Department of Political Science
435 Old Main
University of Arkansas, Fayetteville
Fayetteville, AR 72701
[redacted]

Jeffrey K. Mullins, Ph.D.
Department of Information Sciences, Walton College
University of Arkansas, Fayetteville
[redacted]

Thomas J. Greitens, Ph.D.
Department of Political Science & Public Administration,
Central Michigan University
[redacted]

References

1. J. N. Bailenson, Nonverbal overload: A theoretical argument for the causes of Zoom fatigue. *Technology, Mind, and Behavior* **2**, (2021).
2. N. R. Council, *The polygraph and lie detection*. (National Academies Press, 2003).
3. W. G. Iacono, G. Ben-Shakhar, Current status of forensic lie detection with the comparison question technique: An update of the 2003 National Academy of Sciences report on polygraph testing. *Law and human behavior* **43**, 86 (2019).

4. E. P. Bucy, Emotional and Evaluative Consequences of Inappropriate Leader Displays. *Communication Research* **27**, 194-226 (2000).
5. E. P. Bucy, J. E. Newhagen, The emotional appropriateness heuristic: Processing televised presidential reactions to the news. *Journal of Communication* **49**, 59-79 (1999).
6. J. S. Seiter, Harry Weger, Jr., Audience perceptions of candidates' appropriateness as a function of nonverbal behaviors displayed during televised political debates. *The Journal of social psychology* **145**, 225-236 (2005).
7. J. K. Burgoon, J. L. Hale, Nonverbal expectancy violations: Model elaboration and application to immediacy behaviors. *Communications Monographs* **55**, 58-79 (1988).
8. J. K. Burgoon, J. B. Walther, Nonverbal expectancies and the evaluative consequences of violations. *Human Communication Research* **17**, 232-265 (1990).
9. S. Mann, A. Vrij, R. Bull, Suspects, lies, and videotape: An analysis of authentic high-stake liars. *Law and human behavior* **26**, 365-376 (2002).
10. G. L. J. Lancaster, A. Vrij, L. Hope, B. Waller, Sorting the liars from the truth tellers: The benefits of asking unanticipated questions on lie detection. *Applied Cognitive Psychology* **27**, 107-114 (2013).
11. L. Ten Brinke, S. Porter, A. Baker, Darwin the detective: Observable facial muscle contractions reveal emotional high-stakes lies. *Evolution and Human Behavior* **33**, 411-416 (2012).
12. M. G. Frank, E. Svetieva, in *Understanding Facial Expressions in Communication*. (Springer, 2015), pp. 227-242.
13. L. F. Barrett, R. Adolphs, S. Marsella, A. M. Martinez, S. D. Pollak, Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological science in the public interest* **20**, 1-68 (2019).
14. J. I. Durán, J.-M. Fernández-Dols, Do emotions result in their predicted facial expressions? A meta-analysis of studies on the co-occurrence of expression and emotion. *Emotion*, (2021).
15. N. A. Coles, J. T. Larsen, H. C. Lench, A meta-analysis of the facial feedback literature: Effects of facial feedback on emotional experience are small and variable. *Psychological bulletin*, (2019).
16. E. A. Clark *et al.*, The Facial Action Coding System for Characterization of Human Affective Response to Consumer Product-Based Stimuli: A Systematic Review. *Frontiers in psychology* **11**, 920 (2020).
17. M. Mortillaro, M. Mehu, K. R. Scherer, Subtly different positive emotions can be distinguished by their facial expressions. *Social Psychological and Personality Science* **2**, 262-271 (2011).
18. D. Dupré, E. G. Krumhuber, D. Küster, G. J. McKeown, A performance comparison of eight commercially available automatic classifiers for facial affect recognition. *Plos one* **15**, e0231968 (2020).
19. B. R. Spisak, M. J. O'Brien, N. Nicholson, M. van Vugt, Niche construction and the evolution of leadership. *Academy of Management Review* **40**, 291-306 (2015).
20. E. L. Rosenberg, P. Ekman, *What the face reveals: Basic and applied studies of spontaneous expression using the facial action coding system (FACS)*. (Oxford University Press, 2020).

21. P. A. Stewart, E. P. Bucy, M. Mehu, Strengthening bonds and connecting with followers: A biobehavioral inventory of political smiles. *Politics & the Life Sciences* **34**, 73-92 (2015).
22. J. D. Martin, H. C. Abercrombie, E. Gilboa-Schechtman, P. M. Niedenthal, Functionally distinct smiles elicit different physiological responses in an evaluative context. *Scientific reports* **8**, 3558 (2018).
23. M. Rychlowska *et al.*, Functional smiles: Tools for love, sympathy, and war. *Psychological science* **28**, 1259-1270 (2017).
24. P. M. Niedenthal, M. Mermillod, M. Maringer, U. Hess, The Simulation of Smiles (SIMS) model: Embodied simulation and the meaning of facial expression. *Behavioral and Brain Sciences* **33**, 417-433 (2010).
25. F. Zhou, S. Kong, C. C. Fowlkes, T. Chen, B. Lei, Fine-grained facial expression analysis using dimensional emotion model. *Neurocomputing* **392**, 38-49 (2020).
26. J. Joo, E. P. Bucy, C. Seidel, Computational Communication Science| Automated Coding of Televised Leader Displays: Detecting Nonverbal Political Behavior With Computer Vision and Deep Learning. *International Journal of Communication* **13**, 23 (2019).
27. U. Hess, S. Hareli, in *The science of facial expression,* J. M. Fernández-Dols, J. A. Russell, Eds. (Cambridge University Press, New York, NY, 2017), pp. 375-396.
28. M. Mehu, K. R. Scherer, A psycho-ethological approach to social signal processing. *Cognitive Processing* **13**, 397-414 (2012).
29. M. J. Owren, D. Rendall, M. J. Ryan, Redefining animal signaling: influence versus information in communication. *Biology and Philosophy*, 1-26 (2010).
30. M. Mehu, M. Mortillaro, T. Bänziger, K. R. Scherer, Reliable Facial Muscle Activation Enhances Recognizability and Credibility of Emotional Expression. *Social Psychological and Personality Science* **2**, 262-271 (2011).
31. P. Ekman, *Telling lies: Clues to deceit in the marketplace, politics, and marriage*. (WW Norton & Company, New York, NY, 2009).
32. A. Gaspar, F. Esteves, P. Arriaga, in *The Evolution of Social Communication in Primates*. (Springer, 2014), pp. 101-126.
33. D. S. Messinger, T. D. Cassel, S. I. Acosta, Z. Ambadar, J. F. Cohn, Infant smiling dynamics and perceived positive emotion. *Journal of Nonverbal Behavior* **32**, 133-155 (2008).
34. K. Kawakami *et al.*, Spontaneous smile and spontaneous laugh: An intensive longitudinal case study. *Infant Behavior and Development* **30**, 146-152 (2007).
35. L. F. Barrett, *How emotions are made: The secret life of the brain*. (Houghton Mifflin Harcourt, 2017).
36. H. Ilgen, J. Israelashvili, A. Fischer, Personal Nonverbal Repertoires in facial displays and their relation to individual differences in social and emotional styles. *Cognition and Emotion*, 1-10 (2021).
37. J. M. Vigil, A socio-relational framework of sex differences in the expression of emotion. *Behavioral and Brain Sciences* **32**, 375-390 (2009).
38. L. R. Brody, J. A. Hall, Gender and emotion in context. *Handbook of emotions* **3**, 395-408 (2008).
39. E. J. Coats, R. S. Feldman, Gender differences in nonverbal correlates of social status. *Personality and Social Psychology Bulletin* **22**, 1014-1022 (1996).

40. J. A. Woodzicka, Sex differences in self-awareness of smiling during a mock job interview. *Journal of Nonverbal Behavior* **32**, 109-121 (2008).
41. M. Mehu, R. I. M. Dunbar, Relationship between smiling and laughter in humans (homo sapiens): Testing the power asymmetry hypothesis. *Folia Primatologica* **79**, 269-280 (2008).
42. L. P. Robertson, Y. I. Russell, Age and gender differences in smiling and laughter: the power asymmetry hypothesis retested. *Human Ethology Bulletin* **31**, 5-14 (2016).
43. M. Mehu, R. I. M. Dunbar, Naturalistic observations of smiling and laughter in human group interactions. *Behaviour* **145**, 1747-1780 (2008).
44. M. Rychlowska *et al.*, Heterogeneity of long-history migration explains cultural differences in reports of emotional expressivity and the functions of smiles. *Proceedings of the National Academy of Sciences* **112**, E2429-E2436 (2015).
45. P. M. Niedenthal, M. Rychlowska, A. Wood, F. Zhao, Heterogeneity of long-history migration predicts smiling, laughter and positive emotion across the globe and within the United States. *PloS one* **13**, e0197651 (2018).
46. F. W. Taylor, *Scientific management*. (Routledge, 2004).
47. A. Fleischmann, M. Ozbilgin, Queering the principles: A queer/intersectional reading of Frederick W. Taylor's "The principles of scientific management.". *Equality, diversity and inclusion at work: Theory and scholarship*, 159-170 (2009).
48. R. B. Denhardt, J. V. Denhardt, The new public service: Serving rather than steering. *Public administration review* **60**, 549-559 (2000).
49. S. Suder, M. Erikson, in *Algorithmic Governance and Governance of Algorithms*. (Springer, 2021), pp. 71-85.
50. D. J. Solove, Understanding privacy. (2008).
51. F. H. Cate, Privacy in the information age. (1997).
52. L. Lessig, *Code And Other Laws of Cyberspace, Version 2.0*. (Basic Books, Boston, MA, 2006), pp. 432.
53. U. S. Court, Whalen v. Roe. 22 Feb 1977. *United States reports: cases adjudged in the Supreme Court at... and rules announced at... United States. Supreme Court* **429**, 589-609 (1977).
54. D. E. Leidner, O. Tona, The CARE Theory of Dignity Amid Personal Data Digitalization. *MIS Quarterly* **45**, (2021).
55. S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. (Profile books, 2019).
56. K. R. Scherer, A. Schorr, T. Johnstone, *Appraisal processes in emotion: Theory, methods, research*. (Oxford University Press, USA, New York, NY, ed. 1, 2001).
57. L. Brandeis, S. Warren, The right to privacy. *Harvard law review* **4**, 193-220 (1890).

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Pel Abbott

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Tuesday, January 11, 2022 9:16:39 AM

NO, NO, NO

Has ANYONE read dystopian science fiction?

Technology is only as good as PEOPLE running it, and since America is the leader in COVID deaths and is the most RACIST country with a high GDP and only worships billionaires not people of actual merit - NO, NO, and NO.

Absolutely no. We can't even do anything about climate change.

We don't need shitty AI watching us 24/7. NO.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Philadelphia Unemployment Project

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

November 29th, 2021

To: Dear White House Office of Science and Technology Policy (OSTP) Staff

From: Daniel Ravizza, Philadelphia Unemployment Project

Contact: [redacted]

I'm Daniel Ravizza, an organizer with the Philadelphia Unemployment Project (PUP), a non-profit advocacy group serving the Philadelphia region for over 45 years in the area of unemployment compensation advocacy. Since 1975, the Philadelphia Unemployment Project has organized the poor and unemployed to fight for economic justice, bringing diverse groups together to bring about major changes that benefit millions of unemployed and impoverished people. PUP has helped the unemployed link with coalition partners in the labor, religious, community, civil rights, and women's movements to increase our power.

Recently, Pennsylvania's Department of Labor and Industry (DLI) implemented online ID verification (IDV) systems to verify claimant's identity through the use of documents uploads and a "selfie" picture that was used to prevent fraud and abuse for both the Pandemic Unemployment Assistance (PUA) and regular Unemployment Compensation (UC) systems. While touted a panacea that would ease the ability of eligible unemployed claimants to quickly receive benefits, our experience has been quite different.

Online identity verification through the use of this technology has impacted claimants and potential claimants who are not fully digitally literate and raises questions of the effectiveness of the program. After the rollout of ID.me in 2021, PUP found ourselves advocating for in-person assistance for individuals who could not complete multi-step online processes required to create and a digital account with the PA Department of Labor and Industry in order to start or continue receiving benefits.

An alarming number of cases of benefits stopping without a final determination has taken place since this summer. Since mid-August, 25% of 384 cases have had benefits stopped in some manner without a final determination, a violation of the Supreme Court *Java* ruling. Of those who contacted PUP who may have had their benefits stopped in violation of Java, 10% cited ID.me as a factor in our communications. PUP has received reports from unemployed persons that have been owed the full amount of PUA (>50 weeks of unemployment) and have been in the appeals process for months after the ending of the program with no resolution. These findings only represent the small fraction of the population that contacted PUP; many more undoubtedly exist in Pennsylvania.

We have had mixed results with claimants who have been sent to do in-person IDV with CareerLink staff. Some have been able to successfully apply in person, yet some have continued having trouble with staff that do not have a knowledge of the protocol or are struggling with resources. Ultimately, it does not bridge the digital divides in our communities that have left many still seeking verification- and thus compensation. For those that are successful in completing ID.me or identity verification, some still are still waiting for benefits to be distributed for weeks or months after completing the process.

ID.me may be a process that exacerbates PA DLI's poor record on promptness of payment. The federal standard for unemployment dictates that 80% of eligible claimants receive their first check 21 days after their first compensable week. Currently, only 32% claimants are receiving their checks within that timeframe.[1] The state's performance continues to lag in later payments as well, as total response time has trended downward since the beginning the summer of this year.

[1] Benefits Timeliness and Quality Reports, United States Department of Labor. Accessed 11/23/21. https://oui.doleta.gov/unemploy/btq.asp

ID.me and digital IDV will continue to challenge communities that a) do not have access to digital devices such as camera-equipped smartphone, laptops, and tablets b) do not have digital literacy skills allow them to create email accounts and upload files to password-protected online portals and c) do not have any sort of internet access at all.

Our concern remains that the expansion of these technologies will leave our most vulnerable communities in a continued loop of confusion without any access to the monetary benefits they are entitled to.

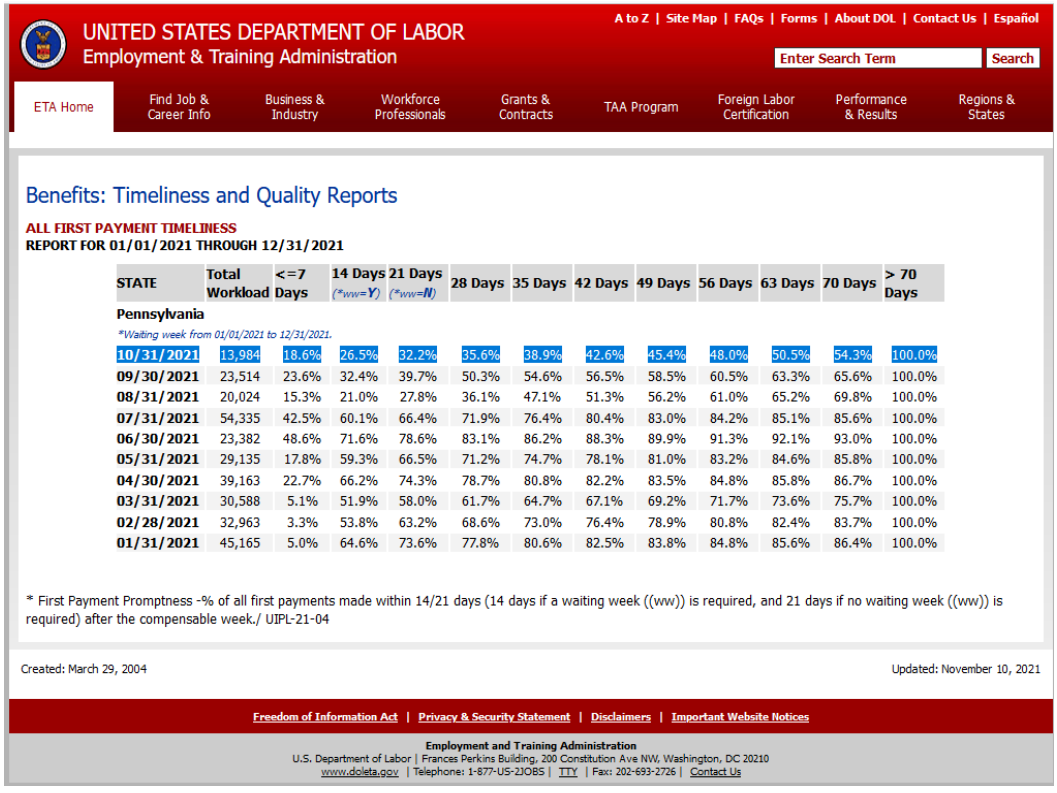
Best,

Daniel Ravizza

Organizer

Philadelphia Unemployment Project

Exhibit A:



UNITED STATES DEPARTMENT OF LABOR
Employment & Training Administration

A to Z | Site Map | FAQs | Forms | About DOL | Contact Us | Español

Enter Search Term | Search

ETA Home | Find Job & Career Info | Business & Industry | Workforce Professionals | Grants & Contracts | TAA Program | Foreign Labor Certification | Performance & Results | Regions & States

Benefits: Timeliness and Quality Reports

ALL FIRST PAYMENT TIMELINESS
REPORT FOR 01/01/2021 THROUGH 12/31/2021

STATE	Total Workload	<=7 Days	14 Days (*ww=Y)	21 Days (*ww=N)	28 Days	35 Days	42 Days	49 Days	56 Days	63 Days	70 Days	> 70 Days
Pennsylvania												
*Waiting week from 01/01/2021 to 12/31/2021.												
10/31/2021	13,984	18.6%	26.5%	32.2%	35.6%	38.9%	42.6%	45.4%	48.0%	50.5%	54.3%	100.0%
09/30/2021	23,514	23.6%	32.4%	39.7%	50.3%	54.6%	56.5%	58.5%	60.5%	63.3%	65.6%	100.0%
08/31/2021	20,024	15.3%	21.0%	27.8%	36.1%	47.1%	51.3%	56.2%	61.0%	65.2%	69.8%	100.0%
07/31/2021	54,335	42.5%	60.1%	66.4%	71.9%	76.4%	80.4%	83.0%	84.2%	85.1%	85.6%	100.0%
06/30/2021	23,382	48.6%	71.6%	78.6%	83.1%	86.2%	88.3%	89.9%	91.3%	92.1%	93.0%	100.0%
05/31/2021	29,135	17.8%	59.3%	66.5%	71.2%	74.7%	78.1%	81.0%	83.2%	84.6%	85.8%	100.0%
04/30/2021	39,163	22.7%	66.2%	74.3%	78.7%	80.8%	82.2%	83.5%	84.8%	85.8%	86.7%	100.0%
03/31/2021	30,588	5.1%	51.9%	58.0%	61.7%	64.7%	67.1%	69.2%	71.7%	73.6%	75.7%	100.0%
02/28/2021	32,963	3.3%	53.8%	63.2%	68.6%	73.0%	76.4%	78.9%	80.8%	82.4%	83.7%	100.0%
01/31/2021	45,165	5.0%	64.6%	73.6%	77.8%	80.6%	82.5%	83.8%	84.8%	85.6%	86.4%	100.0%

* First Payment Promptness -% of all first payments made within 14/21 days (14 days if a waiting week ((ww)) is required, and 21 days if no waiting week ((ww)) is required) after the compensable week./ UIPL-21-04

Created: March 29, 2004 Updated: November 10, 2021

Freedom of Information Act | Privacy & Security Statement | Disclaimers | Important Website Notices

Employment and Training Administration
U.S. Department of Labor | Frances Perkins Building, 200 Constitution Ave NW, Washington, DC 20210
www.doleta.gov | Telephone: 1-877-US-2JOBS | TTY | Fax: 202-693-2726 | Contact Us

Benefits Timeliness and Quality Report for PA, accessed 11/23/21.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Project On Government Oversight

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

PROJECT ON GOVERNMENT OVERSIGHT

January 15, 2022

Office of Science and Technology Policy
Executive Office of the President, Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Via email: BiometricRFI@ostp.eop.gov

Subject: Comment in Response to Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

To the Office of Science and Technology Policy:

Thank you for the opportunity to submit comments to the White House Office of Science and Technology Policy regarding use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes. Law enforcement use of face recognition involves the risk of misidentification as well as misuse — each of which causes serious harm to civil rights, civil liberties, and public welfare.

Our comment will focus on one biometric identification technology — face recognition — that is already used on a large scale by local, state, and federal law enforcement. Our comment describes the multitude of dangers face recognition, as currently deployed, poses to civil rights and civil liberties, examines how current federal government policies contribute to this danger, and recommends a series of White House policies to reduce the harm face recognition causes.

Founded in 1981, the Project On Government Oversight (POGO) is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles.

The Constitution Project at POGO centers its work on issues such as guarding against improper and overbroad surveillance, including unchecked face recognition. In 2019, The Constitution Project at POGO convened a face recognition task force of expert stakeholders to examine the impact of face recognition surveillance.[1] The task force included academics, tech experts, civil rights and civil liberties advocates, and law enforcement officials. Our group concluded that any law enforcement use of face recognition should be subject to strong limits, and provided a set of policy recommendations to support legislatures in the creation of reasonable but necessary limits.

[1] Task Force on Facial Recognition Surveillance, Project On Government Oversight, Facing the Future of Surveillance (March 4, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/.

Law Enforcement's Use of Face Recognition Is Already Significant

At least one in four state and local police departments have the capacity to run face recognition searches, either directly or through a partnering agency.[2] According to a *BuzzFeed News* investigative report, over 1,800 publicly funded agencies have used Clearview AI — a face recognition system that is especially problematic for developing a photo database built on scraping social media without users' consent.[3]

The FBI oversees a massive face recognition system through its Facial Analysis, Comparison, and Evaluation Services Unit, with capacity to scan hundreds of millions of photos, including nearly one out of every three drivers' license photos.[4] In addition to conducting face recognition scans for its own investigations, the FBI also employs its Next Generation Identification-Interstate Photo System to process requests for scans largely from state and local law enforcement.[5] The FBI no longer discloses how many face recognition searches it runs, but it previously processed as many as 8,000 searches per month on average.[6]

Federal use of face recognition extends beyond the FBI. Sixteen federal agencies use face recognition, including half a dozen that employ it in criminal investigations.[7] Notably, Immigration and Customs Enforcement has in recent years run thousands of face recognition searches of state drivers' license databases,[8] sometimes without oversight and approval of state officials.[9] ICE's access to face recognition appears to be a driving factor in the detention of immigrants.[10]

Face Recognition Misidentifications Cause Serious Harm to Civil Rights, Civil Liberties, and Public Welfare

One of the most acute risks of face recognition is its potential to misidentify individuals. In terms of law enforcement use, this could lead to incorrect identification of suspects, as well as wrongful arrest and incarceration.

---

[2] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, Georgetown Law Center on Privacy and Technology, The Perpetual Line-Up: Unregulated Police Face Recognition in America (October 18, 2016), Sec. V. https://www.perpetuallineup.org.
[3] Ryan Mac et al., "Surveillance Nation," *BuzzFeed News*, April 9, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition?bfsource=relatedmanual.
[4] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, Georgetown Law Center on Privacy and Technology, The Perpetual Line-Up: Unregulated Police Face Recognition in America (October 18, 2016), Appendix: Federal Bureau of Investigations, https://www.perpetuallineup.org/jurisdiction/federal-bureau-investigation.
[5] Congressional Research Service, Federal Law Enforcement Use of Facial Recognition Technology (October 27, 2020), https://sgp.fas.org/crs/misc/R46586.pdf.
[6] FBI, "November 2021 Next Generation Identification (NGI) System Fact Sheet," https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view; FBI, "November 2017 Next Generation Identification (NGI) System Fact Sheet," https://www.eff.org/files/2018/02/11/november_2017_ngi_system_fact_sheet_-_fbi.pdf.
[7] U.S. Government Accountability Office, "Facial Recognition Technology: Current and Planned Uses by Federal Agencies" (August 24, 2021) https://www.gao.gov/products/gao-21-526.
[8] Drew Harwell, "FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches," *Washington Post*, July 7, 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.
[9] Drew Harwell and Erin Cox, "ICE has run facial-recognition searches on millions of Maryland drivers," *Washington Post*, February 26, 2020, https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.
[10] Drew Harwell and Erin Cox, "ICE has run facial-recognition searches on millions of Maryland drivers," *Washington Post*, February 26, 2020, https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/ ("[CASA] now says ICE's open access to MVA photos and other data was a main reason for the detentions").

Face Recognition Misidentifications Stem from a Variety of Causes, Many of Which Cannot Be Prevented

First, the quality of face recognition algorithms can vary significantly, causing acute harms to civil liberties. Notably, many algorithms misidentify women and people of color at a higher rate than other people. Studies by the National Institute of Standards and Technology; the Massachusetts Institute of Technology, Microsoft, and AI Now Institute researchers; the American Civil Liberties Union; and an FBI expert all concluded that face recognition systems misidentify women and people of color more frequently.[11] Most recently, the National Institute of Standards and Technology found that some systems were 100 times more likely to misidentify people of East Asian and African descent than white people.[12] Failure to recognize the significance of this problem — and account for it in selection and review of software, training, and auditing — will undermine investigations, seriously endanger civil rights, and undermine efforts to reduce systemic bias in policing and the criminal justice system.

Second, image quality can also significantly impact the accuracy of matches. Sets of reference images — databases containing previously identified faces — in face recognition systems are typically high-resolution photos of a person directly facing a camera at close range, such as for a mug shot photo. But probe images — from which law enforcement seeks to identify individuals — are derived from a wide range of situations, which creates the potential for low image quality and erroneous results. Bad lighting, indirect angles, distance, poor camera quality, and low image resolution all make misidentifications more likely.[13] These poor image conditions are more common when photos and videos are taken in public, such as with a CCTV camera. But these low-quality images often serve as probe images for face recognition scans, without proper consideration for their diminished utility.[14]

Third, even when using more effective software and higher quality images, system settings can make face recognition matches prone to misidentification. For example, the way law enforcement sets confidence thresholds — a metric used to compare which proposed matches within a system are more likely to be accurate — can undermine the reliability of results. The lower the confidence threshold, the more likely the "match" is actually a false positive. So, if law enforcement entities set face recognition systems to always return potential matches — no matter how low confidence the

[11] Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (December 19, 2019), 2, https://doi.org/10.6028/NIST.IR.8280; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proceedings of Machine Learning Research, vol. 81 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Joy Buolamwini and Inioluwa Deborah Raji, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society (2019), https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognitionfalsely-matched-28; Brendan Klare et al., "Face Recognition Performance: Role of Demographic Information," IEEE Transactions on Information Forensics and Security, vol. 7, no. 6 (December 2012), http://openbiometrics.org/publications/klare2012demographics.pdf.

[12] Grother, Ngan, Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2.

[13] Task Force on Facial Recognition Surveillance, Project On Government Oversight, Facing the Future of Surveillance (March 4, 2019), Sec. II. https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/.

[14] "CCTV feeds facial recognition systems for law enforcement," *Biometric Technology Today*, vol. 2015, no. 4 (April 2015): 3, https://www.sciencedirect.com/science/article/abs/pii/S0969476515300539.

threshold — they will receive untrustworthy data. Troublingly, some law enforcement entities, including the FBI, do just that.[15]

In the absence of safeguards to address this range of misidentification risks, face recognition will continue to provoke errors, harm innocent individuals, and exacerbate inequalities in how different communities are policed.

Using Face Recognition to Generate Leads Does Not Avoid Harms Such as Wrongful Arrests

Law enforcement officials supporting the use of face recognition, such as FBI Director Christopher Wray, downplay the dangers of misidentification by arguing that face recognition is just used for leads.[16] But this ignores a basic fact: Leads can vary immensely in how reliable or delusive they are, as well as how much or how little they might impact the course of an investigation. Law enforcement has previously relied heavily on certain "scientific" forensic evidence techniques — techniques that have been touted as presumptively objective, consistent, and reliable — that were, in fact, highly misleading.[17] As is the case with bite-mark analysis or lie detector tests,[18] the fact that face recognition is merely used as a lead does not prevent it from producing errors that cause the arrest or incarceration of innocent individuals.

Individuals could be — and in numerous recorded cases have been — charged in part based on how a face recognition match affects the direction of an investigation early on. Law enforcement overconfidence in the accuracy of matches can promote confirmation bias and sloppy follow-up, limiting the ability to identify face recognition errors.[19]

It is also important to recognize that even if errors in face recognition systems are eventually discovered and accounted for, face recognition mismatches can form the basis of individuals becoming investigative targets. A variety of disruptive and potentially traumatic police actions can

---

[15] Jim Trainum, "Facial Recognition Surveillance Doesn't Necessarily Make You Safer," Project On Government Oversight, July 22, 2019, https://www.pogo.org/analysis/2019/07/facial-recognition-surveillance-doesnt-necessarily-make-you-safer/; According to then-FBI Deputy Assistant Director Kimberly Del Greco, its system is set up so that it "returns a gallery of 'candidate' photos [reference photos] of 2-50 individuals (the default is 20)." Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing before the House Committee on Oversight, 116th Cong. (June 4, 2019) (statement by Kimberly Del Greco, Deputy Assistant Director, FBI Criminal Justice Information Services Division), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use; Erin M. Priest, Privacy and Civil Liberties Officer, FBI, Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System (May 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view
("A gallery of two to fifty photos will be returned, with the law enforcement agency choosing the size of the gallery. If no choice is made, a default of twenty photos is returned.").

[16] For example, during a 2020 Congressional hearing, FBI Director Christopher Wray responded to inquiries on face recognition by stating, "We use it for lead value. We don't use facial recognition as a basis to arrest or convict." House Judiciary Committee. Oversight of the Federal Bureau of Investigation: Hearing before the House Judiciary Committee, 116th Cong. (February 5, 2020), https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780.

[17] See President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (September 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[18] Joseph Stromberg, "Lie detectors: Why they don't work, and why police use them anyway," *Vox*, December 15, 2014, https://www.vox.com/2014/8/14/5999119/polygraphs-lie-detectors-do-they-work.

[19] For example, in one incident, New York City Police Department officers allegedly took a face recognition match, and then rather than try to legitimately confirm or disconfirm its accuracy, instead texted a witness, "Is this the guy…?" along with a single photo, rather than following proper procedure to use a photo array. Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019, https://www.flawedfacedata.com/.

flow from such errors, such as being stopped, searched, monitored for prolonged periods of time, or detained and questioned. These harms will be disproportionately borne by people of color so long as algorithmic bias is present in face recognition systems, and more generally so long as systemic bias impacts policing and our criminal justice system.

It is critical when evaluating these harms to consider the real-world human cost. Take for example the impact that a faulty face recognition match had on Robert Williams, who was arrested at his home and subsequently held in custody for 30 hours:

> During the time that I was in custody, my wife was dealing with the emotional and practical immediate fall out. My daughters were scared, wondering why their father had been arrested and whether he would come home. My wife had to comfort them. While I was away, our oldest daughter turned over a family photo that was sitting out on the family furniture because she couldn't bear looking at a picture of her Daddy under the circumstances. My wife also had to call my employer and explain to them where I was and why I wouldn't be coming to work that day. They could have fired me right then …. My daughters can't unsee me being handcuffed and put into a police car. They continue to suffer that trauma. For example, after I returned from Jail, they started playing cops and robbers games where they tell me that I'm in jail for stealing. And even today, when my daughters encounter the coverage about what happened to me, they are reduced to tears by their memory of those awful days.[20]

Despite this traumatic experience, Williams describes himself as "lucky" that the harm he and his family unjustly experienced was not more severe.[21]

Finally, the notion that face recognition matches are merely leads that serve as one of many components of an investigation is often simply untrue. There are already three documented cases where individuals were wrongfully arrested — with two spending time in jail — based entirely on bad face recognition matches.[22] According to a 2020 *New York Times* investigation of face recognition systems in Florida, "Although officials said investigators could not rely on facial recognition results to make an arrest, documents suggested that on occasion officers gathered no other evidence."[23] And because use of face recognition in investigations is often hidden from arrestees and defendants, there are likely many similar instances of face recognition being the sole basis for an arrest that remain hidden from the public.

Lack of Disclosure Augments Misidentification Risks and Undermines Due Process Rights

---

[20] Facial Recognition Technology: Examining Its Use By Law Enforcement: Hearing before the House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security, 117th Cong. (July 13, 2021) (statement of Robert Williams), https://docs.house.gov/meetings/JU/JU08/20210713/113906/HMTG-117-JU08-Wstate-WilliamsR-20210713.pdf.

[21] Facial Recognition Technology: Examining Its Use By Law Enforcement: Hearing before the House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security, 117th Cong. (July 13, 2021) (statement of Robert Williams), https://docs.house.gov/meetings/JU/JU08/20210713/113906/HMTG-117-JU08-Wstate-WilliamsR-20210713.pdf.

[22] Kashmir Hill, "Wrongfully Accused By An Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; K. Holt, "Facial recognition linked to a second wrongful arrest by Detroit police," *Engadget*, July 10, 2020, https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html; Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[23] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

The risks of misidentification causing serious harm are increased by the fact that use of face recognition is often hidden from defendants. Given the wide range of technical factors that can impact face recognition's effectiveness, it is critical that defendants are notified and given the opportunity to examine face recognition technology whenever it is used in an investigation, as they would with any other complex forensic tool.

Despite the importance of disclosure, it rarely occurs.[24] In some jurisdictions, law enforcement uses facial recognition thousands of times per month, and defendants almost never receive notice of its use in investigations.[25] Yet even as law enforcement relies on the technology for investigations, they obscure it from examination in court by defendants and judges.[26]

Defendants have a vested interest in reviewing a variety of factors, such as algorithm quality, the software settings police used, and whether any other potential matches were discovered or investigated that could provide exculpatory or mitigating evidence. This is key not only to protecting innocent individuals, but also to preserving constitutionally guaranteed due process rights of all defendants and promoting genuine public safety.

Furthermore, guaranteeing access to this information is not only critical for due process rights, but also acts as an important safeguard to deter corner cutting and inappropriate use of face recognition during investigations.

Face Recognition Also Creates Risks of Pervasive Surveillance that is Fundamentally Incompatible with Democratic Society

One of the most important aspects of face recognition is that even if the government could mitigate the dangers of misidentification, doing so would not lessen the dangers of the technology as a whole. Simply put, face recognition surveillance is dangerous when it does not work, but also dangerous in a different — yet equally important — way when it does.

In the digital age, privacy rights do not just protect the inside of our homes from improper intrusion; they are also critical safeguards from overbearing government power. As Justice Sonia Sotomayor warned about emerging surveillance technologies when the Supreme Court first examined the issue of electronic location tracking, "making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track … may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[27]

---

[24] Aaron Mak, "Facing Facts," *Slate*, January 25, 2019, https://slate.com/technology/2019/01/facial-recognition- arrest-transparency-willie-allen-lynch.html.
[25] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[26] Face recognition "can play a significant role in investigations, though, without the judicial scrutiny applied to more proven forensic technologies." Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[27] *United States v. Jones*, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring).

If unrestrained in its use, face recognition surveillance offers so much information and power to government that it could upend basic rights and foundations of democracy. In authoritarian regimes such as China, face recognition is used as a means of social control, with the technology serving as a means of mass cataloging of activities and draconian enforcement of minor offenses.[28] It has been weaponized for continuous surveillance and brutal oppression of its Uighur minority.[29] It is used to identify, discourage, and detain pro-democracy protesters.[30]

The frightening abuse of face recognition technology is not limited to China. Officials in the U.S. have already used the technology to undermine fundamental features of democracy here.

According to a *South Florida Sun Sentinel* investigation, in 2020, law enforcement repeatedly used face recognition to identify and catalog peaceful protesters. Fort Lauderdale police ran numerous face recognition searches to identify people who might be a "possible protest organizer" or an "associate of protest organizer" at a peaceful Juneteenth event to promote defunding the police. Boca Raton police also ran face recognition scans on half a dozen occasions throughout May 2020 targeting protesters during peaceful events. And the Broward Sheriff's Office ran nearly 20 face recognition searches during this same time period for the purpose of "intelligence" collection, rather than to investigate any criminal offense.[31]

Face recognition has also been used to selectively target individuals who are protesting, with law enforcement using the technology to rapidly scan protests for individuals with active bench warrants for unrelated offenses. Several years ago, Baltimore police used face recognition amid protests to find individuals with "outstanding warrants and arrest[ed] them directly from the crowd," in a selective effort that appeared to be aimed at disrupting, punishing, and discouraging demonstrators from protesting.[32]

Federal Use of Face Recognition Should be Seriously Curtailed to Protect Civil Rights and Civil Liberties

Federal use of face recognition contains serious flaws, creating potential for both overreliance on misidentifications as well as misuse. The FBI systems guarantee that match results are returned for any scan, amplifying the risk of errors, as does the lack of oversight that stems from failure to disclose the use of face recognition to courts and defendants. FBI officials can conduct face

[28] Alfred Ng, "How China uses facial recognition to control human behavior," *CNet*, August 11, 2020, https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.
[29] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Drew Harwell and Eva Dou, "Huawei tested AI software that could recognize Uighur minorities and alert police, report says," *Washington Post*, December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.
[30] Paul Mozur, "In Hong Kong Protests, Faces Become Weapons," *New York Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html; Stephan Kafeero, "Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests," *Quartz Africa*, November 27, 2020, https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/.
[31] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?" *South Florida Sun Sentinel*, June 26, 2021, https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html.
[32] Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun*, October 11, 2016, https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

recognition searches pursuant to both criminal investigations or mere open assessments, meaning that searches do not require probable cause, or even suspicion of wrongdoing.[33]

ICE face recognition systems can similarly be used for photos that are "in furtherance of ongoing investigations," and can be used to support immigration detention and deportation so long as the scan is not conducted "solely in furtherance of civil immigration enforcement."[34]

The risks of face recognition being misused should be taken especially seriously in light of how federal law enforcement has used surveillance to target protesters[35] and the press in recent years,[36] as well as lawmakers, their staff, and their families.[37]

Currently, the only meaningful restriction on federal law enforcement use of face recognition is the FBI requirement that matches cannot serve as the sole basis for arrests or other law enforcement action.[38] But for the reasons previously described, requiring that face recognition is only used for leads does not eliminate the risk of error. And lack of disclosure to defendants removes a key safeguard in ensuring that even this rule is effectively applied.

In order to effectively reduce the dangers posed by face recognition surveillance, we recommend the White House establish the following policy requirements for all federal law enforcement use of the technology:

- **Probable cause rule:** Require that all scans be predicated on probable cause that the individual to be identified has committed, is committing, or is planning to commit the offense being investigated.
- **Serious crime limit:** Limit use of face recognition to the investigation of violent felonies.
- **Disclosure requirements:** Require that any use of face recognition during an investigation is disclosed to defendants.

---

[33] Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing before the House Committee on Oversight, 116th Cong. (June 4, 2019) (statement by Kimberly Del Greco, Deputy Assistant Director, FBI Criminal Justice Information Services Division), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use; Erin M. Priest, Privacy and Civil Liberties Officer, FBI, Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System (J2019).

[34] Department of Homeland Security, U.S. Immigration and Customs Enforcement, "Privacy Impact Assessment for the ICE Use of Facial Recognition Services," (May 13, 2020) https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

[35] Jimmy Tobias, "Exclusive: ICE Has Kept Tabs on 'Anti-Trump' Protesters in New York City," *The Nation*, March 6, 2019, https://www.thenation.com/article/archive/ice-immigration-protest-spreadsheet-tracking/.

[36] Tom Jones, Mari Payton, and Bill Feather, "Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database," *NBC 7*, March 6, 2019, https://www.nbcsandiego.com/investigations/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html; Ryan Devereaux, "Journalists, Lawyers, And Activists Working On The Border Face Coordinated Harassment from U.S. and Mexican Authorities," *The Intercept*, February 8, 2019, https://theintercept.com/2019/02/08/us-mexico-border-journalists-harassment/; Charlie Savage and Katie Benner, "Trump Administration Secretly Seized Phone Records of *Times* Reporters," *New York Times*, June 11, 2021, https://www.nytimes.com/2021/06/02/us/trump-administration-phone-records-times-reporters.html; Jana Winter, "Operation Whistle Pig: Inside the secret CBP unit with no rules that investigates Americans," *Yahoo News*, December 11, 2021, https://news.yahoo.com/operation-whistle-pig-inside-the-secret-cbp-unit-with-no-rules-that-investigates-americans-100000147.html?guccounter=1.

[37] Katie Benner, Nicholas Fandos, Michael S. Schmidt, and Adam Goldman, "Hunting Leaks, Trump Officials Focused on Democrats in Congress," *New York Times*, June 14, 2021, https://www.nytimes.com/2021/06/10/us/politics/justice-department-leaks-trump-administration.html.

[38] Erin M. Priest, Privacy and Civil Liberties Officer, FBI, Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System (May 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

Federal Assistance to State and Local Law Enforcement for Face Recognition Use is Dangerously Unregulated and Must be Reformed

In addition to its direct use by federal law enforcement, the federal government provides significant support for face recognition surveillance by state and local law enforcement, with inadequate safeguards.

The FBI Next Generation Identification-Interstate Photo System (NGI-IPS) provides state and local law enforcement across the country with the ability to run face recognition searches on a mass scale. Searches can be run through NGI-IPS so long as the relevant photos are "obtained pursuant to an authorized criminal investigation," but does not require probable cause or even suspicion of wrongdoing. FBI policy authorizes use of its system to identify exercising First Amendment-protected activities (such as lawful assembly and protests) so long as the scanned photo is "pertinent to and within the scope of an authorized law enforcement activity."[39]

These rules are insufficient to protect against pervasive surveillance and selective targeting, including the type of selective targeting that has previously been directed at peaceful protesters.

Further, FBI rules contain no known restrictions on which law enforcement entities are authorized to run scans through its systems, including those that may be under investigation by the Justice Department for systemic violation of constitutional rights — investigations the White House describes as "critical tools to promote constitutional policing in jurisdictions where reform is warranted."[40] This raises the important question of why the department would provide access to a powerful technology such as face recognition — which is susceptible to abuse and undermining constitutional rights — to police departments even as it acts to curtail systemic abuse within those departments.

Similar to its own policy rules, the FBI provides no meaningful restrictions on how state and local law enforcement use NGI-IPS for face recognition searches, other than to require that matches cannot serve as the sole basis for law enforcement actions such as arrests,[41] an inadequate measure to guard against both overreliance on misidentifications as well as misuse. Even when NGI-IPS is used in a proper manner for legitimate law enforcement needs, the consistent pattern of leaving defendants uninformed undermines critical due process rights to review investigative evidence and techniques.

Further, the federal government should examine and act on its role in promoting inadequately restricted face recognition systems that are operated at the state and local level. Federal grant

[39] Erin M. Priest, Privacy and Civil Liberties Officer, FBI, Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System (May 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.
[40] The White House, "FACT SHEET: The Biden-Harris Administration is Taking Action to Restore and Strengthen American Democracy," December 8, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/08/fact-sheet-the-biden-harris-administration-is-taking-action-to-restore-and-strengthen-american-democracy/.
[41] Erin M. Priest, Privacy and Civil Liberties Officer, FBI, Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System (May 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

funding for local policing has directly been used to create face recognition systems.[42] Federal funds are also used to develop mass video surveillance networks that power the collection of images run through local face recognition systems.[43]

The federal government bears responsibility if it — either by providing direct access to scans or funding for locally managed systems — enables state and local law enforcement to use face recognition in a manner that endangers civil rights and civil liberties, and should act to prevent such use. We recommend the White House establish the following policy requirements regarding assistance to state and local law enforcement involving face recognition:

- **Probable cause rule:** Only allow state and local law enforcement entities to run searches through NGI-IPS or other federal face recognition systems if scans are predicated on probable cause that the individual to be identified has committed, is committing, or is planning to commit the offense being investigated.
- **Serious crime limit:** Only allow state and local law enforcement entities to run searches through NGI-IPS or other federal face recognition systems if scans are for the investigation of violent felonies.
- **Prohibit use to bad actors:** Prohibit use of NGI-IPS or other federal face recognition systems by law enforcement entities under pattern and practice investigations for biased policing and other unconstitutional practices.
- **Disclosure requirements:** Require that any state and local law enforcement entity that uses NGI-IPS or other federal face recognition systems disclose such use to defendants.
- **Funding contingent on reasonable regulations:** Require that any state or local law enforcement entity that uses federal funding for face recognition or video surveillance that could be used for face recognition scans be conditioned on that entity abiding by these probable cause rules, serious crime limits, and disclosure requirements for its own use of face recognition.

Thank you for the opportunity to provide this comment in response to the White House Office of Science and Technology Policy's request for information. We strongly hope the White House will adopt the recommended policies in support of its ongoing commitment to civil rights, civil liberties, and improving racial equity in criminal justice and policing.

Sincerely,

Jake Laperruque

Senior Policy Counsel
The Constitution Project at the Project On Government Oversight

[42] See e.g., Department of Justice Bureau of Justice Assistance, "Facial Recognition Technology," September 6, 2016, https://bja.ojp.gov/funding/awards/2016-dj-bx-1049.
[43] See e.g., Aaron Mondry, "Criticism mounts over Detroit Police Department's facial recognition software," *Curbed Detroit*, July 8, 2019, https://detroit.curbed.com/2019/7/8/20687045/project-green-light-detroit-facial-recognition-technology.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Recording Industry Association of America

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Comments of the Recording Industry Association of America on the Office of Science and Technology Policy Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

Delivered via email to BiometricRFI@ostp.eop.gov

<RFI Response: Biometric Technologies>

January 14, 2022

The Recording Industry Association of America ("RIAA") welcomes this opportunity to respond to some of the questions posed by the Office of Science and Technology Policy ("OSTP") in its request for information ("RFI")[1] regarding public and private sector uses of biometric technologies.

The RIAA is the trade organization that supports and promotes the creative and commercial vitality of music labels in the United States, the most vibrant recorded music community in the world. Our membership – which includes several hundred companies, ranging from small-to-medium-sized enterprises to global businesses – creates, manufactures and/or distributes sound recordings representing the majority of all legitimate recorded music consumption in the United States. In support of its mission, the RIAA works to protect the intellectual property and First Amendment rights of artists and music labels; conducts consumer, industry, and technical research; and monitors and reviews state and federal laws, regulations, and policies.

RIAA's interest in this RFI relates primarily to general principles that should be employed whenever copyrighted sound recordings or music videos are used to train artificial intelligence enabled applications, including AI-enabled biometric technologies.

Introduction

The United States boasts over one million revenue-generating sound recording artists and songwriters.[2] Overall, the music industry contributes $170 billion to the nation's economy, supports 2.47 million jobs and accounts for over 236,000 businesses in the United States.[3] At the core of all this activity is the creativity of sound recording artists, songwriters, musicians, producers, recording engineers and countless other participants in the music industry that bring

[1] 86 Fed. Reg. 56,300 (Oct. 8, 2021).
[2] Source: http://50statesofmusic.com/?USimpact.
[3] Source: http://50statesofmusic.com/?USimpact.

music to life. Their creative output is protected by copyright, which is both recognized in the U.S. Constitution[4] and in the U.N. Universal Declaration of Human Rights.[5]

With this background in mind, we offer the following comments.

Question 6: Governance Programs, practices or procedures applicable to the context, scope, and data use of a specific use case.

To ensure that any AI enabled implementation is transparent, fair, and accountable, including any biometric AI enabled technology, the AI developer should implement the following processes:

Licensing and Clearances. The AI developer should use only those training materials for which either the AI developer has received appropriate licenses or clearances for the reproduction or other exploitation of those materials, or training materials that are in the public domain. OSTP should prohibit the use of any copyrighted materials for training unless the AI developer has received the appropriate licenses or clearances. Wholesale copying of sound recordings merely for the purpose of "training" an AI system is an insufficient basis for a finding of fair use, much like wholesale copying for the training of human students is not fair use.[6] As courts have found, where a use would not constitute fair use when done in the physical world, it does not constitute fair use in the digital world.[7] Similarly, where wholesale copying would not be considered fair use for teaching humans when performed with older technologies, it should not be considered fair use later when done to "teach" an algorithm with newer technologies. Accordingly, and to avoid harm to rights holders and mitigate the risk to AI developers, AI developers should obtain licenses or other clearance to use any copyrighted training materials, or they should instead rely on public domain materials.[8]

Record keeping. In addition, an AI developer should maintain adequate records of at least the following: what copyrighted works or other materials are being ingested by the AI process and

[4] U.S. Const. art. 1, § 8, cl. 8 ("To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries;").
[5] art. 27, § 2 ("Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author").
[6] *See e.g. Blackwell Publ'g, Inc. v. Excel Research Grp*., LLC, 661 F. Supp. 2d 786 (E.D. Mich. 2009) (third party copying copyrighted content in course packs without authorization to sell them to students not fair use); *Am. Geophysical Union v. Texaco, Inc*., 60 F.3d 913 (2d Cir. 1995) (copying of articles by researchers beyond what was permitted in the license for the articles was not fair use); *Weissmann v. Freeman*, 868 F.2d 1313 (2d Cir. 1989) (professor's unauthorized copying and distribution of a copyrighted article to his students not fair use); *Educ. Testing Serv. v. Katzman*, 793 F.2d 533 (3d Cir. 1986), abrogated on other grounds by *eBay, Inc. v. MercExchange, LLC*, 547 U.S. 388 (2006) (copying of a copyrighted test for test preparation education not fair use).
[7] *Brammer v. Violent Hues Prods*., LLC, 922 F.3d 255, 269 (4th Cir. 2019) ("Such a use would not constitute fair use when done in print, and it does not constitute fair use on the Internet.").
[8] OSTP should be wary of making any recommendations concerning the use of training materials under the fair use doctrine. The fair use doctrine is a fact-intensive inquiry that requires a deliberative analysis under the four factors for fair use set forth in 17 USC § 107. Therefore, relying on fair use should not be taken lightly or without a full grasp of the relevant facts of each particular situation.

for what purposes; copies of the licenses or clearances the developer has obtained to use the works or materials for such purposes; and what are the outputs of the AI process. Because AI ingestion or "training" will typically not happen in the public eye, it will be difficult if not impossible for copyright owners to monitor the unauthorized use of their intellectual property without such records. Proper record keeping of what content was ingested as part of the AI process should help ensure transparency and enhance accountability. In addition, such record keeping with respect to the licenses or clearances obtained will act as a check against rampant infringement in connection with AI inputs. It also can help track potentially problematic AI outputs, such as "deep fakes" or other outputs that may infringe intellectual property rights. This will help ensure fairness and build trust.

* * *

We thank OSTP for the opportunity to submit our views.

[redacted]
Victoria Sheckler
SVP, Deputy General Counsel
Recording Industry Association of America

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Robert Wilkens

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Friday, October 15, 2021 1:52:10 PM

In terms of Artificial Intelligence "diagnosing" cognitive abilities and mood:

-I am on Social Security Disability because a computerized test Diagnosed me as having [redacted] a Psychiatric Condition – This was around [redacted].

-Dr. [redacted] who was at [redacted] Medical Center at the time told me (1) I don't want that diagnosis (I did not understand), and also (2) It was because I answered the following question (from memory): "Have you ever heard voices that no one else could hear?" with Yes because I had definitely worn headphones/earbuds which other people probably could not hear. Psychiatrically a patient (whom didn't wear headphones) should have always answered no to that because they would believe the voices were really there.

-The diagnosis leads to medication which (if you research enough) you may find out can cause the conditions they would treat. An example would be because dopamine blocking medication ("anti-psychotics") cause more dopamine receptors to grow (for survival), and now if you withdraw too quick from the medication the problem is "worse" than it would've been without the medication. I'm not 100% convinced I can withdraw safely, but something called pruning suggests there may be a method.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Ron Hedges

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

ARTIFICIAL INTELLIGENCE DISCOVERY & ADMISSIBILITY CASELAW

(See generally, for a compendium of case law, etc., addressing electronic information in criminal investigations and proceedings, Understanding electronic information in criminal investigations and actions | Mass.gov)

People v. Wakefield, 175 A.D.3d 158, 107 N.Y.S.3d 487 (3d Dept. 2019)

> Defendant was subsequently charged in a multicount indictment in connection with the victim's death. Law enforcement collected a buccal swab from defendant to compare his DNA to that found at the crime scene. The data was eventually sent to Cybergenetics, a private company that used a software program called TrueAllele Casework System, for further testing. The DNA analysis by TrueAllele revealed, to a high degree of probability, that defendant's DNA was found on the amplifier cord, on parts of the victim's T-shirt and on the victim's forearm. . . At the *Frye* hearing, Supreme Court heard the testimony of Mark Perlin, the founder, chief scientist and chief executive officer of Cybergenetics, among others. Following the *Frye* hearing, the court rendered a decision concluding that TrueAllele was generally accepted within the relevant scientific community . . . Perlin also testified that TrueAllele is designed to have a certain degree of artificial intelligence to make additional inferences as more information becomes available. Perlin explained that, after objectively generating all genotype possibilities, TrueAllele answers the question of "how much more the suspect matches the evidence [than] a random person would," and the answer takes the form of a likelihood ratio. . . Supreme Court found that "there [was] a plethora of evidence in favor of [TrueAllele], and there [was] no significant evidence to the contrary" (47 Misc 3d at 859). In view of the evidence adduced at the *Frye* hearing, we find that the court's ruling was proper (see *People v Hamilton*, 255 AD2d 693, 694 [1998], *lv denied* 92 NY2d 1032 [1998]; see generally *People v Wesley*, 83 NY2d 417, 426-427 [1994]).

State v. Loomis, 371 Wis.2d 235, 881 N.W.2d 749 (2016)

> The defendant was convicted of various offenses arising out of a drive-by shooting. His presentence report included an evidence-based risk assessment that indicated a high risk of recidivism. On appeal, the defendant argued that consideration of the risk assessment by the sentencing judge violated his right to due process. The Supreme Court rejected the argument. However, it imposed conditions on the use of risk assessments.

State v. Morrill, No. A-1-CA-36490, 2019 WL 3765586 (N.M. App. July 24, 2019)

> Defendant asks this Court to "find that the attestations made by a computer program constitute 'statements,' whether attributable to an artificial intelligence software or the software developer who implicitly offers the program's conclusions as their own." (Emphasis omitted.) Based on that contention, Defendant further argues that the automated conclusions from Roundup and Forensic Toolkit constitute inadmissible hearsay statements that are not admissible under the business record exception. In so arguing, Defendant acknowledges that such a holding would diverge from the plain language of our hearsay rule's relevant definitions that reference statements of a "person." . . . Based on the following, we conclude the district court correctly determined that the computer generated evidence produced by Roundup and Forensic Toolkit was not hearsay. Agent Peña testified that his computer runs Roundup twenty-four hours a day, seven days a week and automatically attempts to make connections with and downloads from IP addresses that are suspected to be sharing child pornography. As it does so, Roundup logs every action it takes. Detective Hartsock testified that Forensic Toolkit organizes information stored on seized electronic devices into various categories including graphics, videos, word documents, and internet history. Because the software programs make the relevant assertions, without any intervention or modification by a person using the software, we conclude that the assertions are not statements by a person governed by our hearsay rules.

State v. Pickett, No. A-4207-19T4 (N.J. App. Div. Feb. 3, 2021)

> In this case of first impression addressing the proliferation of forensic evidentiary technology in criminal prosecutions, this appeal required the court to determine whether defendant is entitled to trade secrets of a private company for the sole purpose of challenging, at a *Frye* hearing, the reliability of science underlying novel DNA analysis software and expert testimony. *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). At the hearing, the State produced an expert who relied on his company's complex probabilistic genotyping software program to testify that defendant's DNA was present, thereby connecting defendant to a murder and other crimes. So long as the State utilized the expert, this court held that defendant is entitled to the discovery of the software's proprietary source code and related documentation under a protective order. [summary]

State v. Saylor, No. 2018-CA-14, 2019 WL 1313375 (Ohio App. March 22, 2019)

> [concurring opinion] Although it found Saylor to be indigent and did not impose the mandatory fine, the court imposed a $ 500 fine and assessed attorney fees and costs; the court also specifically disapproved a Risk Reduction sentence or placement in the Intensive Program Prison (IPP).
>
> {¶ 50} I have previously voiced my concerns about the almost unfettered discretion available to a sentencing court when the current case law apparently does not permit a review for abuse of discretion. *State v. Roberts*, 2d Dist. Clark No. 2017-CA-98, 2018-Ohio-4885, ¶ 42-45, (Froelich, J., dissenting). However, in this case, the trial court considered the statutory factors in R.C. 2929.11 and R.C. 2929.12, the individual sentences were within the statutory ranges, and the court's consecutive sentencing findings, including the course-of-conduct finding under R.C. 2929.14(C)(4)(b), were supported by the record.
>
> {¶ 51} As for the trial court's consideration of ORAS, the "algorithmization" of sentencing is perhaps a good-faith attempt to remove unbridled discretion – and its inherent biases – from sentencing. Compare *State v. Lawson*, 2018-Ohio-1532, 111 N.E.3d 98, ¶ 20-21 (2d Dist.) (Froelich, J., concurring). However, "recidivism risk modeling still involves human choices about what characteristics and factors should be assessed, what hierarchy governs their application, and what relative weight should be ascribed to each." Hillman, *The Use of Artificial Intelligence in Gauging the Risk of Recidivism*, 58 The Judges Journal 40 (2019).
>
> *9 {¶ 52} The court's statement that the "moderate" score was "awfully high," given the lack of criminal history, could imply that the court believed there must be other factors reflected in the score that increased Saylor's probable recidivism. There is nothing on this record to refute or confirm the relevance of Saylor's ORAS score or any ORAS score. Certainly, the law of averages is not the law. The trial court's comment further suggested that its own assessment of Saylor's risk of recidivism differed from the ORAS score. The decision of the trial court is not clearly and convincingly unsupported by the record, regardless of any weight potentially given to the ORAS score by the trial court. Therefore, on this record, I find no basis for reversal.

United States v. Shipp, 392 F.Supp.3d 300 (E.D.N.Y. July 15, 2019)

> The court has serious concerns regarding the breadth of Facebook warrants like the one at issue here. The Second Circuit has observed that "[a] general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be

> 'akin to a residence in terms of the scope and quantity of private information [they] may contain.'" Ulbricht, 858 F.3d at 99 (quoting Galpin, 720 F.3d at 445); see also Galpin, 720 F.3d at 447 (explaining that "[t]his threat demands a heightened sensitivity to the particularity requirement in the context of digital searches"). This threat is further elevated in a search of Facebook data because, perhaps more than any other location—including a residence, a computer hard drive, or a car—Facebook provides a single window through which almost every detail of a person's life is visible. Indeed, Facebook is designed to replicate, record, and facilitate personal, familial, social, professional, and financial activity and networks. Users not only voluntarily entrust information concerning just about every aspect of their lives to the service, but Facebook also proactively collects and aggregates information about its users and non-users in ways that we are only just beginning to understand. . . Natasha Singer, What You Don't Know About How Facebook Uses Your Data, N.Y. TIMES, Apr. 11, 2018, https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html (explaining that Facebook tracks users and non-users, collects biometric facial data, and "can learn almost anything about you by using artificial intelligence to analyze your behavior"). (See also Aff. ¶ 27 (explaining that "Facebook also provides its users with access to thousands of other applications ('apps') on the Facebook platform")). Particularly troubling, information stored in non-Facebook applications may come to constitute part of a user's "Facebook account"—and thus be subject to broad searches—by virtue of corporate decisions, such as mergers and integrations, without the act or awareness of any particular user. . . Compared to other digital searches, therefore, Facebook searches both (1) present a greater "risk that every warrant for electronic information will become, in effect, a general warrant," Ulbricht, 858 F.3d at 99, and (2) are more easily limited to avoid such constitutional concerns. In light of these considerations, courts can and should take particular care to ensure that the scope of searches involving Facebook are "defined by the object of the search and the places in which there is probable cause to believe that it may be found."

Wi-Lan Inc. v. Sharp Electronics Corp., 992 F.3d 1366 (Fed. Cir. 2021)

This was an appeal from an award of summary judgment of noninfringement. The district court held that the plaintiff lacked sufficient admissible evidence to prove direct infringement after it found a printout of source code inadmissible. The plaintiff sought to admit the source code to establish that systems used by the defendants "actually practiced" a methodology patented by the plaintiff. The Federal Circuit affirmed.

The plaintiff argued on appeal, among other things, that the source code printout was a business record that was admissible under the business records exception to the hearsay rule:

To establish that the source code printout was an admissible business record under Rule 803(6), Wi-LAN was required to establish by testimony from a 'custodian or other another qualified witness' that the documents satisfied the requirements of the Rule. Wi-LAN argues that it properly authenticated the source code printout through the declarations of the chip manufacturers' employees. We agree with the district court that the declarations could not be used to authenticate the source code printout on the theory that the declarations were a proxy for trial testimony or themselves admissible as business records.

As Wi-LAN notes, declarations are typically used at summary judgment as a proxy for trial testimony. But declarations cannot be used for this purpose unless the witness will be available to testify at trial. Under Federal Rule of Civil Procedure 56(c)(2), Wi-LAN was required to 'explain the admissible form that is anticipated.' Fed. R. Civ. P. 56(c)(2) advisory committee's notes on 2010 amendments. Wi-LAN argued that it met this burden by explaining that the declarants were available to testify at trial. The district court, however, found the opposite. Indeed, when asked by the court at the summary judgment hearing whether the declarants would appear at trial, Wi-LAN's counsel responded that Wi-LAN did not 'think that [it would be] able to force them to come to trial.' ***.

Wi-LAN thus did not establish that the declarants would be available to testify at trial and, as a result, the declarations could not be used as a substitute for trial testimony. *E.g., Fraternal Order of Police, Lodge 1 v. City of* Camden, 842 F.3d 231, 238 (3d Cir. 2016) (testimony admissible if declarants were available to testify at trial); *J.F. Feeser, Inc. v. Serv-A-Portion, Inc.,* 909 F.2d 1524, 1542 (3d Cir. 1990) ('[H]earsay evidence produced in an affidavit opposing summary judgment may be considered if the out-of-court declarant could later present the evidence through direct testimony, i.e., in a form that 'would be admissible at trial.'' (*quoting Williams v. Borough of West Chester*, 891 F.2d 458, 465 n.12 (3d Cir. 1989)).

Wi-LAN also seems to argue that it properly authenticated the source code printout because the declarations were custodial declarations that were themselves admissible as business records under Rule 803(6). Wi-LAN, however, admits that it obtained the source code printout and declarations by filing lawsuits against the manufacturers and then dismissing the lawsuits without prejudice after the manufacturers provided Wi-LAN with the source code printout and declarations it sought. Wi-LAN even explains that '[t]he lawsuits were necessary to secure production of the source code and declarations because [the system-onchip manufacturers] had refused to cooperate in discovery.' ***. *The declarations thus do not constitute a 'record [that] was kept in the course of a regularly conducted activity of a business.' Fed. R. Evid. 803(6)(B). Instead, the declarations were created and prepared for the purposes of litigation, placing them outside the scope of the exception. As a result, the declarations were not*

admissible as business records for use to authenticate the source code printout. [emphasis added].

The Federal Circuit also rejected the plaintiff's reliance on Rule 901(b)(4):

Wi-LAN also appears to argue that the district court should have found the source code printout admissible under Federal Rule of Evidence 901(b)(4). Rule 901(b)(4) permits a record to be admitted into evidence if '[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances' 'support a finding that the item is what the proponent claims it is.' Fed. R. Evid. 901(a), (b)(4).

In support of its Rule 901(b)(4) argument, Wi-LAN states only that 'there was no legitimate reason to question the trustworthiness of the source code.' ***. The district court concluded that the source code printout's 'appearance, contents, substance, internal patterns, [and] other distinctive characteristics,' Fed. R. Evid. 901(b)(4), did not satisfy Rule 901(b)(4)'s strictures 'given the highly dubious circumstances surrounding the production and the lack of indicia of trustworthiness in the source code,' ***, as described in the previous Section. On this record, the district court did not abuse its discretion in refusing to treat the source code printout as evidence under Rule 901(b)(4).

Moreover, the Federal Circuit rejected the plaintiff's reliance on Rule 703:

Wi-LAN alternatively argues that the source code printout should have been admitted into evidence under Federal Rule of Evidence 703.4 Wi-LAN's expert submitted a report stating that Sharp's and Vizio's television sets infringe the claimed methods of the '654 patent by the use of the source code. Wi-LAN's expert did not attempt to authenticate the source code printout. But Wi-LAN argues that its expert should be able to opine on the meaning of the inadmissible source code printout and to provide the inadmissible source code printout to the jury despite Wi-LAN's failure to authenticate the source code printout.

Wi-LAN's argument presents two separate and distinct questions: (1) whether the source code printout was admissible because it was relied on by the expert and (2) whether the expert's testimony relying on the source code was admissible to establish infringement. The answer to the first question is 'no' because expert reliance does not translate to admissibility. The answer to the second question is also 'no' because Wi-LAN did not establish that experts in the field 'reasonably rely on' unauthenticated source code.

Concluding its discussion of admissibility, the Federal Circuit rejected the plaintiff's argument that it should have extended discovery:

In light of these admissibility issues, Wi-LAN's fallback position is that the district court should have granted it additional time to obtain an admissible version of the source code. We

disagree. Wi-LAN had ample time to obtain the source code and to find custodial witnesses to authenticate the source code over the course of discovery but failed to do so.

Wi-LAN had been on notice since early 2016 that it was going to need the system-on-chip source code from third parties to prove its direct infringement case. Throughout the litigation, Wi-LAN repeatedly requested extensions of time to obtain the source code from the third-party manufacturers. Ultimately, however, Wi-LAN only procured a single printout version of the source code with declarations after suing the third-party manufacturers.

Wi-LAN, as the district court found, 'had ample time and opportunities over years of litigation to obtain evidence of infringement from the [system-on-chip] manufacturers' but failed to do so. ***. Given this record, the district court did not abuse its discretion in denying Wi-LAN an additional opportunity to obtain an admissible form of the source code.

And, for something different: *Thaler v. Hirshfeld,* No. 1:20-cv-00903-LMB-TCB, 2021 WL 3934803 (E.D. Va. Sept. 2, 2021)

This was an appeal from the refusal of the USPTO to process two patent applications. The plaintiff alleged that he was the owner of DABUS, "an artificial intelligence machine" listed as the inventor on the applications. The applications included a document through which DABUS had "ostensibly assigned all intellectual property rights" to the plaintiff. The court held:

Before the Court are the parties' cross-motions for summary judgment, which address the core issue—can an artificial intelligence machine be an 'inventor' under the Patent Act? Based on the plain statutory language of the Patent Act and Federal Circuit authority, the clear answer is no.

***

*** plaintiff's policy arguments do not override the overwhelming evidence that Congress intended to limit the definition of 'inventor' to natural persons. As technology evolves, there may come a time when artificial intelligence reaches a level of sophistication such that it might satisfy accepted meanings of inventorship. But that time has not yet arrived, and, if it does, it will be up to Congress to decide how, if at all, it wants to expand the scope of patent law.

RJH rev. 9/11/21

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Science, Technology, and Public Policy Program at University of Michigan Ann Arbor

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

GERALD R. FORD SCHOOL OF PUBLIC POLICY
UNIVERSITY OF MICHIGAN

January 15, 2022

Dr. Eric Lander
Director
Office of Science and Technology Policy
1600 Pennsylvania Ave NW
Washington, DC 20500

Re: Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Dear Dr. Lander,

Thank you for the opportunity to comment on the question of regulating AI-enabled biometric technologies. I am writing in my capacity as Director of the Science, Technology, and Public Policy (STPP) program. The STPP Program is a research center based in the Gerald R. Ford School of Public Policy at the University of Michigan in Ann Arbor. Our mission is to address urgent questions at the intersection of science, technology, policy, and society, with the aim of producing more just and equitable science and technology policies. We bring a rigorous interdisciplinary lens to understanding these concerns, and translating them to policymakers, engineers, scientists, and civil society.

STPP's research team recently conducted an investigation of the potential implications of using facial recognition (FR) technology in schools, and our findings are that FR brings many harms with very few rewards. Some of these harms have already been realized (See https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition-technology-schools for the full report and additional documentation).

On this basis of this research, we strongly recommend that facial recognition be banned in school settings, on the basis of the far-reaching harm it is capable of; however, should schools proceed with its implementation, we have policy recommendations regarding its development, deployment, and regulation.

Exhibited and potential harms of facial recognition in schools

FR perpetuates racism and other forms of bias. Using FR technology in schools is likely to amplify, institutionalize, and potentially weaponize existing racial biases, resulting in disproportionate surveillance and humiliation of marginalized students. It is likely to mimic the impacts of school resource officers (SROs), stop-and-frisk policies, and airport security. All of these interventions purport to be objective and neutral systems, but in practice they reflect the structural and systemic

biases of the societies around them. All of these practices have had racist outcomes due to the users of the systems disproportionately targeting people of color.

These cases have also revealed that technologies that target subjects along racist lines result in negative psychological and social outcomes for these subjects, in this case school children. The use of metal detectors in schools decreases students' sense of safety, for example. Because FR is a similar surveillance technology that has potential to amplify user biases, it is likely that FR systems in schools will disproportionately target students of color, harming them psychologically and socially. Finally, FR algorithms consistently show higher error rates for people of color, with white male subjects consistently enjoying the highest accuracy rates. In sum, students of color are more likely to be targeted by FR surveillance and more likely to be misidentified by FR. multiplying the negative impacts of the tool.

FR brings state surveillance into the classroom. Implementing FR in schools will normalize the experience of being constantly surveilled, starting at a young age. Furthermore, once implemented, it will be hard to control how administrators use FR and for what purposes. The case of closed- circuit television (CCTV) reveals how surveillance technologies can undergo mission creep: CCTV systems in secondary schools in the United Kingdom (UK) were originally instituted for school security, but in practice became most often used for monitoring student behavior. It is likely that FR will also undergo mission creep as administrators expand the usage of the technology outside of what was originally defined. The normalization of surveillance will result in negative psychological and social effects for students. Several cases demonstrate that surveillance technologies make subjects feel powerless, as they feel that they are always being watched. This is likely to be replicated with FR in schools. Finally, limited data protections in the face of widespread surveillance puts subjects' privacy at greater risk, and this would also be a significant risk for children in schools with FR systems.

FR punishes nonconformity. FR in schools is also likely to discipline young people in unexpected ways, by narrowing the definition of the "acceptable student" and punishing those who fall outside that definition. For example, CCTV systems in UK secondary schools led many students to reclassify their expressions of individuality and alter their behavior. Students reported that their style of dress seemed to influence how likely they were to be disciplined, meaning that non-criminal expressions of individuality could warrant punishment for students. Students also reported avoiding certain areas where they were likely to be surveilled, and behaving in ways less likely to draw attention. Additionally, FR is likely to further marginalize minority groups, as India's Aadhaar system did. Aadhaar excludes citizens who have damaged fingerprints or eyes, which disproportionately impacts marginalized people including manual laborers and leprosy patients. This often means that these individuals are unable to access food rations or welfare, thus harming groups that were already disadvantaged.

FR in schools is likely to similarly exclude students, given that students of color, immigrant students, students with disabilities, gender non-conforming students, and low-income students all are likely to have lower accuracy and higher flag rates both automatically due to the design of FR and by human administrators of the system. Depending on how the school is using FR, this could result in already marginalized students being incorrectly marked absent for class, prevented from checking out library books or paying for lunch. FR systems in schools are poised to privilege some students and exclude and punish others based on expressions of individuality and characteristics outside of their control.

FR companies profit from children's personal data. FR in schools is likely to generate new data on students and create new markets in commodifying student data. Previous experience with similar data-generating technologies suggests that providers of these technologies will seek to commodify data collected, creating concerns about ownership, consent, value, and market exploitation. Providers may even offer FR services at no cost in exchange for the ability to collect and monetize the data. There is limited legal and policy clarity about whether citizens own their data. Most cases suggest that though citizens do not have ownership over their biometric data, they have a right to full, informed consent. This framing has been reinforced by the dozens of biobanks that scientists and governments have created over the last few decades, which assert ownership over human DNA samples and other specimens, along with their resulting data. However, given the design of FR tools, which are meant to be applied broadly to any and all faces that move through or near a given system, advance consent may be difficult or impossible to obtain. Further, there is concern that making biometric data collection a routine part of school life, especially without any explicit discussion about where and how to release this data, teaches students that it is normal and unremarkable to give away biometric data and have it used to track your location, purchases, and activities. Altogether, our analysis indicates that the institution of FR in schools threatens students' data privacy and security, will result in data collection without consent, and will create a culture of permissiveness regarding data collection, leaving children particularly vulnerable to unauthorized use of their personal information.

FR is inaccurate. Establishing and maintaining accuracy in FR systems in schools will likely be very difficult. FR is neither as accurate nor as unbiased as developers claim it will be, meaning that users likely will have misaligned expectations of the technology, and be willing to entrust it with work for which it is fundamentally unsuited. In addition, while FR is seductive because the automated face-matching process seems to side step individual biases, humans and our judgment are involved at every step. For example, just as humans make final matching determinations with closed- circuit television (CCTV) and fingerprinting, so will they with FR technology. As we have seen in those cases, though these technologies are often automatically accepted by users as objective and highly accurate, they are actually influenced by human bias and error. Additionally, the lack of regulation surrounding the breathalyzer suggests that a similar lack of regulation of FR in schools could result in errors in the calibration of the technology and in how results are interpreted. Some may argue that

the way to address these problems is through enhanced accuracy. But perfect accuracy would potentially make FR in schools even more damaging in the ways described above.

Further, cases of similar technologies illuminate how excitement over a technological fix can lead to entrenchment, even if the tool is not necessarily accurate. These cases also show the sustained resources and training needed to maintain accuracy, the difficulty of assessing accuracy for low-probability events, the problems with having courts as the ultimate arbiters of accuracy, the racial bias that is embedded in surveillance technologies, and the challenge of having local officials determine accuracy among heterogeneous products. Overall, it is difficult to imagine how FR systems will establish and maintain a high level of accuracy in schools.

Recommended governance for facial recognition in schools

Owing to the overwhelmingly adverse effects observed and anticipated when implementing and using facial recognition in schools, **we strongly recommend that FR technology be banned in schools**. However, recognizing that such technology is likely to be implemented, accepted, and eventually pervasive, we have outlined recommendations that would serve to mitigate the harmful effects of FR and allow for fair, safe, and ethical use whilst protecting the privacy and mental and social well-being of vulnerable student bodies. Should FR be introduced into schools, we urge caution and extensive deliberation to ascertain whether such investments are ultimately beneficial. Public input, especially from the most vulnerable stakeholders – students of color, the disabled, gender-nonconforming individuals, and immigrants – must be considered and factored into decision-making, and investment based on supposed technological accuracy must be superseded by considerations of the technology's impacts on social, ethical, racial, and economic dimensions inherent in school systems. As existing laws and policies are insufficient to manage the novelty, emergence, and potential scope and power of FR, clear and robust regulations are necessary to protect students; laws must also allow for periodic revision and opportunities for regulatory change, as FR technology evolves and consequences become clear, and as new challenges arise.

Policy Recommendations: National Level

1. Implement a **nationwide moratorium** on all uses of FR technology in schools. The moratorium should last as long as necessary for the national advisory committee to complete its work and for the **recommended regulatory system** to be fully and safely implemented on a national level. We anticipate that this process, and hence this moratorium, will last **5 years**.
2. Enact comprehensive data privacy and security laws if they are not already in place.
3. Convene a national advisory committee to investigate FR and its expected implications, and to recommend a regulatory framework to govern this technology. The national advisory committee should be **diverse in terms of both demographic and professional expertise**. This committee should include experts in: technical dimensions of FR (e.g., data scientists); privacy, security, and civil liberties laws; social and ethical dimensions of technology; race

and gender in education; and child psychology. The committee should also include those involved in kindergarten through high school (K-12) operations, including teachers, school administrators, superintendents, high school students, and parents or guardians of elementary and middle school students. Government officials from relevant agencies (e.g., in the US, the Department of Education and Federal Communications Commission) should be invited to participate in the committee as ex officio members; they could provide important insight into the regulatory options available. Representatives of FR companies should be invited to testify periodically in front of the committee, so that their perspectives can be considered in the regulatory process. Finally, efforts should be made to elicit community perspectives, ideally through **deliberative democratic efforts**.

4. Create **additional oversight mechanisms** for the technical dimensions of FR

Policy Recommendations: State Level

If a state allows FR in schools, it should create programs and policies that fill in any gaps left by national policy as well as establishing new infrastructure for the oversight and management of district-level FR use.

5. **Convene a state-level expert advisory committee to provide guidance to schools and school districts**, if a regulatory framework is not created at the national level. There should be a moratorium on adopting FR in schools until this guidance has been provided.
6. **Establish technology offices**, perhaps within state departments of education, to help schools navigate the technical, social, ethical, and racial challenges of using FR and other emerging educational technologies. These offices should also **provide resources and oversight** to ensure that school and district staff are properly trained to use FR technology in a way that is consistent with state laws.

Policy Recommendations: School and District Level

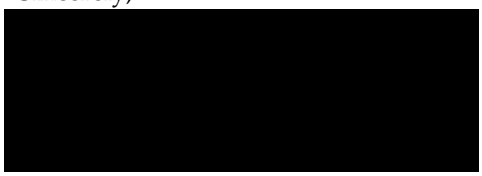
Schools and school districts are directly responsible for the installation and operation of FR, and for any disciplinary action that follows from identification, so they are responsible for most of the oversight actions.

7. If any alternative measures are available to meet the intended goals, do not purchase or use FR.
8. Perform a thorough evaluation of FR, including ethical implications, before purchasing it. This is even more crucial in the absence of national regulations or state-level guidance.
9. Develop a plan for implementing the technology before using it.
10. Do not purchase FR systems that use student social media accounts to improve the technology.
11. Do not use FR technology to police student behavior.
12. Delete student data at the end of each academic year or when the student graduates or leaves the district, whichever comes first.
13. Employ at least one person dedicated to managing and maintaining the FR technology in each school.

14. Provide regular, age appropriate guidance to parents, guardians, and students that includes information about why the school has deployed FR, how it will be used, how data will be managed, and what protections are in place to ensure accuracy and equity
15. Establish a pilot period and re-evaluation process before full-scale implementation of the technology.

In conclusion, we appreciate OSTP's efforts to investigate biometric technologies. We believe the evidence fully supports increased regulation of these technologies to protect Americans from their potential harms. Thank you in advance for your consideration of our comments.

Sincerely,



Shobita Parthasarathy, Ph.D.
Professor
Director, Science, Technology, and Public Policy program
Gerald R. Ford School of Public Policy
University of Michigan
[redacted]
https://stpp.fordschool.umich.edu/

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Security Industry Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Submitted Electronically
January 15, 2022

Dr. Eric S. Lander
Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

Dear Director Lander:

On behalf of the Security Industry Association (SIA), we are pleased to submit comments in response to the Office of Science and Technology Policy (OSTP) Request for Information (RFI) on the Public and Private Sector Uses of Biometric Technologies, which seeks stakeholder input regarding the proliferation of biometric technologies that positively impact our society, secure critical infrastructure, and bolster U.S. and allied leadership in research and development (R&D) of these advanced technologies.

SIA represents more than 1,100 security solutions providers, ranging from large global technology firms to local small businesses. Our membership includes manufacturers, software developers, and systems integrators that install and maintain security technology for end users in both the government and commercial sectors. SIA members provide robust security solutions that protect people, sensitive data and networks, physical structures, proprietary information, and vital U.S. national security interests.

SIA's Role in Promoting the Responsible Use of Biometrics

Advances in biometrics modalities such as facial recognition, fingerprint matching and iris recognition, are dramatically improving the performance of authentication, access control and security systems and other technology solutions our industry produces that benefit society in many ways. U.S. government agencies,[1] law enforcement,[2] and commercial sectors[3] are expanding their investments and adoption of biometrically enabled solutions across many applications due the advantages they provide. As an association of developers and suppliers of

[1] https://www.gao.gov/assets/gao-21-526.pdf; https://www.gao.gov/assets/gao-20-568.pdf
[2] https://www.gao.gov/assets/gao-21-435sp.pdf
[3] https://www.gao.gov/assets/gao-20-522.pdf

these technologies, SIA is committed to helping ensure that end-users employ biometrics technologies in a lawful, ethical, and nondiscriminatory manner.

SIA and our members continue to develop research, implementation guidance, public policy proposals and other resources to illustrate how biometrics, when used appropriately and for purposes that are clearly defined, provide specific and important benefits to our society. Some examples include: 1) SIA's letter to President Biden and Vice President Harris[4] urging the administration and Congress to consider policies that enable American leadership in developing biometric technologies; 2) policy principles[5] that guide the commercial sector, government agencies and law enforcement on how to use facial recognition in a responsible, ethical and nondiscriminatory manner; 3) comprehensive public polling[6] on facial recognition use across specific applications.

Public Sector Biometrics Applications

SIA members actively contribute and supply biometrics solutions to the following federal agencies and sub-agencies:

- **U.S. Department of Justice:** Under the FBI's Criminal Justice Service unit, SIA members support the CJIS division's biometrics programs involving fingerprint, palm print, iris and facial recognition capabilities. For example, for facial recognition queries against criminal records, CJIS uses the FBI Next Generation Identification (NGI) System in conjunction with the Interstate Photo System (IPS) and the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit. Both NGI-IPS and FACE enable state and local law enforcement to probe photo searches against criminal databases and support investigatory efforts to crack cold cases, solve violent crimes, and find missing children.
- **U.S. Department of Defense**: The U.S. Army has long supported advanced biometric programs and systems that aide warfighters in identifying suspected terrorists and persons of interest abroad. Army personnel leverage biometric capture devices that incorporate fingerprint, facial and iris recognition modalities to uncover and disseminate contextual data during mission-critical scenarios. The Army has also integrated facial recognition systems into processes that aim to facilitate efficient, secure base access control.
- **U.S. Department of Homeland Security (DHS):** For testing the accuracy of facial and iris recognition algorithms, a considerable number of SIA members participate in DHS's annual Biometric Technology Rally – a multistakeholder forum that invites biometric vendors and experts to objectively measure biometric performance under end user-specific use cases, such as traveler screening, high-throughput scenarios, and face masks.[7]
- **U.S. Customs & Border Protection (CBP):** CBP's *Biometric Entry/Exit* program supports air entry and exit identification processing of passengers – with facial recognition being the predominant modality. As a voluntary means for a traveler to verify

[4] https://www.securityindustry.org/report/sia-letter-to-president-and-vice-president-on-facial-recognition/
[5] https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/.
[6] https://www.securityindustry.org/report/u-s-public-opinion-research-on-the-support-of-facial-recognition/.
[7] https://www.dhs.gov/science-and-technology/biometric-technology-rally.

their identity, CBP facial recognition systems enable travelers to navigate through airport checkpoints securely and seamlessly. [8] At ports of entry, to date, CBP has identified more than 1,100 imposters (individuals attempting to illegally enter the country under false identities) by utilizing facial recognition technology.[9]

- **U.S. Department of State:** Pursuant to federal law, visa applicants are required to submit fingerprint data prior to an application's review. Under the State Department's *Antiterrorism Activities* programs, the department has deployed several identification, comparison, and evaluation systems that integrate biometrics technology to detect fraudulent travel documents at domestic and international locations.
- **Transportation Security Administration (TSA):** TSA utilizes SAFETY Act certified biometric modalities to expedite passenger flow while enhancing security protocols needed to authenticate identification credentials. Additionally, TSA's Trusted Traveler Programs, such as TSA Pre-check and the Registered Traveler Program, rely on biometric data submitted by a traveler during the enrollment and security screening stages.

The National Institute of Standards and Technology (NIST) supports development of high-quality biometric technologies suitable for government use through its testing and evaluation programs. For example, led by NIST's Information Technology Laboratory Image Analysis Unit, the facial recognition vendor test (FRVT) program assesses the capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. Viewed worldwide as the gold standard for objectively testing algorithm performance, most SIA members developing facial recognition solutions submit their algorithms for testing and evaluation. Many SIA members submit other biometric algorithms, including fingerprint[10] and iris[11] algorithms, to NIST tests as well.

Commercial Biometrics Applications

Here are some examples of commercial sectors to which SIA members supply biometrics solutions:

- **Airlines**: Most flagship airlines have adopted facial recognition systems as a method to expeditiously board passengers without having desk and gate agents manually check travel documents. According to polling that SIA commissioned[12] and various reporting conducted by CBS[13] and NBC,[14] travelers overwhelmingly support airline use of this technology since it reduces wait times and improves airline efficiency.

[8] https://biometrics.cbp.gov/.
[9] https://www.cbp.gov/newsroom/local-media-release/cbp-expands-simplified-arrival-four-ports-entry-washington-state.
[10] https://www.nist.gov/programs-projects/fingerprint-recognition.
[11] https://pages.nist.gov/IREX10/.
[12] https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/.
[13] *https://www.cbsnews.com/news/facial-recognition-delta-tsa/; https://www.cbsnews.com/video/airlines-using-facial-recognition-technology-to-reduce-wait-times-ahead-of-holiday-travel-season/*
[14] https://www.nbcnews.com/nightly-news/video/how-facial-recognition-will-change-the-way-you-travel-124677189642

- **Hospitality & Entertainment**: To enhance the customer experience, hotels, sports stadiums, and concert venues are increasingly incorporating biometric platforms to accelerate check in and, in certain cases, provide contactless identity verification at select venues.
- **Retail & Financial Services:** The seamless interaction between consumer and mobile device now enables the financial sector to leverage biometric authentication features that provide more security for mobile transactions and enrollment. Additionally, the financial services industry is adopting biometric solutions to curb and detect fraudulent transactions.
- **Healthcare:** Biometrics are used to verify patient identification prior to major medical procedures and administering medications, ensure authorized access to clean rooms and other secure areas, as well as provide a touchless interface limiting the need for front-line health workers to swipe badges or type in codes.
- **Critical Infrastructure:** Biometrics are used to secure critical infrastructure that provide and deliver among other things the nation's communications, energy, water and transportation services, and manufacturing facilities that produce our nation's energy, food and medicine.

SIA Response to OSTP RFI

OSTP's *Federal Register* notice structures the RFI to allow stakeholders to comment on six key points germane to the use of biometric technologies and data. Furthermore, OSTP held two listening sessions that featured participants representing diverse industries and organizations. SIA and several of our members appreciated the opportunity to participate in both events, and we commend OSTP for convening multi-stakeholder forums to provide the Office with a range of perspectives on biometrics use across both routine and complex applications.

However, before we respond to each individual point noted in the RFI, it is imperative to address the recent calls to ban or place a moratorium on the use of facial recognition and several other biometric technologies. SIA firmly opposes legislation, policies, and funding restrictions that directly or indirectly impose a blanket ban or moratorium on the use of biometric technologies.[15]

Rather than enact sweeping, harmful bans or moratoriums, policymakers should work earnestly to construct balanced legislation that preserves proven benefits, creates reasonable safeguards and maintains U.S. leadership in the development of these technologies. Forums that allow diverse participants to build relationships and engage in frank, off-the-record dialogue over an adequate timeframe, will afford the best opportunity for policymakers to work with stakeholders to find areas of agreement and identify needed polices regarding advanced biometric technologies.

Point No. 1: Descriptions of use of biometric information for recognition and inference.

SIA represents companies that focus on safety and security solutions, in which biometrics technologies (as defined in the RFI) are typically utilized for identification, and verification purposes, versus inference of attributes.

[15] https://www.securityindustry.org/2021/06/16/security-industry-association-opposes-reintroduction-of-facial-recognition-biometric-technology-moratorium-act/.

For example, as explained below, facial recognition, as defined by NIST and understood in the industry, is used for two distinctly different types of applications: *verification*, which helps determine that a person is who they claim to be, and *identification*, which generally helps human analysts determine whether an image of an unknown person matches an identity in a specific database.

- **Verification (also referred to as authentication)** – helps verify a person is who they claim to be.
    - In this case, the system checks data derived from a submitted photo or live image against an existing template to verify that it is the same person, hence the term one-to-one (or 1:1) matching. Performance is measured by the verification rate – the rate at which the system correctly verifies that a pair of images are of the same person based on the similarity score. The primary benefit of this configuration is providing an additional factor for authenticating an individual and greater assurance that an individual is who they are claiming to be. This configuration is applicable to banking, electronic payment, personal electronic device unlocking, employee time and attendance, secure building or door access for employees and guests, air traveler entry-exit and other border crossing systems, passports, preventing identity theft and fraud and other uses.

- **Identification (also referred to as discovery)** – helps determine who a person is.
    - In this case, the system compares data derived from a probe photo or live image of an unknown person to a set of existing templates in a gallery or database. This is called one to many (or 1:N) matching. Searches of the data set using an algorithm return a match candidate or group of match candidates based on the similarity score. If there are no close potential matches, none are returned. Performance is measured by the accuracy rate – the rate at which the matching image is returned as a candidate – or, conversely, the failure rate – the rate at which a matching image is not returned despite being in the data set.

    - The primary benefit of this configuration is that it automates the initial step of sifting through large numbers of photos, where it is more efficient, objective and accurate than human analysts performing this same initial step manually prior to reviewing potential matches, with established morphological practices similar to latent print analysis.

Point No. 2: Procedures for and results of data driven and scientific validation of biometric technologies.

The RFI notes that "*Many concerns have been raised about the use of biometric technology, ranging from questions about the validity of the underlying science; differential effectiveness, outcomes, and harms for different demographic groups…"* Policymakers should look to established and reliable U.S. testing programs such as NIST's testing programs for facial recognition, iris and other modalities, and DHS's Biometrics Tech Rally, for the most accurate, independent, and objective scientific information on biometric technology performance.

This is the widespread consensus among biometric vendors, academic experts, data scientists, and international partners. Unfortunately, there are many examples where non-scientific tests of publicly available facial recognition algorithms have yielded inaccurate information and generalizations about accuracy, and media reports have mischaracterized early research.

NIST FRVT:
In NIST's 2019 report that specifically evaluated facial recognition algorithms' performance across demographic groups, NIST found that top-performing algorithms exhibited "undetectable" differences in false positive error rates across demographic groups.[16] And according to data from a more recent evaluation in 2021, each of the top 150 facial recognition algorithms tested by NIST are over 99% accurate in matching photos across Black male, white male, Black female and white female demographics.[17] For the top 20 algorithms, accuracy of the highest performing demographic versus the lowest varied only between 99.7% and 99.8% true accept rates. Unexpectedly, white male was the lowest performing of the four demographic groups for the top 20 algorithms. For 17 of these algorithms, accuracy for white female, Black male and Black female are nearly identical at 99.8%, while they are least accurate for the white male demographic at 99.7%.

NIST research on facial recognition has documented massive improvements overall accuracy in recent years, noting even in 2018[18] the software tested was at least 20 times more accurate than it was in 2014, and in 2019 finding "close to perfect" performance[19] by high-performing algorithms with "miss rates" against a database of 12 million images averaging 0.1%. On this measurement, the accuracy of facial recognition is reaching that of automated fingerprint comparison,[20] which is generally viewed as the gold standard for identification.

DHS Biometrics Tech Rally:
Facial and iris recognition systems tested during DHS's most recent Biometrics Technology Rally exhibited significant advancements under high-stress testing scenarios, such as high throughput and testing accuracy with the use of face masks.[21] Given the unpredictable travel environment due to COVID-19, biometric vendors welcomed these changes in testing procedures since it fully examined how facial and iris recognition systems can adapt in different scenarios.

To underscore and reinforce the significant progress, technological improvements, and broader public perception, here are the most notable 2020 metrics:

[16] *See* pp. 4, 8 – https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; *see also* https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/.
[17] https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/.
[18] https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.
[19] https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49.
[20] https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf.
[21] *See DHS S&T Summary of 2020 Biometrics Technology Rally,* https://www.dhs.gov/science-and-technology/biometric-technology-rally#.

- On efficiency without face masks, which averages transaction times for volunteers at rally stations, all five facial recognition systems met or exceeded the minimum threshold for a transaction time of no more than eight seconds.
- For satisfaction without face masks, which tests volunteer attitudes towards the facial recognition acquisition systems, all five facial recognition systems met or exceeded the 90 percent satisfaction threshold, and the most accurate achieved over 99% accuracy.
- For matching true identification rate (TIR), which measures TIR expressed as the percentage of acquired images that were correctly – the most common measurement for traveler identification at ports of entry – 47 out of 60 tested face system combinations met the threshold without masks. Thus, S&T classified these 47 systems as a "high-throughput system."
- TIR rates with masks were expectedly lower, but S&T staff contend that the accuracy rates exceeded expectations, and the top-performing system was over 98% accurate.

Point No. 3: Security considerations associated with a particular biometric technology.
Generally, biometric templates used in advanced comparison technologies cannot be reverse engineered to reconstruct a person's biometric traits like a face or fingerprint. This engineered architecture adds an additional layer of privacy and security. Moreover, biometric data transmission, storage and processing should be optimized to ensure privacy and security using encryption and other cybersecurity and privacy best practices that protect biometric data. Solutions should follow a distributed data approach by limiting biometric data stored in central repositories and storing this data in the form of encrypted digital templates rather than original images. Each developer measures and records templates differently, providing an additional layer of security by making this data useless if compromised, either for identification or as a credential outside of the system that created it. As with processing algorithms, advances are being made in data security with techniques such as homomorphic encryption that allows processing without decrypting data.

Outside and apart from the software and database used to create the faceprint, a faceprint by itself does not contain any personally identifiable information and cannot be used to re-create the digital image it was derived from. Each vendor uses a different process to create and compare faceprints unique to that particularly proprietary software. A faceprint created in one system cannot be used within in another. In this way, a faceprint created using mathematical vectors acts as secure cryptography, preventing identity hacking even if data is stolen, and naturally serves to limit unauthorized use by third parties. Thus, necessary data security measures are not any greater for faceprints than they would be for fingerprints or photos.

Point No. 4: Exhibited and potential harms of a particular biometric technology.
With virtually any technology, there are risks that manufacturers and users must account for throughout the development and operational use of products. These can involve both how technology itself performs and how it is used by human operators. This is no different for biometric technology. Using facial recognition as an example, given the demonstrably high performance and accuracy rates evidenced by NIST's recent FRVT reports detailed above, the assertion often repeated in media accounts that facial recognition technology is inherently less accurate for certain demographics is flatly inaccurate.

However, if used inappropriately, we recognize that even biometric technologies that perform highly accurately overall and across demographic groups can still pose risks to privacy, civil rights, civil liberties, and human rights. We have also seen examples where authoritarian governments have used advanced biometric technologies in ways that violate privacy and other human rights. Countries that lack a strong rule of law and commitment to human rights cannot, and should not, lead in development and performance in biometrics technologies. Many of the top participants in NIST's facial recognition vendor test are Chinese companies – and in some cases, listed on the Bureau of Industry & Security "Entity List." U.S. leadership, in partnership with close allies and other democratic countries, in modeling responsible biometrics development and use is important to establish a standard of practice abroad that supports human rights, rejects and prevents mass-surveillance practices, and bolsters our ability to lead future technology innovation.

Point No. 5: Exhibited and potential benefits of a particular biometric technology.
Its critical to consider the benefits of a particular biometric modality across many use cases. Here are a few out of thousands of success stories from U.S. law enforcement investigative applications:

- **Human trafficking:** In April 2019, a California law enforcement officer saw a social media post about a missing child from the National Center for Missing and Exploited Children. The officer used facial recognition which returned a list of online sex ads featuring the girl. According to a story in WIRED,[22] the girl had been "sold for weeks," and the officer's actions helped drive a process that "recovered the girl and removed her from trauma." Thousands of missing children have been found and rescued with the help of facial recognition technology tools available to law enforcement.
- **Counterterrorism:** On August 2019, New York Police Department detectives used facial recognition to help identify a man who sparked terror by leaving rice cookers in and around a subway station.[23] Detectives pulled still images from security footage and used facial recognition software, along with additional investigative work, to identify the suspect within an hour. NYPD officials were quoted saying, "To not use technology like this would be negligent" and "this is the most important type of case that we'd see out there: a possible terrorist attack in NYC."
- **Identifying a Suspected Killer Who Targeted LGBTQ+ Victims:** Three members of the LGBTQ+ community were shot and killed by a man at a local home in Detroit, Michigan, in 2019. Using facial recognition as a secondary tool, Detroit police officers were able to identify a man suspected of killing LGBTQ+ individuals. The suspect was charged with three counts of murder, in addition to other charges.[24]

[22] https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/.
[23] https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/.
[24] https://www.detroitnews.com/story/news/local/detroit-city/2019/06/06/detroit-man-charged-triple-lgbtq-killings/1373342001/

Point No. 6: Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case.

We recommend OSTP review the following policy templates extensively put forth by law enforcement organizations, U.S. Federal government agencies, thinks tanks, and private industry:

1) SIA Policy Principles for the Responsible and Effective Use of Facial Recognition Technology
2) U.S. Major Cities Chiefs Association Report on Facial Recognition Technology in Modern Policing – Recommendations and Considerations
3) International Association of Chiefs of Police Guiding Principles for Law Enforcement's Use of Facial Recognition Technology
4) U.S. Department of Justice, Bureau of Justice Assistance Face Recognition Policy Development Template For Use In Criminal Intelligence and Investigative Activities
5) U.K. British Security Industry Association Ethical and Legal Use Guide for Automated Facial Recognition.
6) World Economic Forum: A Framework for Responsible Limits on Facial Recognition Use Case – Flow Management
7) Center for Strategic and International Studies: Facial Recognition Technology – Responsible Use Principles and the Legislative Landscape

Conclusion

We commend OSTP for facilitating multi-stakeholder forums and allowing stakeholders to provide input on these important matters. If OSTP considers policy development in this area, we strongly encourage staff to review SIA's position in supporting the responsible and ethical use of biometric technologies. The U.S. must continue to exercise its leadership in the development and adoption of these emerging technologies to serve as an example to our allies, enable greater competition, and foster future innovation.

Respectfully Submitted,

[redacted]

Don Erickson
Chief Executive Officer
Security Industry Association
Silver Spring, MD
www.securityindustry.org

Staff Contact: Joe Hoellerer, [redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Sheila Dean

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI; MBX OSTP Biometric
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Wednesday, December 15, 2021 2:46:24 PM
Attachments: [redacted]

ATTN: Office Science and Technology Policy

BiometricRFI@ostp.eop.gov

CC: Suresh Venkatasubramanian c/o biometric@ostp.eop.gov

RE: RFI Response: Biometric Technologies

Document # 2021-21975

CIT# 86 FR 56300

Wednesday, December 15, 2021

Dear OSTP Administrators,

This is a letter of response for public input/RFI for generalized uses of US biometrics in government and in the marketplace.

The uses of Facial Recognition Technology should be banned, globally, for use in generalized visual surveillance in the US and more broadly, the world, to conform to a standard that regards basic human rights. The ability to narrow down on targeted individuals should be limited to those who already have a law enforcement biometric profile and inquiry to do a comparative analysis of offending acts captured. Therefore, there is no need for placing biometric markers on the general public in technical view of the Internet, CCTV or streaming video. The human rights violation track record is not limited to the example of the People's Republic of China, but for the sake of time, please refer to well documented repertoire of public dissents on the uses of FRT on persecuted populations, more submitted by other colleagues as expected.

Uses of Leidos and other competing biometric scanners at US airports should be eliminated based on the low proportionate comparative threat analysis of flyers who actually had genital explosives. Leidos, while I am sure will lobby to have their machines instilled by TSA, in US airports, should not lobby to maintain an invasive and demoralizing process instituted by the Obama Administration to inspect every US flyers genitals before entering the air transit area. While I do realize that TSA policy is not the specific burden of the OSTP offices, the demands for your influence to "improve" this process and policy will be expected. The best way to improve this TSA policy is to abolish it, eliminate the body scanners, all ensuing data and to apologize for the government's molestation of American flying publics.

Solicited recusal and recall of corporate contracts using PRC biometric surveillance to US cities & police departments to conform to US State Department policy and US embargoes in times of public conflict with The People's Republic Of China. US

government buyers of Hikvision and Dahua technologies should be required to immediately remove, uninstall all biometric enabled technologies and return them to your offices for information systems audits, based on national security conveyances conforming to China's PIPL law. I am sure they should not be exchanged for more biometric appliances, because in point 1, I requested that you ban all uses of generalized FRT and biometric surveillance be banned as subpar Human Rights standard.

Thank you for your audience on this important matter. I would like to add that my sense of 'what it's like' to be profiled has pains and sensations of humiliation associated with it. When my face is being examined by an unknowable surveillant I tend to feel somatic jaw and sinus pressure pain sensation under my eyes and adjacent to my nose. That's very specific, but this is the time when you document such things as evidence of public non-consent. I would add that previous administrations, Obama & Trump would collect input, much like this. While dissent and complaints from privacy advocates were collected, they performed the inverse of recommendations and did indeed double down, in contempt of solicited basic human rights advocacy. I urge you to not do that. Please present non-consent as non-consent in this input and not as means and need to escalate the uses of biometric technical work using public resources.

I thank you sincerely for the opportunity to generate thoughtful input on the subject of privacy, identity and biometrics at the OSTP. I look forward to reviewing your published findings.

Sincerely,

Sheila Dean
Privacy & Identity Rights Advocate
[redacted]

###

S.Dean

[redacted]

"Trust is the union of intelligence and integrity."- A Yogi

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Software & Information Industry Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Comments of the Software & Information Industry Association (SIIA) on the Request for Information on Public and Private Sector Uses of Biometric Technologies

Submitted to the Office of Science and Technology Policy

January 14, 2022

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the Request for Information on Public and Private Sector Uses of Biometric Technologies (the RFI) issued by the Office of Science and Technology Policy (OSTP).[1]

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. As the only association representing a diverse array of technology companies across the information landscape, SIIA believes in consumer privacy protections and responsible use of emerging technologies, including those that utilize biometric information.

We commend OSTP's efforts to develop a Bill of Rights for an Automated Society,[2] and appreciate the steps that OSTP has taken, through this RFI and a series of roundtables and listening sessions, to hear from consumers, businesses, academics, and the American public. Artificial intelligence (AI) is having a profound impact on all aspects of society and the impact will only continue. Leadership in developing policy to ensure that AI technologies are developed and used responsibly and in accordance with societal expectations is critical. We appreciate OSTP's role in ensuring that emerging technologies advance (and do not undermine) efforts to support diversity, equity, and inclusion (DEI) and individual privacy.

This submission is divided into four parts. First, we provide general recommendations on developing policy guidance on biometric information. These recommendations, applicable more generally to AI, are developed with a view towards policymaking, regulatory development, and statutory drafting rather than providing technical background on questions raised in the RFI. Second, we address the definitions of "biometric information" and "biometric technologies" as used in the RFI. Third, we highlight some of the many socially beneficial uses of biometric information that we have gleaned from our member companies. Fourth, we discuss the need for federal privacy legislation as a critical step on the path towards developing guidance on biometrics.

[1] Office of Science and Technology Policy, Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Fed. Reg. 86, 193, 56300-02 (Oct. 8, 2021).
[2] See Eric Lander and Alondra Nelson, American Need a Bill of Rights for an AI-Powered World, *Wired* (Oct. 8, 2021).

Guiding Principles for Developing Policy on Biometric Information and Biometric Technologies

One of the challenges inherent in developing governance rules for emerging technologies is that the technologies are constantly evolving. Business and consumers alike need predictability and as a society it is important that we develop practical guardrails to ensure responsible collection and use. We are encouraged by OSTP's focus on the *uses* of biometric information. We believe that focusing on uses is a prudent way to approach the development of guiding principles and regulatory and legislative recommendations.

Building on the approach taken in the RFI, we offer for consideration several guiding principles as OSTP continues its work on biometrics and on the broader Bill of Rights for an Automated Society. Overall, we believe the goal should be for a flexible policy and regulatory framework that will promote both innovation and responsible use—including uses of biometric information that benefit marginalized communities—and establish necessary guardrails that reflect societal norms and expectations.

First, we recommend that OSTP adopt a **technology-neutral approach** to developing policy. We believe the focus should be on transparency, information collection, and information use rather than the technological tools— and the underlying algorithms—that facilitate that collection and use. The distinction may be subtle, but it is an important one. Biometric information may be collected through numerous technologies and a one-size-fits-all approach will not be sufficiently flexible to provide a groundwork as advances occur. In most cases, a piece of software is not inherently good or bad—much like a hammer is neither good nor bad—and the key is to focus on how the software—or hammer—is used in practice.[3]

Second, we recommend that OSTP look to develop a **risk-based approach**. With respect to the field of biometrics, there is a range of risks to individual rights and other values depending on the type of information collected, how that information is stored and used, and what consumers' expectations are. For example, use of a fingerprint for the sole purpose of verifying identity to unlock a smartphone represents a low-risk situation; so, too, is using biometric information for facial authentication to assist educators in comparing a prior image of the individual to themselves to ensure the proper individual is taking an exam. Many companies use biometric tools strictly for identifying and authenticating consumers with strict use and storage restrictions on that information. These circumstances are likely to result in less risk that consumer data will be re-processed or shared for a secondary purpose. On the other hand, a government-run mass surveillance program using facial recognition that compares faces to images in a large database without restriction represents a high-risk situation; this can occur in a less transparent environment, without consent, where there is a potential for information asymmetry and infringement of constitutionally protected rights.

Responsibility, security, and accountability for biometric information should be commensurate with risk. One way to think about how to build out a risk-based approach is to identify the potential harms—such as discrimination and privacy violations—that could arise out of use, misuse, or abuse of biometric information and design contextualized collection and use restrictions to prevent those harms.

[3]

The harms should be measured based on injury-in-fact to the consumer and consumer expectations. We believe such restrictions or guardrails are critical, but they should be as narrowly tailored as possible to support innovation and positive use cases that benefit society.

Third, we recommend that OSTP support efforts currently underway in the U.S. government to develop **guidelines for responsible and ethical use** of AI technologies – which should include those technologies that collect and use biometric information. The work of the National Institute of Standards and Technology (NIST) in developing a risk management framework and establishing guidelines to address algorithmic bias is especially encouraging.[4] NIST has also led many efforts to shape the very first, overarching technical standards and testing for biometrics, starting decades prior to the widespread use of biometrics in routine consumer transactions that we see today. [5,] Alignment of key stakeholders, including industry groups, government stakeholders, private companies, and consumer advocacy groups to existing principles and standards like those adopted by NIST will lead to further harmonization of policy and technical foundations for how biometric information is collected and used.

Fourth, we recommend that OSTP **distinguish between public and private** collection and use of biometric information.

In the private context, we note that many companies have built robust frameworks for assessing how they collect and use biometric information. Our members are using biometrics in a wide variety of safe, effective, and efficient applications and contexts that present many benefits to stakeholders and the public, are done in a transparent manner and in accord with consumer expectations. Our members adhere to industry standards and many have established self-regulatory frameworks and principles[6] to ensure pre- and post- deployment impact assessments are conducted both prior to collection of biometric information and upon use of that information for various purposes.

In addition, some companies have proactively chosen to curb some forms of biometrics, including the use of facial recognition technologies, by placing moratoriums on public sector sales, or determining it would be best not to offer the technology at all, due to findings about inappropriate use in public settings.[7] We would encourage OSTP to foster these efforts and focus efforts towards policy that would promote these frameworks and provide appropriate checks on the highest risk situations.[8]

[4] See NIST, AI Risk Management Framework Concept Paper (Dec. 13, 2021); NIST, A Proposal for Managing and Identifying Bias in Artificial Intelligence (June 2021).
[5] See NIST, Biometrics.
[6] See, e.g., Adobe, Ethical Approach to AI; Google, AI Principles.
[7] See Taylor Kay Lively, Facial Recognition in the US: Privacy Concerns and Legal Developments, *Security Technology* (Dec. 2021).
[8] With respect to personal consumer devices (laptops, cell phones, etc.), that use biometric information for facial recognition, many private companies have built-in consumer engagement features that allow consumers to determine the specific uses of the technology, how the technology uses the information and what decisions and outputs are then gathered from that application. This empowers consumers about how their own information is and will be used.

The public sector or government experience with biometric information presents a different situation and we believe that OSTP can play an important role in guiding the government's collection and use of such information.

Governments can make use of biometric information to verify access to benefits, for national security, public safety, and law enforcement purposes, to counter fraud, to assist in providing public health services, and so on. Yet there is limited guidance on how the federal government *should* be collecting and using biometric information. Questions abound about what biometric information the government may appropriately collect, how that information is obtained, and how the information is used consistent with the rights guaranteed by the Constitution.[9] Concerns have been raised about whether the Fourth Amendment provides sufficient protection to individuals—and clarity to government actors—about what information may be collected and how it can be used.[10] Congress has introduced several bills that would direct the U.S. government on use (or non-use) of facial recognition technologies, [11] yet much can be accomplished through Executive Branch action alone. Many states and local governments are grappling with this issue.[12] It is important that the federal government confront these issues and provide a model for the nation.

Defining Biometric Information and Biometric Technologies

In this part of our submission, we address the definitions of key terms as they appear in the RFI and offer suggestions on how to amend these definitions to support OSTP's policy making efforts.

Biometrics is a category that has been subject to many definitions. As in other areas of advanced technology, including artificial intelligence more generally, it is important to get the definitions right in the first instance. With the Constitution's Bill of Rights as a comparison, we recommend that OSTP

---

[9] See, e.g., Matthew Doktor, Facial Recognition and the Fourth Amendment in the Wake of *Carpenter v. United States*, *Univ. of Cincinnati L. Rev.*, v.89, issue 2, at 552-74 (2021); Glenn Gerstell, "Failing to Keep Pace: The Cyber Threat and Its Implications for Our Privacy Laws," remarks to Georgetown Cybersecurity Law Institute (May 23, 2018) (reprinted at *Lawfare*).

[10] Ibid.

[11] See, e.g., H.R.3907 (117th Cong.), Facial Recognition and Biometric Technology Moratorium Act of 2021 (June 2021) (proposing to "prohibit federal government use of facial recognition technologies, provide a private right of action, and remove federal aid from agencies using the technology"); S.1265 (117th Cong.), The Fourth Amendment Is Not For Sale Act (Apr. 2021) (proposing to "prohibit law enforcement from purchasing personal data without a warrant and prevent law enforcement and intelligence agencies from buying illegitimately obtained data"); see also S.3035 (117th Cong.), Government Ownership and Oversight of Data in Artificial Intelligence Act of 2021 (Nov. 2021) (proposing interagency working group to develop guidance for the federal government and contractors around the development and use of AI).

[12] Several states have passed laws governing the public use of facial recognition technology, a subset of biometrics. Virginia and Pennsylvania require prior legislative approval before deploying facial recognition technologies, and states like Massachusetts, Utah, Kentucky, and Louisiana require law enforcement to submit written requests to the state agency that stores the database. Some states, including Massachusetts, Washington, and Maine, have placed additional administrative requirements like obtaining a warrant or court order or meeting a probable cause standard on government entities, while the state of Washington requires public entities and law enforcement to obtain public notice, hold community meetings, and publish an accountability report prior to using facial recognition. California, Mississippi, and Massachusetts have banned local government use of facial recognition. Other states have enacted narrow bans on the use of police body cameras that have facial recognition.

ensure that guiding principles are sufficiently flexible to survive technological advances. At the same time, to the extent OSTP's efforts will ground future regulatory action and lawmaking, there is a risk that definitions with too much flexibility could render enforcement and oversight impractical and have unforeseen, negative consequences.

As OSTP continues in its efforts to assess how biometric information is collected and used and the impacts that biometric technologies have, we recommend that OSTP focus its definitions in the following ways.

First, we recommend that OSTP limit the definition of "biometric information" to measurements of immutable physical characteristics. The definition used in the RFI – "any measurements or derived data of an individual's physical (e.g., DNA, fingerprints, face or retina scans) and behavioral (e.g., gestures, gait, voice) characteristics" – goes beyond this by including "derived data" in the definition.

We are aware of no existing legal precedent that defines biometric information to include information *derived from* physical characteristics. We are concerned that including "derived data" in the definition could lead to policy that does not sufficiently target the core issues around biometric information and, potentially, is used to ground formal guidance or rules that would be virtually impossible to comply with. This, in turn, will make it more challenging to ensure that public and private actors are meeting whatever obligations they may have to treat biometric information with special care and generate unpredictability among the public about what is and is not allowable.

We consider biometric information to refer to immutable physical characteristics – such as fingerprints, retinas, DNA, and facial features – that can be used for authentication or recognition, which OSTP defines to include both "verification" and "identification". This accords with definitions that are used by the Department of Homeland Security (DHS) and NIST. DHS, for example, describes biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition."[13] NIST offers several definitions, each referring to physical and/or behavioral characteristics, rather than derivations from these characteristics.[14] The Code of Federal Regulations and the U.S. Code use definitions that are generally aligned with these.[15]

---

[13] See Dept. of Homeland Security, Biometrics.
[14] See NIST Computer Security Resource Center, Biometrics.
[15] See 5 CFR 850.103 ("Biometrics means the technology that converts a unique characteristic of an individual into a digital form, which is then interpreted by a computer and compared with a digital exemplar copy of the characteristic stored in the computer. Among the unique characteristics of an individual that can be converted into a digital form are voice patterns, fingerprints, and the blood vessel patterns present on the retina of one or both eyes."); 21 CFR 1300.03 ("Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both distinctive to the individual and measurable."); 27 CFR 73.3 ("Biometrics. A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable."); 34 CFR 99.3 ("Biometric record as used in the definition of *personally identifiable information,* means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting."); see also 46 USC 70123 ("For the purposes of this section, the term 'biometric identification' means use of fingerprint and digital photography

Likewise, jurisdictions that have enacted laws on biometric information have not expanded it to include derivations of physical or behavioral characteristics. The Illinois Biometric Information Privacy Act (BIPA), one of the most extensive biometrics-related legislation enacted at the state level, "does not include information derived from items or procedures excluded under the definition of biometric identifiers."[16]

Second, we have concerns that including "behavioral characteristics" in the definition will present challenges for policy guidance on the collection and use of information based on immutable physical characteristics. Information based on gestures, gait, signature, keystrokes, and so on are often highly situation dependent and subject to environment-based stressors or emotional reactions like fatigue, happiness, and so on. While there may be value in developing guidelines for how public and private actors collect and use such information, we believe this should be done outside the context of biometrics. These types of information are less reliable for verification and identification purposes as they are not immutable. We would also exclude voice recordings, digital photographs, and speech-to-text services for similar reasons. Expanding the category of biometric information to include personal information or personally identifiable information is a form of mission creep that will have unknown consequences. In this regard, we recommend that approach taken by Illinois in BIPA, which excludes "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[17]

Third, we urge OSTP to focus the term "biometric technologies" to those uses of biometric information for recognition – identification and authentication – and not include those technologies that draw inferences based on biometric information. We believe that a focus on identification and authentication will provide a strong groundwork for setting policy around biometrics without introducing a significant amount of uncertainty introduced by extending policy to those technologies that may use biometric information to draw inferences.

Identification and authentication are related but distinct uses of biometric information. While subtle, the difference between the two is that biometric identification is a process that captures biometric information and then compares it to a large database of stored biometric information in order

---

images and facial and iris scan technology and any other technology considered applicable by the Department of Homeland Security.").

[16] 740 ILCS 14, sec. 10, Illinois Biometric Information Privacy Act of 2008. BIPA excludes photographs from its definitions of biometric information and identifiers, although we would urge clarity in exempting photographs as this issue has been subject to conflicting judicial interpretations in Illinois. See, e.g., Data Extracted from Photographs: Covered Under BIPA?, *The National Law Review* (Mar. 25, 2021). Similar language has been proposed in federal bills, including the National Biometric Information Privacy Act of 2020 (S. 4400, 116th Cong., Aug. 2020).

[17] 740 ILCS 14, sec. 10, Illinois Biometric Information Privacy Act of 2008. Nevertheless, we do not recommend BIPA as a model for liability. BIPA's statutory violation provisions have led to an avalanche of lawsuits for statutory damages without a showing of injury or harm or improper use of biometric information, including lawsuits based on routine employer practices, cybersecurity breaches, and other topics. See, e.g., Illinois Policy Institute, Illinois employers flooded with class-action lawsuits stemming from biometric privacy law (October 2017); Roy Maurer, SHRM, TopGolf Settles Biometric Privacy Lawsuit (July 19, 2021); BlankRome, Analyzing BIPAs Newest Class Action Trend: Targeting the Use of Voice-Powered Technologies (Aug. 30, 2021); Buchanan Ingersoll Rooney, Biometric Privacy Laws Create New Avenue for Data Breach Class Actions (Nov. 17, 2020).

to identify an individual. Law enforcement typically use this type of facial recognition. Contrary to this, biometric authentication involves verifying an individual's identity by comparing it to the same individual's previously provided biometric information. An iPhone uses this type of technology when Face ID is enabled; it is also used, in the education context, for example, to verify that the proper individual is taking an exam. We would urge OSTP to make this distinction clear in any policy guidance arising out of the RFI.

While biometrics may be used, as the RFI states, "for inference of cognitive and/or emotional states," we believe this category of uses should be treated differently. We are concerned that extending any guidance on biometrics to inferential uses could undermine efforts to set clear guardrails and ensure predictability for consumers and businesses alike. Inferential uses, or "soft biometrics," cannot be depended upon, with high accuracy, to identify a person or enable verification of identity.[18] Thus, technologies using biometric information in this manner present a very different risk profile for individual rights and values. We recommend further fact finding on this category of use cases with a focus on the particular risks (and harms) that such technologies may generate.

Positive Use Cases of Biometrics

We listened closely to the comments shared during OSTP's three listening sessions and while we respect the opinions shared, believe it important to highlight some of the beneficial uses of biometric tools. Indeed, despite attention around abuses of biometric information,[19] we believe it is important to recognize the ways in which biometric information can be used to generate socially beneficial uses – including uses that help to remove barriers and provide access to services for marginalized communities. In addition, technologies can use biometric information to create more secure means to authenticate users, contributing to cybersecurity; streamline processes in public health settings; facilitate increased and more efficient access to social benefits; improve public safety; and assist educators across the learning environment.

Tools that gather and use biometric information have the potential to address concerns around diversity, equity, and inclusion and provide services that improve the lives of people from marginalized communities. One example is the biometrics for individuals with disabilities, particularly in instances when these individuals are surfing the web and are required to authenticate their online presence. Features like voice recognition to authenticate web presence could support individuals with physical disabilities. Individuals with sight loss may benefit from a variety of biometric logins, such as fingerprint, face, or iris authentication, which can simplify authentication, for example, when asked to authenticate sight-based CAPTCHA images. Those with dyslexia may also stand to benefit from biometrics, as opposed to strictly memory-based authentication log-in information, like passwords.[20]

---

[18] See, e.g., Abdelgader Abdelwhab and Serestina Viriri, A Survey on Soft Biometrics for Human Identification, in *Machine Learning and Biometrics*, Jucheng Yang et al., eds. (London: IntechOpen, 2018); U. Park and A. K. Jain, Face Matching and Retrieval Using Soft Biometrics, *IEEE Transactions on Information Forensics and Security*, v.5, issue 3, at 406-15 (Sept. 2010); A. Dantcheva, What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics, 11 *IEEE Transactions on Information Forensics and Security*, v.11, issue 3, at 441-67 (Mar. 2016).

[19] See Office of the Privacy Commissioner of Canada, Clearview AI ordered to comply with recommendations to stop collecting, sharing images (Dec. 14, 2021).

[20] See Abby Young-Powell, Ensuring Biometrics Works for Everyone, *Raconteur* (Feb. 2021).

Research suggests that the algorithms and underlying data fueling some biometric technologies like facial recognition technologies need to be further optimized to support all individuals. To date, bias in facial recognition technologies has led to instances of unethical, biased, and/or discriminatory uses for marginalized communities. But biometrics has the potential, once it is fully optimized for use by diverse populations, to decrease inequity and support people of color and people in marginalized communities, particularly if it helps these very communities who are most at-risk for security hacks, credit fraud, and other negative repercussions to accessing their social benefits.

And the facts are compelling that the future of biometrics is bright. Research by the Center for Strategic and International Studies demonstrates that some of the most accurate facial recognition technologies have an error rate of 0.08% in April 2020, down from an error rate of 4.1% in 2014, according to tests conducted by NIST.[21]

We want to highlight a few of the many case studies from our members that reflect socially beneficial uses of biometric information.

- Google built a machine learning system using open-sourced models to expand the database of forms, expressions and physical characteristics of sign language. This gives individuals with disabilities and their caregivers a better understanding of the types of expressions of sign language that exist and creates a continuously updated database of examples.[22]
- TurnitIn, through ExamSoft, provides access to authentication software that education and professional credentialing institutions can use to validate the identity of the test taker. This provides institutions with a means to preserve the integrity of the test-taking experience while also providing easier access to exams and learning environments.
- Adobe has launched a suite of biometric features, including a forward-thinking facial verification (through a selfie) and government ID authentication, as part of its Document Cloud, which can be used to authenticate remote documents and workstreams. The Government ID Authentication tool compares the selfie to the Government ID to authenticate the user, which provides time and cost savings and creates seamless regulatory compliance for banks, private companies and governments alike. Nearly 8 billion signature transactions have taken place in a one-year period, and nearly half of all Fortune 100 companies are using AdobeSign. This is yet another mechanism that will eliminate the cumbersome nature of paper signatures, create efficiencies for consumers and businesses, and can lead to significant gains for marginalized communities, especially communities with disabilities.

Federal Privacy Legislation is a Necessary First Step

Lastly, we encourage OSTP to play a proactive role in supporting efforts underway to advance a general federal privacy bill. Many of the concerns that the public has raised around the uses of biometric technologies dovetail with concerns around privacy. Yet, the United States has no general application privacy law. We strongly endorse the bicameral efforts underway to advance a comprehensive federal privacy law that will provide strong and meaningful consumer protections (such as individual rights to

[21] See William Crumpler, "How Accurate are Facial Recognition Systems – and Why Does It Matter?," Center for Strategic & Intl. Studies (Apr. 2020).
[22] Kemal El Moujahid, Machine learning to make sign language more accessible, Google - The Keyword (Dec. 2021).

notice, access, control, correction, deletion, and portability), permit socially beneficial uses of consumer data - particularly publicly available information - and promote innovation and competition in the American economy. The legislation should both protect consumers from harm caused by the unreasonable collection and misuse of their personal data and prevent and remedy data practices that stifle innovation and stagnate data flows and routine business processes.

We are at a unique moment politically when, after years of debate, there appears to be bipartisan support for comprehensive federal privacy legislation. SIIA is working actively with the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce to support their efforts to craft a comprehensive federal privacy law that reflects these core elements.

Although some federal privacy legislation proposals address the collection and use of biometric information and others do not, establishing a nationwide, harmonized framework for personal information would, at a minimum, establish a foundation on which to develop targeted guidance on how biometric information is collected and used.[23] A federal privacy law could help to close the gaps that exist across other civil rights and sectoral laws to ensure that companies use data equitably, fairly, and in non-discriminatory manners. It could also establish high-level guardrails regarding the collection and use of biometric information, harmonizing the needs of consumers with those of businesses to foster a healthier digital ecosystem.

We encourage OSTP—and the Biden-Harris Administration—to lend its voice to advance these efforts.

Contact Information

Please direct any inquiries regarding this submission to Paul Lekas, SIIA Senior Vice President for Global Public Policy ([redacted]) and Divya Sridhar, SIIA Senior Director for Data Protection ([redacted]).

[23] At the state level, California and Colorado's consumer privacy laws–the California Privacy Rights Act or CPRA, effective January 2023 and the Colorado Privacy Act, effective July 2023–include language that allows consumers further control over facial recognition data. California provides consumers with rights to access, opt-out of the sale of and delete their facial recognition data; Colorado will require businesses to obtain consent prior to processing consumers' facial recognition data. Another area of debate is whether private entities should be allowed to use facial recognition in public accommodations. To date, only Portland, Oregon and Baltimore have enacted regulations that limit commercial uses of facial recognition technologies.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Stephanie Dinkins and the Future Histories Studio at Stony Brook University

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Thoughts around and contributions to an A.I. Bill of Rights as requested by The White House Office of Science and Technology (OSTP)proposal to develop a "bill of rights" to protect American citizens against the potentially harmful consequences of A.I. or, more specifically, biometric data (facial recognition, voice analysis, heart rate tracking, etc.). November 2021.

The original United States Bill of Rights spells out Americans' rights in relation to their country. It purports to guarantee civil rights and liberties to the individual and sets rules for due process of law. Given the codified function of white supremacy and its many tendrils, not all people benefit equally from the bill of rights.

This effort is spearheaded by Stephanie Dinkins, Professor & Director of the Future Histories Studio (FHS) part of the DISCO Network, Department of Art, Stony Brook University, with input from FHS researchers, members of AI.Assembly, related artists, and Stony Brook University Campus Community members.

Prologue

People who live with the threat and discomfort of knowing the rights and liberties set out by the Bill of Rights are still not equally applied or protected.

“...a rights framework offers a wrongheaded approach to mediating the relationship between technology (created by human beings) and vulnerable populations within our society (also human beings). The history of international human rights establishes the global rights infrastructure as an aspirational rhetoric with significance in law, custom, and politics, but hardly as a safeguard against the continuing violence that is meted out against vulnerable and/or historically victimized populations within nation-states or against the violence (economic, political, and social) facing vulnerable and historically -victimized peoples and lands around the world. As written above, the question separates "A.I. systems" from their human creators and the human economic interests that are inevitably tied to their existence and perpetuation. As we have yet to find a "bill of rights" either within the USA or around the world, the Universal Declaration of Human Rights (UDHR) or International Conventions of Civil, Political Rights, (ICCPR) and International Convention of Economic, Social and Cultural Rights (ICESCR), that adequately protects human beings from other human beings, why is the rights framework being deployed in the obfuscatory way in relation to A.I.? I would suggest that the lessons of the human rights and civil rights history around the world offer useful insights into mediating the shifting relationships between human beings and technology and that these would be useful sites of allegory, theory, and empirical analysis.”

– **Abena Ampofoa Asare**, Associate Professor, Modern African Affairs & History, Department of Africana Studies, Stony Brook University

In response to The White House Office of Science and Technology Policy (OSTP) call to engage the American public in the process of developing a Bill of Rights for an Automated Society, we offer the following requirements and rights for consideration.

Honored personhood and the Right to Opt-Out

As individuals and related communities, we require the same rights concerning biometric data as they would their person, personal information, and data created via personal digital tools.

As individuals and related communities, we have the right to opt-out of providing biometric data in both public and private spaces.

Transparency/ Non-Obfuscation / The Right to be Forgotteb

In lieu of the right to opt-out, individuals and related communities must be told ***any*** time biometric data is recorded or collected by private, public, and governmental entities and organizations.

- Standard of interaction- Individuals must be notified when data of any type related to their being is collected at each point of collection. This is especially true of more passive biometric technologies such as voice and iris recognition.
- Reasons for data collection must be explained and publicly announced in clear, generally understandable language. Notification must be available in be central repository and at the site of collection.
- The method of data collection, storage location and duration of resulting data, and instructions for redress must also be shared.

As individuals and related communities, we have the right to be forgotten.

- When data is collected, it can not be kept in perpetuity. Unless proactively consented to data provided consensually, must be destroyed within a reasonable timespan. One week could be defined as "reasonable."
- The burden to forget is the responsibility of the organizations, governments or persons collecting the data. This right to be forgotten must be written into the original code/system and enacted automatically on a preordained schedule.

As individuals and related communities, we require that government use of biometric data, and A.I. more generally, will not be obfuscated or laundered through the use of non-governmental organizations.

> For example, if the United States employs Amazon to develop broad surveillance, they are not absolved because it was a contractor the did the work. Likewise, if the police purchase data sets from a phone company, the police should be bound by all rules as if they were obtaining the information themselves.

As individuals and related communities, we require that algorithms and datasets used to support biometric systems must be transparent. All A.I.. used on any public must utilize datasets that reflect the public (with respect to demographics, such as gender and race) on which it will be used to train the A.I..

As individuals and related communities, we require that consent to provide biometric data not be coerced as a condition of usage of a product, service or technology.

Privacy & Redress

As individuals and related communities, we require that biometric data created by personal technologies such as wearable sensors, mobile phones, home-based care and communications technologies and bodily implants may not be accessed, used without consent, or triangulated with data from other sources.

As individuals and related communities, we require that biometric data collected about them will not be used in research without consent. When consented to profit-sharing, arrangements must be made.

Accountability

As individuals and related communities, we require that companies and government agencies that deploy A.I. be held accountable for any bias or discrimination which results from the use of the A.I., as if it were done by a human being.

An example, if a bank uses A.I. to determine lending policy and the policy ends up discriminating based on race, the bank would be as liable if the lending decisions were made by people. Or if a manufacturer of self-driving cars deploys systems that do not recognize Black pedestrians at the same rate as white pedestrians, they will be liable for civil rights violations in addition to any other penalties that arise from this design flaw.

As individuals and related communities, we require those who are not US citizens, mbe granted the same rights with regard to A.I. as US citizens.

> For example, if US airline companies rely on A.I. (either their own or governmental) to deny passage of a Nigerian citizen, that person should be able to challenge the denial and have access to review the algorithm and/or dataset that led to their denial.

As individuals and related communities, we require all uses of A.I. by the military should be subject to review by citizens with no ties to the military.

Checks and balances & Trust

As individuals and related communities, we require both human and automated checks and balances of computational surveillance and decision-making systems. Checks and balances must be enacted regularly and keep pace with the speed of technological advancement.

As individuals and related communities, we require that the public (or public representatives) have the right to review and analyze the algorithms underlying biometric technologies and algorithmic systems more generally. Datasets used to train any machine learning system must also be made available for review, augmentation and edit.

As individuals and related communities, we require that an organization akin to the FDA or CDC, be created to guide the development of biometric systems and provide centralized oversight.

Individuals, communities, and autonomous entities require public and private entities to collect biometric data to use blockchain or other traceable technologies to track and engender trust in the process of data collection and disposal.

As individuals and related communities, we require that the government is not permitted to deploy A.I. for purposes that would either be illegal or impossible for unaided human analysis.

As individuals and related communities, we require A.I. systems be regularly audited for historical and contemporary biases. Proof of audit and transparency of the process must be publicly available.

Profiling through Data

As individuals and related communities, we require that their biometric data never be aggregated into a composite portrait created from data collected from multiple collection sites.

As individuals and related communities, we have the right to fact-check and edit the story aggregate data tells about them.

As individuals and related communities, we have the right to legal and monetary recourse for personal information inferred and divulged from aggregated data without consent.

As individuals and related communities, we require that government institutions and agencies not be able to obtain, store or cross-reference personal information which they would not otherwise be able to keep, access or cross-reference.

> For example, people coming to a lecture at a university can reasonably assume anonymity and expect not to be surveilled by the police. With facial recognition technology crossed with access to driver's license photos, the technology exists for the government to compile lists of most attendees.

Monetization and Profit Sharing

As individuals and related communities, we require that biometric data collected about them not be monetized or otherwise used for profit in public, private or governmental spheres.

As individuals and related communities, we require that biometric data collected about us will not be used in research without consent. When consented to, profit-sharing arrangements must be made.

Care

As individuals and related communities, we require biometric systems to resist the hyper-rational, binary lens of efficiency and profit in favor of technological ecologies, to care for individual entities and communities while encouraging complexity, plurality, and generosity in our data-centric ecosystems.

As individuals and related communities, we require our A.I. ecosystems, inclusive of biometrics, to be infused with a diversity of nuanced values, beliefs and representations toward the equitable distribution of resources and mutually beneficial systems of care.

As individuals and related communities, we require that biometric systems be developed with the understanding that the boundaries between sovereign consciousness, nature, power, and social reality are shifting. Our A.I. ecosystems must be developed, planned, and deployed with these ideas at the forefront.

As individuals and related communities, we require our A.I. ecosystems, inclusive of biometrics, be developed, carefully administered, and deployed to support and care for global society instead of being ruled by fear and the pursuit of profit.

EPILOGUE

Mutations, adaptations, genetic drift, hybridity, and other mechanisms allow life to explore the landscape of possibilities. Life folds back on itself in an evolution of evolution: the first cells replicated by fission; but eventually developed sexual reproduction, which vastly accelerated evolutions' landscape exploration. Human physical labor similarly folds nature back on itself, as Marx pointed out. Expressive (i.e. semiotic; informational) value is the means by which culture can pass on adaptations without waiting for genetics: language, writing, and technology. And in its most recent recursive turn, machine intelligence folds human culture back on itself. The idea that it too contains a fundamental creativity--that A.I. will explore its own space of possibilities--means that it is all the more urgent to map out evolutionary trajectories for generative justice and ensure they are deeply embedded in these new algorithmic regimes from the start.

See Evolving Systems for Generative Justice: Decolonial Approaches to the Cosmolocal.

Available from: https://www.researchgate.net/publication/356664131_Evolving_Systems_for_Generative_Justice_Decolonial_Approaches_to_the_Cosmolocal [accessed Dec 24, 2021]

–Ron Eglash, Professor, Stamps School of Art & Design/ Professor, School of Information, and Audrey Bennett, Professor, Stamps School of Art & Design, University of Michigan

995

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

TechNet

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

January 15, 2022

Office of Science and Technology Policy
1650 Pennsylvania Ave NW
Washington, D.C. 20502

Re: TechNet comment regarding notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

To Whom It May Concern:

TechNet appreciates the opportunity to submit a written comment in response to the Office of Science and Technology Policy's (OSTP) notice requesting information regarding public and private sector use of biometric technologies. TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over four million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

The growth of the data-driven economy continues to fuel economic and social opportunity not just in the technology industry, but throughout every sector of the global economy. As we've seen in recent months, the need to secure critical U.S. infrastructure is urgent, and according to Accenture, a TechNet member, 68 percent of business leaders feel that their organization's cybersecurity is at risk. In order to meet the cybersecurity needs of today's increasingly interconnected digital world, policymakers and industry leaders must focus their efforts on promoting the adoption and use of voluntary, adaptable, risk management-based approaches to meet this changing environment and effectively manage cybersecurity risk.

Artificial intelligence (AI) is transformational technology that revolutionizes the way we live and work and helps us solve the greatest challenges of our

time. AI can enhance productivity, democratize and expand access to important services, and advance product innovation. AI is being used to defend our country against cyberattacks, detect and deter fraud, deliver high-quality health care solutions, assist persons with disabilities, help individuals make better financial decisions, and train workers, among other applications. AI development should be embraced because its potential for improving our lives is almost limitless. However, AI innovation must be developed and implemented responsibly.

Biometric Technology in Practice

The COVID-19 pandemic has accelerated the digitalization of businesses, consumers, and the government, and laid bare the connectivity barriers faced by many who have had to transition crucial aspects of life online. Biometric technology, through the use of AI, is used in a variety of ways every day to protect against identity fraud, improve user experience, and increase access to services.

One example use case that helps improve the lives of individuals is digital identity verification. This technology quickly and accurately uses unique traits such as their face, thumbprint, etc to ensure that the user is who they say they are when conducting business virtually. This not only helps to minimize fraud, but it provides an improved user experience based on efficiency and security.

In addition to protecting against identity fraud, using biometric technology to verify individuals increases access to services. For example, in the financial services sector biometric based digital identity verification has been used to increase access to services for individuals with thin credit files, as is common for young people, immigrants, and historically marginalized groups. Fintech companies are at the forefront of implementing biometric technology, which has helped their services provide underserved communities with non-traditional credit history opportunities to overcome the barriers of accessing credit.

Promoting Innovation while Protecting Consumers

TechNet strongly supports the government's efforts to better understand and utilize this technology. TechNet supports regulatory sandboxes as a means to explore feasibility in a safe and collaborative framework, which have proven very successful with prior emergence of developing technologies. The potential for regulatory sandboxes, if established in a transparent and

good-faith manner, is revolutionary. For example, the Consumer Financial Protection Bureau created a regulatory sandbox for businesses operating in the financial technology space. This sandbox was instrumental for both government and private sector to better understand risks, provide consumers with safe services, and predict what type of regulation would best serve this unique market without hindering innovation.

This intersection of government regulation and private sector innovation should be championed as a way to meet consumer demand while ensuring a process is in place to identify and address potential risks. Industry standards for identity verification are a key way to independently validate the performance of a technology, and we are already seeing international efforts to create uniformity within this sector.

Human Supervision

Human oversight of biometric technology is a key assurance to providing consumers with secure products and services. However, the core function of biometric technology would be vastly undercut, and potentially deemed inefficient, if humans were to be involved in every instance of biometric authentication. Humans are also susceptible to making errors, which ultimately can be minimized through the use of AI. There should be clear and reasonable standards for how human oversight interacts with biometric technology to ensure regulations are not disproportionately burdensome and hindering the groundbreaking positive benefits ushered in by the use of AI ushers in. For example, human oversight should be intended to focus on specific high-risk instances where the evidence supporting the need for human oversight is strong.

TechNet appreciates this opportunity to submit comments to this RFI. As policies and regulations form to meet the evolving technological landscape, it is important that new laws prioritize the positive benefits that AI can offer the world. TechNet stands ready to partner with you in implementing this and other emerging technologies.

Response: If you have any questions regarding this comment letter, please contact Carl Holshouser, Senior Vice President, at [redacted].

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

The Alliance for Media Arts and Culture, MIT Open Documentary Lab and Co-Creation Studio, and Immerse

THE ALLIANCE FOR MEDIA ARTS + CULTURE | MIT OPEN DOCUMENTARY LAB | CO CREATION STUDIO | IMMERSE
CREATIVE DISCUSSION OF EMERGING NONFICTION STORYTELLING

ARTISTS STATEMENT for a Proposed US AI Bill of Rights

We are artists, scientists, journalists, media-makers and human rights activists who actively engage with Artificial Intelligence including biometric technologies. We explore their creative potential and we critique these technologies. We engage with US and global public audiences through our work. We serve as an intermediary between the scientists and technologists and the public, helping members of the public better understand the implications of AI technologies and how they relate to broader efforts to capture and interpret reality.

In our work, we address security considerations, known vulnerabilities, issues of data privacy, bias, and transparency. We argue for consent and the ability to opt-out of AI-enabled manipulations and/or influences. We create public awareness about the harms these unregulated AI systems bring to specific groups including Black and Brown communities, people with disabilities, LGBTQ+, Indigenous communities, youth, and to the general public. We believe in the necessity of human responsibility.

We strongly urge and call for an expansive array of voices to be included as an integral part of the development and co-authorship of an AI Bill of Rights. We further urge that people from these communities have a leadership role in the agencies and structures created to make decisions and protect the public with regard to AI development. This means not only technologists, corporations, lawyers, and politicians, but also human rights activists, artists, journalists, bearers of culture and intergenerational communities from around the globe.

With this statement, organized by The Alliance for Media Arts + Culture, MIT Open Documentary Lab and Co-Creation Studio, and *Immerse*, we, the undersigned, also include an incomplete but important list of artistic, scientific and journalistic projects and studies from our communities that directly address these issues (in the Appendix below). We urge the process of developing an AI Bill of Rights be actively animated and informed by this work, and our community.

SIGNED,

Wendy Levy, *The Alliance for Media Arts + Culture*
Sarah Wolozin, *MIT Open Documentary Lab, Immerse*
Katerina Cizek, *Co-Creation Studio at MIT Open Documentary Lab, Immerse*

and

Agatha S. Park, *Media Artist*
Ambar Reyes, *MIT ODL Researcher*
Amelia Winger-Bearskin*, Banks Preeminence Chair and Assistant Professor of AI and the Arts at the University of Florida, Digital Worlds Institute*
Andrea Kim, *Fulbright Research Fellow*
Andrew Demirjian, *Associate Professor/ Hunter College*
Andy Beach, *CTO, Media & Entertainment, Microsoft*
Ankur Vora
Anna Van der Wee, *Director, producer Wild Heart Productions*
Anya Rous, *VP of Production, Multitude Films*
Artemis Willis, *Research Fellow*
Asma Nobari Khoshmehr
Assia Boundaoui, *Independent Investigative Journalist and Artist*
B. Ruby Rich, *Film Quarterly*
Barry Threw, *Executive Director - Gray Area Foundation for the Arts*
Beckie Stocchetti, *Executive Director, Hawai'i International Film Festival*
Brenda Webb, *Executive Director*
Brittany Delany, *Artist*
C Dalrymple*, PBS Utah*
Carol Dysinger, *Prof. at NYU Grad Film*
Caroline A. Jones, *Professor, art historian, critic, curator*
Christopher Buttimer, *Post-doctoral Associate, MIT*
Cindy Bishop, *Director of technology, creative*
Cindy Poremba
Claire Jervert, *Artist*
Claudia Romano, *Producer, MIT Open Documentary Lab*
Cristina Kotz Cornejo, *Media Maker*
Daniel Toner, *WGBH*
Debra Swack, *Fulbright and Education Specialist SUNY Research Foundation/New Media Artist*
Dejan Grba, *Artist, researcher, and scholar*
Deniz Tortum, *Filmmaker*
Derek Curry & Jennifer Gradecki, *Assistant Professors, Northeastern University*
Diboer Lei
Dr. Ellen Pearlman, *Research Fellow MIT Open Doc Lab, Director ThoughtWorks Arts*
Dr. Heidi Boisvert, *CEO & Founder, futurePerfect lab & Assistant Professor of AI & the Arts*
Ella Fasciano, *Tufts University Documentary Film Student*

Emma Raynes, *Director of Programs, Magnum Foundation*
Eric Grunwald, *Interim Director, English Language Studies, MIT*
Faisal Anwar, *Hybrid Artist, Curator, Karachi Biennial 22. Founder Innovation lab, culturelab.art*
Gabriel Vieira-Posada, *MIT Fellow*
Gisele Gordon, *Media Artist*
Gordon Quinn, *Founder and Artistic Director*
Grayson Earle, *Lecturer, New School*
Halsey Burgund, *independent artist; Fellow at MIT Open Documentary Lab*
Henry Ajder, *deepfake and synthetic media expert*
Howard Phillips, *Professor*
Ilana Schoenfeld, *Learning Designer—MIT The Education Arcade (TEA)*
Ileana Doble Hernandez, *Ileana Doble H Studio*
Jack Walsh, *Filmmaker*
Jared Willard, *Machine Learning Researcher*
Jasmine Heyward, *University of Westminster*
Jason Livingston, *Media artist*
Jeff Soyk, *MIT Open Doc Lab Fellow Alum*
Jessica Clark, *Executive Director, Dot Connector Studio*
Joanna Martine Wright, *Fellow MIT Open Documentary Lab, Honorary Senior Research Fellow, Bangor University, UK*
José Magalhães, *Quadratura da Net*
Josefina Buschmann
Joseph Steele, *PhD Candidate (CU Boulder) and Affiliate (Vrije Universiteit Ams. NL)*
julia scher, *professor emeritus KHM*
Julie Hermelin, *Managing Partner; Gutsy Media*
June Cross, *Filmmaker*
Karo Durojaiye, *Artist/Designer*
Karim Ben Khelifa, *Nonfiction storyteller*
Kelly Wagman, *PhD student, University of Chicago*
Kieran, *Sundance Institute*
L. Mattock Scariot, *Director*
Lara Baladi, *MIT faculty*
Laurids sonne, *Graduate student,University of Colorado, Boulder*
Lee Boot, *Director, Imaging Research Center, UMBC*
Liam Corcoran, *Entrepreneur*
Logan Coale, *Software Engineer*
Lynette Wallworth, *VR Wallworth*

M. Kamal Sinclair, *Co-Leader, Guild of Future Architects*
marc böhlen, *Professor, University at Buffalo*
Mark Shepard, *Associate Professor of Architecture and Media Study / University at Buffalo*
Mashinka Firunts Hakopian
Mathew Rappaport, *Associate Professor, Columbia College Chicago*
Mathieu Pradat, *Author and Director, MIT Open Documentary Lab Fellow*
Maya Hawke, *Editor*
Melinda Weekes-Laidlow, *CEO*
Michaela Holland, *XR Consultant*
Michaela Pnacek, *York University, Toronto*
Michèle Stephenson, *Director / Producer / Rada Studio*
Monda Webb, *Founder, Little Known Stories Production Company*
Natalie Bullock Brown*, Documentary Accountability Working Group*
Ngardy Conteh George, *Filmmaker*
Nim Shapira, *Artist*
Oghenekaro, *Artist*
Paco de Onís, *Executive Director, Skylight*
Patricia Finneran, *Story Matters Media*
Patricia Roberts (Antelles), *Designer*
Penelope Jagessar Chaffer, *Research Fellow*
Peter Grosz, *Roustabout Media*
Peter Keough, *Writer/Boston Globe*
Rashin Fahandej, *Assistant Professor of Emerging and Interactive Media*
Rebecca Evanhoe, *Conversation Designer, Author, Visiting Assistant Professor*
Rekha Malhotra
Riley Wong, *Machine Learning Engineer*
Rina Kim
Roger Leisner, *Founder/Owner of Radio Free Maine*
Rowena Chodkowski, *Concordia University*
Ryat Yezbick, *Guild of Future Architects*
Samantha King
Samuel Kauffmann, *Professor Emeritus, Boston University, College of Communication*
Sandra Rodriguez, *Creative Director*
Sarah MacDonald
Sean Flynn, *Program Director & Co-Founder, Points North Institute*
Shamsher Virk, *Executive Director, ZERO1: The Art & Technology Network*
Shel Evergreen, *Science Writer*
shirin anlen, *Creative Technologist and Artist/ Research Fellow at MIT Open Documentary Lab*

Siobhan O'Flynn, *Assistant Professor, Director, Canadian Studies Program*
Sito Fossy Biosa, *Bandung Institute of Technology & VISUAREKAN*
Sky Sitney, *Co-Director, Double Exposure Investigative Film Festival*
Sohin Hwang, *Artist*
Stephanie Lepp, *Producer*
Susan Margolin, *St Marks Productions*
Ting Zhang, *Project Lead, Local News Lab, Brown Institute*
Thomasin B Durgin, *Artist*
Toma Peiu, *Instructor, PhD Candidate - Emergent Technologies and Media Arts Practices, U of Colorado Boulder*
Tosca Terán, *Interdisciplinary artist*
Tracy Heather Strain, *The Film Posse*
Virginia Keller, *Roustabout Media*
William Uricchio, *Professor, MIT*
Yucef Merhi, *Affiliate Researcher, Fellow / MIT Open Documentary Lab*
Ziv Schneider, *Artist and Creative Technologist*

Appendix: Relevant Artistic Work and Research Studies

Title of Work	Link to Work
Always There, Sternberg Press 2002	https://www.sternberg-press.com/product/always-there/
Facial Poetry	http://www.cibernetic.com/art/project/facial-poetry/index.html
Seek	http://culturelab.art/portfolio/seek/
Riot	http://karenpalmer.uk/portfolio/riot/
Android Portrait Project	http://www.clairejervert.com/shop
False Positive	http://www.false-positive.net/
Neurospeculative Afro Feminism	http://www.hyphen-labs.com/nsaf.html

Algorithmic Bias Training, or, Lectures for Intelligent Machines	http://www.mashinkafirunts.com/algorithmic-bias-training-or-lectures-for-intelligent-machines/
Brittle Opacity: Ambiguities of the Creative AI	https://2021.xcoax.org/data/pdf/xCoAx2021-Grba.pdf
Animal Patterning Project	https://becoming.ink/animal-patterning-project / https://thewrong.tv/doomscroll
Poesía Facial	https://cibernetic.com/art/project/poesia-facial/index.html
Poet on Earth	https://cibernetic.com/art/project/poet-on-earth/index.html
Just Joking: Deepfakes, Satire, and the Politics of Synthetic Media	https://cocreationstudio.mit.edu/just-joking/
Cloud Mapping Project	https://contemporaryarts.mit.edu/pub/cloudmappingproject/release/3 https://vimeo.com/520782433
PINK PASTEL EXTENDED	https://drive.google.com/drive/folders/1WiKqq6iwgHV-QQmsT3BB83MzV9uzeZ5m?usp=sharing
fairlyintelligent.tech	https://fairlyintelligent.tech/
Limbic Lab	https://futureperfectlab.com/portfolio/limbic-lab/ or https://www.ted.com/talks/heidi_boisvert_how_i_m_using_biological_data_to_tell_better_stories_and_spark_social_change?language=en
Stealing Ur Feelings	https://github.com/noahlevenson/stealing-ur-feelings
Deep Dream: The Art of Neural Networks	https://grayarea.org/event/deepdream-the-art-of-neural-networks/
Why don't the cops fight each other?	https://graysonearle.com/cops/
Antecedent Technology	https://immerse.news/antecedent-technology-b3a89956299d

Before Everyone Was Talking About Decentralization, Decentralization Was Talking to Everyone	https://immerse.news/decentralized-storytelling-d8450490b3ee
Marrow	https://immerse.news/when-machines-look-for-order-in-chaos-198fb222b60a
Chomsky vs Chomsky	https://mediaspace.nfb.ca/epk/chomsky-vs-chomsky/
In Event of Moon Disaster	https://moondisaster.org
Pre-Crime Calculator	https://precrime-calculator.azurewebsites.net/
The Open Biometrics Project	https://realtechsupport.org/projects/biometrics.html
Conversations with Things: UX Design for Chat and Voice	https://rosenfeldmedia.com/books/conversations-with-things/
VIVX	https://skylight.is/vivx/
Omnia per Omnia	https://sougwen.com/project/omniaperomnia
Orbis tertius	https://toscateran.ca/portfolio/orbis-tertius/
Transgenic Morphosis	https://toscateran.ca/portfolio/transgenic-morphosis/
And Laid Him On The Green	https://vimeo.com/354131681/9d3525bde5
Sick Speech	https://vimeo.com/449806018/83620a3486
Alexa is no joke, video, 02:16	https://vimeo.com/665395433
Future Rites	https://vimeo.com/manage/videos/624502503
Sisyphus 2.0 (short film, 7 min, dir. Luiza Parvu, Toma Peiu)	https://vimeo.com/rootfilmsro/sisyphus20
Collective Wisdom: Co-Creating within communities, across disciplines and with AI	https://wip.mitpress.mit.edu/collectivewisdom
Tech as Art: Supporting Artists Who Use Technology as a Creative Medium	https://www.arts.gov/about/publications/tech-art-supporting-artists-who-use-technology-creative-medium
Boogaloo Bias	https://www.boogaloo-bias.art/

Deep Reckonings	https://www.deepreckonings.com/
POV: Points of View	https://www.grximmersive.com/pov
[radical] signs of life	https://www.heidiboisvert.com/work/radical-signs-of-life-2/ or https://vimeo.com/70526438
XTH Sense - Biocreative Instrument	https://www.heidiboisvert.com/work/xth-sense / or https://vimeo.com/164177468
The Emotions after Charles Darwin	https://www.leoalmanac.org/vol19-no4-without-sin/
Deep Else: A Critical Framework for AI Art	https://www.mdpi.com/2673-6470/2/1/1/htm
Charbagh	https://www.surrey.ca/arts-culture/surrey-art-gallery/exhibitions/garden-machine
Symbiosis/\Dysbiosis	https://www.symbiosis-dysbiosis.com
AIBO: An Emotionally Intelligent Artificial Intelligence Brainwave Opera - Can An AI Be Facist?	https://www.youtube.com/watch?v=1vjvcexiMkk
ONES and ZEROES – The Bias Murders by Monda Raquel Webb ©2018	https://www.youtube.com/watch?v=2NGlbSqCEB8
Symphony of Noise VR	https://www.youtube.com/watch?v=QjImklTvAxk
Noor: A Brain Opera - Is There A Place In Human Consciousness Where Surveillance Cannot Go?	https://www.youtube.com/watch?v=URv_iz631Y0
Making a New Reality	makinganewreality.org
The Poppy Jasper International Film Festival Educational Programs	pjiff.org
SKYWORLD / CLOUDWORLD	https://www.studioamelia.com/work/skyworld

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

The International Brotherhood of Teamsters

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

INTERNATIONAL BROTHERHOOD OF TEAMSTERS

JAMES P. HOFFA
General President

25 Louisiana Avenue, NW
Washington, DC 20001

KEN HALL
General Secretary-Treasurer

202.624.6800
www.teamster.org

January 15, 2022

Submitted via BiometricRFI@ostp.eop.gov < *RFI Response: Biometric Technologies* >

Re: The Office of Science and Technology Policy (OSTP) requests input from interested parties on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.

The IBT and Its Interest

The International Brotherhood of Teamsters ("IBT" or "Teamsters") submits this Comment in response to OSTP's request for input. The IBT is a labor organization founded in 1903. It represents more than 1.4 million hardworking men and women in various industries across the United States, Canada, and Puerto Rico. For over a century, the IBT and its members have worked to guarantee workers a living wage and the benefits they deserve, both through negotiating strong collective bargaining agreements and by supporting employment legislation that lifts all workers. The IBT has a strong interest in ensuring that A Bill of Rights for an Automated Society is equipped to address the difficult challenges presented by new emerging technologies.

Technological developments in the form of automation, artificial intelligence, and robotization are having a profound impact on our country's economy, labor market, and workforce. The undeniable impact can in significant part be attributed to incongruous laws and regulations pertaining to employee surveillance and employee health and safety, and the reduction in the labor workforce for certain industries. While there is no denying that with modern day technology, innovation and opportunity are endless, these new tools have also led to serious problems that must be addressed to prevent and decrease the disproportionate effect on marginalized workers, individuals, families, and communities. The following sections discuss priority issue(s) for the labor community concerning the use of artificial intelligence and similar computer-based programs. Furthermore, each section seeks to clearly identify and define an issue resulting from the misuse of technology, briefly discuss the ramifications of the issue, and discuss any practical solutions for combating the harmful impact each issue has on Labor. For this comment, technology shall generally mean any automated or algorithmic; system, database, or program, driven by artificial intelligence.

Unlawful Surveillance of Workers

Federal laws and regulations, as currently enforced, fails to account for the ability of employers to utilize technology as a means of unlawfully surveilling workers and union activity. Section 7 of the National Labor Relations Act (NLRA) grants employees the rights to engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection; and

Section 8 forbids employers "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7."[1] When assessing these protections from a surveillance viewpoint, the National Labor Relations Board[2] (NLRB) takes two approaches: the literal surveillance of workers, such as the photographing or videotaping of employees engaged in protected activities; and the promulgation, maintenance, or enforcement of work rules that create an impression of surveillance.[3] Of course, the capabilities of modern technology have left employers with little need to engage in the literal surveillance of workers, as most employers can make use of technology to implement otherwise justifiable work rules for the real purpose of illegal surveillance. Charges brought against employers under a theory of creating an impression of surveillance also face significant hurdles before finding success as legal precedent provides inapt consideration to an employer rule's connection to employers' right to maintain discipline and productivity in their workplace; and whether the potential adverse impact on worker rights is outweighed by justifications associated with the rule.[4]

Under the current legal framework, surveillance of employees is widespread as employers are allowed to search employees' personal property, including their vehicles, whenever on company premises; and monitor employee activity on any company issued communication devices, computer systems, or network.[5] Tools such as navigation software, item scanners, wristbands, thermal cameras, security cameras and recorded footage are utilized by employers to surveil workforces for illegal purposes and stifle employee concerted activity. For example, reports have well documented Amazon's use of heat maps and data such as team-member sentiment and a diversity index to figure out which stores have a higher probability of unionizing.[6] The absence of effective surveillance standards has systematically confined unions and workers in a defensive posture, constantly confronting employee disciplinary sanctions in court or arbitration; in which employers seek to purge workers that organize or speak out in the pursuit of better working conditions.[7] To ensure new and emerging data-driven technology is used in a trustworthy manner,

[1] *See* 29 U.S.C. § 158(a).
[2] Congress in 1935 created the National Labor Relations Board (NLRB). Decisions of the Board can be appealed to the appropriate United States Court of Appeals. Under § 3(d) of the NLRA (29 U.S.C.A. § 153), the General Counsel has final authority to investigate unfair labor practice charges, issue formal complaints of unfair labor practices, and prosecute such complaints before the Board.
[3] *See* Quicken Loans, Inc. v. Natl. Lab. Rel. Bd., 830 F.3d 542 (D.C. Cir. 2016). Protection includes a prohibition on employers spying on employees engaged in union activities or creating the impression of spying on employees engaged in union activities.
[4] *See* The Boeing Company, 365 NLRB No. 154 (Dec. 14, 2017).
[5] *See* Caesars Entertainment, 368 NLRB 143 (2019); Verizon Wireless and Commun. Workers of Am., 369 NLRB No. 108 (N.L.R.B. June 24, 2020); Employees are left with no recourse to address employer policies that disguise surveillance motives connected to rights generally reserved in management rights clause or employer handbook.
[6] *See* Leon, H. (2020, April 23). *Whole Foods secretly upgrades tech to target and squash unionizing efforts*. Observer. Retrieved December 29, 2021, from https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/; Bose, N. (2020, August 31). *Amazon's surveillance can boost output and possibly limits unions -study*. Reuters. Retrieved December 29, 2021, from https://www.reuters.com/article/amazoncom-workers-surveillance-idUSL4N2FW0CK.
[7] Building trust among workers, especially those workers without union representation, is an important prerequisite for any workplace collective action. There is a likely possibility that modern employer surveillance and the fear of retaliation by an employer will deter workers from activities that build trust and lead to collective action. *See* Charlotte Garden, Labor Organizing in the Age of Surveillance, 63 *St. Louis U. L.J.* 55 (2018), p 66. https://digitalcommons.law.seattleu.edu/faculty/814. Workers at companies like Amazon have reported that their employer has used modern workplace surveillance technology to deter workplace organizing and retaliate against

a Bill of Rights for an Automated Society should include labor protections for workers that find employer workplace rules that depend on data produced by modern technology, illegal if its' use can be reasonably construed to prohibit or diminish the exercise of labor rights by employees.

Robotization of the Human Workforce

Federal Laws and regulations, as currently enforced, fail to account for employers expanding utilization of technology as a means of setting abnormally dangerous worker productivity quotas.[8] The NLRA does grant employees the right to bargain over mandatory subjects such as health and safety;[9] and provides protection for workers that refuse to work over abnormally dangerous safety condition.[10] However the ability to bargain requires the element of "concertedness," where two or more people are acting together, or one person is acting on the behalf of others.[11] Additionally, legal precedent suggests that the source of the employees' concern must relate to a condition over which the employer has control.[12] Also, for protection for refusing to work in abnormally dangerous conditions, the harm must be objectively demonstrable.[13]

Similarly, The Occupational Safety and Health Act (OSH Act) was enacted to assure safe and healthful working conditions for working men and women. To that end, the Occupational Safety and Health Administration (OSHA) has promulgated guidance in effort to protect employees from retaliation when they refuse to work in imminently dangerous situations that present "a risk of death or serious physical harm."[14] Recent efforts at the state level have also

employees who engage in it. *See* Daniel Hanley & Sally Hubbard, Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power, Open Market Institutes (2020), pp 12-13. https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf; Olivia Solon & April Glaser, Fired, interrogated, disciplined: Amazon warehouse organizers allege year of retaliation, NBC News (2021). https://www.nbcnews.com/business/business-news/fired-interrogated-disciplined-amazon-warehouse-organizers-allege-year-retaliation-n1262367

[8] State level efforts have been made. *See* CA LEGIS 197 (2021).

[9] *See* NLRB v. Am. Nat'l Can Co., 924 F.2d 518, 524 (4th Cir. 1991) (citing Holyoke Water Power Co., 778 F.2d 49, 51 (1st Cir. 1985), cert. denied, 477 U.S. 905, 91 L. Ed. 2d 565, 106 S. Ct. 3274 (1986)).

[10] Section 502 deals with the rights of employees who refuse to perform work in unsafe conditions where a contractual no-strike provision would make such activity unprotected. *See Whirlpool Corp. v. Marshall*, 445 U.S. 1, 17-18 fn. 29 (1980); *Tamara Foods*, 692 F.2d 1171, 1183 (8th Cir. 1982), cert. denied 103 S.Ct. 2089 (1983); *Banyard v. NLRB*, 505 F.2d 342, 348 (D.C. Cir. 1974). There are significant limitations for employees seeking to address health and safety concerns under the Railway Labor Act (45 U.S.C. § 152) as well. For example, *See* Taylor v. Am. Airlines, 943 F. Supp. 1164 (W.D. Mo. 1996); Air Line Pilots Ass'n Intern. v. N.W. Airlines, Inc., 570 F.2d 257 (8th Cir. 1978); Union Pacific Railroad Company v. Brotherhood of Maintenance of Way Employes Division of International Brotherhood of Teamsters, 2020 WL 7643217 (D. Neb. 2020), subsequent determination, 2021 WL 65508 (D. Neb. 2021); Int'l Bhd. of Teamsters v. UPS Co., 447 F.3d 491 (6th Cir. 2006).

[11] *See generally* id. Section 502 covers stoppages by a single employee without. . . "concerted" activity.

[12] *See* National Transportation Service, 240 NLRB 565 (1979), whether an employer has control over the conditions of employment of its employees in sufficient manner so as to enable it to bargain effectively with a union. Under Section 502 . . . immaterial as to whether it is within the employer's control.

[13] *See* Tns, Inc., 309 NLRB 1348 (N.L.R.B. 1992). Under Section 7 employees' do not need for the belief to be objectively reasonable.

[14] *See* OSH Act of 1970, Pub. L. 91-596, § 2, 84 Stat. 1590, 1590. Employee may refuse an assignment that involves "a risk of death or serious physical harm" if all of the following conditions apply: (1) the employee "asked the employer to eliminate the danger, and the employer failed to do so"; (2) the employee "refused to work in 'good faith'" (a genuine belief that "an imminent danger exists"); (3) " [a] reasonable person would agree that there is real

sought to fill the regulatory void. A new California law, AB 701, attempts to regulate productivity quotas for warehouse distribution centers. AB 701[15] requires employers to provide a written description of productivity quotas to employees subject to potential adverse employment action that could result from failure to meet the quota; prohibits employers from requiring that workers meet a quota that prevents them from taking meal or rest breaks or complying with other health and safety laws; and prohibits adverse action against an employee for failure to meet a quota that has not been disclosed or does not allow a worker to comply with meal and rest break or occupational health and safety laws.[16]

For Unionized workers, productivity quotas are often established in contract negotiations between management and labor unions. Bargaining obligations under the NLRA often lead the two parties to negotiate a reasonable level of production for employees in various roles and with different levels of experience. Unionizing can be a remedy for workers in the face of unfair discipline because of a dangerous productivity quotas enforced by automated surveillance technology, and ensure employees have a say in the degree to which employers can use automated surveillance technology to make disciplinary decisions.[17] Nevertheless, the reality for most nonunionized workers is much different. Most are forced to work under quotas that are unilaterally set by management and are subject to unimpeded termination for failing to make quotas.[18] With automated workplace surveillance becoming the new normal,[19] and without any say in how employers use surveillance technology, workers have already seen these technologies used as the sole means for dispensing workplace discipline and termination.[20]

danger of death or serious injury"; and (4) " [t]here isn't enough time, due to the urgency of the hazard, to get it corrected through regular enforcement channels, such as requesting an OSHA inspection."

[15] *See* CA LEGIS 197 (2021), 2021 Cal. Legis. Serv. Ch. 197 (A.B. 701). Applies to employers of 100 or more employees at a single warehouse distribution center or 1,000 or more employees at one or more warehouse distribution centers in the state.

[16] *See* id. Allows a current or former to request one written description of each quota to which the employee is subject and a copy of personal work speed data. An employer must abide by this request and there shall be a rebuttable presumption of unlawful retaliation if an employer in any manner discriminates, retaliates, or takes any adverse action against any employee requesting quota information or making a complaint related to a quota; Authorizes an action for injunctive relief to obtain compliance.

[17] *See* International Brotherhood of Teamsters, ABF Freight National Master Agreement (2019), p 106, https://teamster.org/wp-content/uploads/2019/12/ABF18MASTERFINAL.pdf; International Brotherhood of Teamsters, UPS Freight National Master Agreement (2018), pp 48-49, https://teamster.org/wp-content/uploads/2018/12/upsf18freightnationalmaster.pdf; International Brotherhood of Teamsters, National Master United Parcel Service Agreement (2018), p 20, https://teamster.org/wp-content/uploads/2018/12/ups18nationalmaster.pdf; International Brotherhood of Teamsters, National Master Freight Agreement (2019), pp 11-12, https://teamster.org/wp-content/uploads/2020/05/mas_nmfa-yrcw_2019-2024.final_04_10_2019.pdf.

[18] *See* Jeanne Mejeur, M. L.-K. (n.d.). *At-will employment - overview*. Retrieved December 30, 2021, from https://www.ncsl.org/research/labor-and-employment/at-will-employment-overview.aspx.

[19] *See* Kathryn Zickuhr, *Workplace surveillance is becoming the new normal for U.S. workers,* Washington Center for Equitable Growth (2021). https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/

[20] *See* Ugo Okere et. al., *Secure Jobs, Safe Workplaces, and Stable Communities: Ending At-Will Employment in Illinois*, National Employment Law Project (2021), p 11. https://www.nelp.org/publication/secure-jobs-safe-workplaces-stable-communities-ending-will-employment-illinois/. Based on a January 2021 survey administered to a representative sample of Illinois workers (n=806), 34 percent of respondents reported electronic monitoring used for workplace discipline and termination at their jobs.

Employers operating in the gig economy, franchise model, or those who misclassify employees as independent contractors,[21] utilize theses employment models to unilaterally control working conditions including productivity quota rates.[22] The problem is particularly grim for employees that work under structures like the Amazon – Delivery Service Provider (DSP) model. Under the DSP model, Amazon uses a system of independent delivery contractors instead of directly employing drivers. Amazon uses their agreements with the delivery contractors to reserve the right to control driver working conditions, closely monitoring their performance, and dispense termination when it deems necessary.[23] Thus, the legal requirement that the source of the employees' concern must relate to a condition over which the employer has control, in order for the concerted activity to be protected, makes it very difficult for employees to take remedial action against a delivery contractor who retains little control by means of contract obligations to a larger economic firm such as Amazon. Protection under the NLRA for workers that refuse to work in abnormally dangerous conditions are also ill-equipped to alleviate employees from these harms. Because of the high bar required for establishing the employees' perception of possible harm, must be objectively demonstrable,[24] it is arguably understandable why poorly researched and documented harm resulting from dangerously high worker productivity quotas are not provided broader protection in the courts.

A lack of regulatory tools has prevented OSHA from addressing worker injuries for years.[25] OSHA has been under funded, understaffed, congressionally stifled on ergonomics and ill equipped to deter employers' behaviors or stop the underreporting of occupational injuries and illnesses. OSHA conducted an average of 38,092 inspections per year under the Obama Administration and an average of 32,610 worksite inspections per year during the first three years of the Trump Administration, a noticeable drop.[26] Furthermore, a 2020 report revealed that as of January 2020, OSHA had "the lowest number of on-board inspectors in the last 45 years, it was estimated that it would take the agency approximately 165 years to inspect each workplace under its jurisdiction just once."[27] Additionally, the financial penalties OSHA has issued for violations

[21] *See* Velox Express, Inc., 2019 L.R.R.M. (BNA) 324327, 2018-19 NLRB Dec. (CCH) P 16580, 2019 WL 4134112 (N.L.R.B. 2019).
[22] *See* 29 U.S.C. § 152(3); Allied Chemical and Alkali Workers of America, Local Union No. 1 v. Pittsburgh Plate Glass Co., Chemical Division, 404 U.S. 157, 92 S. Ct. 383, 30 L. Ed. 2d 341, 1 Employee Benefits Cas. (BNA) 1019, 78 L.R.R.M. (BNA) 2974, 66 Lab. Cas. (CCH) ¶ 12254 (1971). The NLRA expressly excludes "independent contractors" from the definition of "employee."
[23] *See* Bloomberg. (n.d.). Bloomberg.com. Retrieved December 31, 2021, from https://www.bloomberg.com/news/features/2021-10-07/amazon-delivery-partners-claim-treated-like-robots-by-algorithms. The program was loosely modeled on FedEx Corp.'s network of independent contractors.
[24] . *See infra* footnote 9. The harm must also be good faith belief.
[25] *See* Adam M. Finkel & Jason W. Sullivan, *A Cost-Benefit Interpretation of the "Substantially Similar" Hurdle in the Congressional Review Act: Can OSHA Ever Utter the E-Word (Ergonomics) Again?*, 63 ADMIN. L. REV. 707, 120 (2011).
[26] *See* Deborah Berkowitz, Nat'l EMP. L. Project, *Worker Safety In Crisis: The Cost Of A Weakened OSHA* 4 (2020), https://s27147.pcdn.co/wpcontent/uploads/Worker-Safety-Crisis-Cost-Weakened-OSHA.pdf [https://perma.cc/7TAU-BMH6].
[27] *See* id.

have historically been insignificant.[28] The maximum penalty for a serious OSHA violation[29] is $13,653, while the maximum for a willful and repeat violation is $136,532.[30] Nevertheless, when OSHA does find a serious violation, it rarely imposes the maximum penalty. In 2019 the average penalty for a serious violation was only $3,717.147.[31] For example, OSHA inspectors issued a mere 67 citations at Amazon warehouses between 2015 and 2019, resulting in fines of $262,132, which represents roughly 0.0087% of Amazon's profits in 2018 alone. [32]

California's Assembly Bill 701 (AB 701),[33] seeks to address the relationship between productivity quotas and high risks of injury or illness by increasing transparency about the use of productivity quotas and placing some restrictions on what behavior can be considered time off task. However, AB 701 fails to mandate a standard[34] that considers, "the relationship between quotas and risk factors for musculoskeletal injuries and disorders. . ."[35] Therefore, while AB 701 may succeed in increasing transparency around the use of productivity quotas, it does little to address the dangerous conditions workers face as emerging technology generates increasingly demanding data-driven productivity quotas for employers.[36]

The NLRA, OSHA, and state level efforts have not adequately dealt with employers' use of modern-day technology, nor have there been successful efforts to properly balance the right of employers to operate their business efficiently with the right of employees to work in an environment absent of intimidation, coercion, and dangerous conditions. The current dichotomy

[28] *See* AM. Fed'n of Lab. & Cong. Of Indus. Orgs., *Death On The Job: The Toll Of Neglect* 18 (2016) [hereinafter 2016 Death On The Job], https://aflcio.org/sites/default/files/2020-10/DOTJ2020_Final_100620_nb.pdf [https://perma.cc/E3QC-G9P9] ("A combination of too few OSHA inspectors and low penalties makes the threat of an OSHA inspection hollow for too many employers.").
[29] A violation is "serious" when "it poses a substantial probability of death or serious physical harm to workers."
[30] *See* OSHA Penalties (2021), Occupational Safety & Health Admin., https://www.osha.gov/penalties [https://perma.cc/5WZA-TLBU]. This is up from a maximum penalty of $13,494 in 2020. See AM. Fed'n of Lab. & Cong. Of Indus. Orgs., Death On The Job: The Toll Of Neglect 19 (2020) [hereinafter 2020 Death On The Job].
[31] *See* id.
[32] *See also* Athena Coal*., Packaging Pain: Workplace Injuries In Amazon's Empire* 6–7 (2019), https://s27147.pcdn.co/wpcontent/uploads/NELP-Report-Amazon-Packaging-Pain.pdf [https://perma.cc/Y836-53TC] ("Amazon sets the standard for delivery and fulfillment in the eCommerce industry and it also undeniably sets the standards for employment practices and working conditions in the industry.").
[33] *See* Press Release, Assemblywoman Lorena Gonzalez, *Assemblywoman Gonzalez Introduces Bill to Protect Warehouse Workers from Hazardous Working Conditions* (Feb. 16, 2021), https://a80.asmdc.org/press-releases/20210216- assemblywoman-gonzalez-introduces-bill-protect-warehouse-workers-hazardous [https://perma.cc/D5MM-VH52]; Assemb. B. 701, 2020–2021 Reg. Sess. (Cal. 2021).
[34] For example, standards could include limit on how many boxes workers are required to fill per hour, or more general safety protocols, like a requirement that workers be given stretch and water breaks every hour.
[35] *See* Assemb. B. 701 § 6726(a); Fifty-one Democrats and 1 Republican voted in favor of the bill, while 1 Democrat and 18 Republicans voted against; Vote on AB 701 – AB 701 Lorena Gonzalez Assembly Third Reading, OPENSTATES, https://openstates.org/vote/7a543fec-6c00-4e5d-b1d8-bd90500cfa6e/ [https://perma.cc/UH6U-X5H2] (last visited June 6, 2021); see also AB-701 Warehouse Distribution Centers, CAL. LEGIS. INFO., https://leginfo.legislature.ca.gov/faces/billVotesClient.xhtml?bill_id=202120220AB70 1 [https://perma.cc/6JH9-KFKX] (last visited June 6, 2021).
[36] *See* Lecher, C. (2019, April 25). *How Amazon automatically tracks and fires warehouse workers for 'productivity'*. The Verge. Retrieved December 30, 2021, from https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations ("Amazon's system tracks the rates of each individual associate's productivity," "and automatically generates any warnings or terminations regarding quality or productivity without input from supervisors." (Amazon says supervisors are able to override the process.)).

many workers face is that of being terminated for failure to keep up with a quota or risk serious injury.[37] For an example, widely reported are the alarming number of injuries suffered by workers in Amazon warehouses, due to workers fear of falling behind targets and being dismissed for poor productivity.[38] Furthermore, Amazon has fired hundreds of employees at a single facility for failing to meet productivity quotas. A spokesperson for the company acknowledged the company once terminated roughly 300 full-time associates for "inefficiency" over a 13-month period.[39] Research has shown that disciplining workers may result in a short-term productivity boost, just as larger employee bonuses accumulated over time result in a higher productivity increase.[40] Therefore, regulating the unabated use of workplace surveillance in cases of worker discipline may be necessary to limit the scaling of automated worker discipline by employers. Left unchecked, employers could use expansive automated disciplinary practices to chase quick productivity increases, which would come at the expense of long-term productivity increases due to employee bonuses and other rewards, in addition to increasing the risk for on-the-job injuries.

The unilateral control over the implementation and utilization of worker productivity quotas, algorithms, and other worker systems driven by artificially intelligent or computer-generated programs must be addressed. Thus, a Bill of Rights for an Automated Society presents a unique and necessary opportunity that should include provision that make the implementation and utilization of worker productivity quotas, algorithms, and systems driven by such technology an indisputable matter of health and safety under Section 7 of the NLRA. Furthermore, the bill should consider a private right of action under OSHA in order to enable workers to file suit when an employer violates an OSHA standard, and the agency was unable to inspect or issue a citation.[41] Additionally, a Bill should expand reporting and disclosure requirements to relevant federal agencies concerning the use of this technology and employee injury data. The correlation between the two should be properly researched, analyzed, and understood.[42] Such data would enable agencies at the federal and state level to understand what kind of intervention or enforcement is and will be required to reduce worker injuries and other harm in the future. [43]

[37] *See* Greene, J. (2021, December 14). *Amazon's employee surveillance fuels unionization efforts: 'it's not prison, it's work'*. The Washington Post. Retrieved December 30, 2021, from https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions/.

[38] *See Amazon's disposable workers: High injury and turnover rates at fulfillment centers in California*. National Employment Law Project. (2021, July 8). Retrieved December 30, 2021, from https://www.nelp.org/publication/amazons-disposable-workers-high-injury-turnover-rates-fulfillment-centers-california/#:~:text=Workers%20at%20Amazon%20warehouses%20have%20an%20alarmingly%20high,as%20high%20as%20the%20average%20for%20other%20warehouses.

[39] See Lecher, C. (2019, April 25). *How Amazon automatically tracks and fires warehouse workers for 'productivity'*.

[40] *See* Wim A Van der Stede, *Sticks and carrots: the effectiveness of penalties versus bonuses*, London School of Economics (2021). https://blogs.lse.ac.uk/businessreview/2021/09/02/sticks-and-carrots-the-effectiveness-of-penalties-versus-bonuses/

[41] See generally CTR. *For Progressive Reform, OSHA'S Next 50 Years: Legislating A Private Right of Action To Empower Workers* 5 (2020), https://cpr-assets.s3.amazonaws.com/documents/OSHA-Private-Right-of-ActionFINAL.pdf [https://perma.cc/EN3X-WB5T]; Nat'l Council For Occupational Safety & Health, National Agenda For Worker Safety And Health 4 (2021), https://nationalcosh.org/sites/default/files/2021-02%20National%20Agenda%20for%20Worker%20Safety%20and%20Health.pdf [https://perma.cc/M22W-VES8]. At present, only OSHA has the right to pursue a claim under the OSH Act, rather than individuals.

[42] In theory, such efforts would contribute significantly to the promulgation of adequate rules and increased enforcement under section 502 of NLRA and other Federal or State regulations that may utilized this information.

[43] *See* id.

Reduction in Blue Collar industry Workers

Federal nor state regulations are equipped to address the alarming decline of blue-collar workers in America because of the job loss to artificially intelligent robots. Furthermore, modern technology has created new reality for white-collar workers as well.[44] While several federal and state laws govern employment mattes, the ubiquity of at-will employment makes this problem a difficult matter to resolve. [45] Presently, the most useful tool is perhaps the NLRA, which guarantees employees right to engage in protected concerted activity, including the right to bargain over mandatory subjects such as employee layoffs. Nevertheless, it is far from being a solution, and there are currently no other laws or regulations that directly address the matter. Though the current dichotomy workers face of being terminated for failure to meet a quota or risking serious injury has certainly contributed to the loss of workers and increased use of robots, there is clearly something gloomier in the works. Whether it be McDonald's introducing self-serve kiosks and firing hourly workers to cut costs, or top-tier investment banks relying on software instead of traders, millions of American workers are facing the potential for job loss.[46] Researchers at MIT and Boston University have projected robots could replace approximately 2 million more workers in the manufacturing industry alone by 2025.[47]

This trend has the potential to adversely impact all classes of workers and it's beyond time to seriously think about how AI should be managed. Over 5 years ago the White House warned between 2.2 and 3.1 million car, bus, and truck driving jobs in the US would be eliminated by the advent of self-driving vehicles, and forecasted an 83 percent chance workers earning less than $20 per hour would lose their jobs to robots, 31 percent of those who make up to $40 an hour would face a chance of being replaced, and those paid more than $40 an hour faced an approximate 4 percent of losing their jobs to automation.[48] In theory, automation and artificial intelligence should be used to assist workers by eliminating or reducing dangerous or complex tasks so they can take on more assignments, making companies more productive and raising wages. Historically, the answer to technological change has been a reinvestment in education and retraining for

[44] *See Augmentative AI and the future of work.* Stanford HAI. (n.d.). Retrieved December 30, 2021, from https://hai.stanford.edu/news/augmentative-ai-and-future-work.

[45] Jeanne Mejeur, M. L.-K. (n.d.). *At-will employment - overview*. Retrieved December 30, 2021, from https://www.ncsl.org/research/labor-and-employment/at-will-employment-overview.aspx. Employment relationships are presumed to be "at-will" in all U.S. states except Montana. The U.S. is one of a handful of countries where employment is predominantly at-will. At-will means that an employer can terminate an employee at any time for any reason, except an illegal one, or for no reason without incurring legal liability. Likewise, an employee is free to leave a job at any time for any or no reason with no adverse legal consequences. At-will also means that an employer can change the terms of the employment relationship with no notice and no consequences.

[46] *See* Kelly, J. (2021, December 10). *Artificial Intelligence has caused a 50% to 70% decrease in wages-creating income inequality and threatening millions of Jobs.* Forbes. Retrieved December 30, 2021, from https://www.forbes.com/sites/jackkelly/2021/06/18/artificial-intelligence-has-caused--50-to-70-decrease-in-wages-creating-income-inequality-and-threatening-millions-of-jobs/?sh=2e6e52681009; Semuels, A. (2020, August 6). Machines and Ai are taking over jobs lost to coronavirus. Time. Retrieved December 30, 2021, from https://time.com/5876604/machines-jobs-coronavirus/.

[47] *See* id.

[48] *See* Shahien Nasiripour, *White House Predicts Robots May Take Over Many Jobs That Pay $20 Per Hour.* The Huffington Post (2016), http://www.huffingtonpost.com/entry/white-house-robot-workers_us_56cdd89ce4b0928f5a6de955.

employees.[49] Many companies deploying automation and AI say the technology allows them to create new jobs for which employees can be retrained, but the number of new jobs is often minuscule compared with the number of jobs lost.[50]

A Bill of Rights for an Automated Society should include provisions for the establishment and supervision of programs for the instruction and training of employers and employees concerning the harms around the use of artificial intelligence in the workplace.[51] Furthermore, consideration should be given to what limited roles, responsibilities, and task should be assigned to artificially intelligent robots. The primary goal of these objectives would be to preserve the human workforce, minimize the risk of injury to workers, and prevent a decline in the quality of life for working class citizens long enough for the country to learn and adjust to modern day technology. The country has a vital interest in making sure workers have the required skill set necessary to find work in today's tech driven world, and furthermore ensure technology controlling or working with sensitive information, hazardous material, or armaments are not devoid of reasonable control. The results of such guidelines would promote stability and safety amongst the labor workforce and society at large.

Conclusion

For the foregoing reasons, A Bill of Rights for an Automated Society should focus on resolving the harmful impact modern day technology is having on marginalized workers, individuals, families, and communities. Thus, the IBT supports The White House Office of Science and Technology efforts in furtherance of said goals.

Respectfully submitted,

/s/
Bradley T. Raymond
General Counsel

cc: Gary Witlen, Esq., International Brotherhood of Teamsters
Willie Burden Jr., Esq., International Brotherhood of Teamsters

[49] *See* Yahoo! (n.d.). *Millions of Americans have lost jobs in the pandemic-and robots and ai are replacing them faster than ever.* Yahoo! News. Retrieved December 30, 2021, from https://news.yahoo.com/millions-americans-lost-jobs-pandemic-102250355.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAABd4s0ZfNesASxSj__jH7CdHWiCp7_UWxb94pZuDyPqomXyXk_G27b4YRNxG8nCkzNGObYZxp6gQ6hBy6VPMKmjTXSB95qSL58Mq1Fu_hMsT0il5FbCdkDLH1tYg06yIjdeiX7DsGjCV91lp9YdS_ZL83FYIspOLU9aMSu7TvHmf.

[50] *See generally* id.

[51] *See generally* for example training and employee education, 29 U.S.C. § 670.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

The Leadership Conference on Civil and Human Rights

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036

[redacted]020

www.civilrights.org

The Leadership Conference

January 14, 2022

Suresh Venkatasubramanian
Office of Science and Technology Policy
Executive Office of the President
The White House
Washington, DC 20500

Re: RFI Response-Biometric Technologies, Document Number: 2021-21975

Dear Dr. Venkatasubramanian,

On behalf of The Leadership Conference on Civil and Human Rights, a coalition charged by its diverse membership of more than 230 national organizations to promote and protect the civil and human rights of all persons in the United States, we write in response to the Request for Information published in the Federal Register on October 8, 2021, titled *Request for Information on Public and Private Sector Uses of Biometric Technologies*. Specifically, these comments will focus on the need to ensure that biometric technologies protect civil rights, prevent unlawful discrimination, and advance equal opportunity.

Technological progress should promote equity and justice as it enhances safety, economic opportunity, and convenience for everyone. In 2014, a coalition of civil rights and media justice groups released "Civil Rights Principles for the Era of Big Data,"[i] calling on the U.S. government and businesses to respect and promote equal opportunity and equal justice in the development and use of data-driven technologies. These principles, along with the Obama White House's subsequent reports on big data, highlighted the need for rules of the road for the private and public institutions whose decisions can ultimately protect or deny civil and human rights.

Today, while the terminology has shifted from "big data" to "AI" and "biometrics," the issues remain the same and the threats technology can pose to civil rights have only grown. Recognizing this increased urgency, in 2020, The Leadership Conference, along with a number of advocacy and civil rights organizations, released updated Civil Rights Principles.[ii]. Of relevance to this inquiry, the Civil Rights Principles propose a set of civil rights protections, including:

Ending High-Tech Profiling. Surveillance technologies are empowering governments and companies to collect and analyze vast amounts of information about people. Too often, these tools are deployed without proper safeguards, or are themselves biased. In some cases, surveillance technologies should simply never be deployed. In other cases, clear limitations and robust auditing mechanisms are needed to ensure that these tools are used in a

responsible and equitable way. Law should hold both the government and private actors accountable for abuses.

Ensuring Justice in Automated Decisions. Statistical technologies, including machine learning, are informing important decisions in areas such as employment, health, education, lending, housing, immigration, and the criminal legal system. Decision-making technologies too often replicate and amplify patterns of discrimination in society. These tools must be judged not only by their design but also, even primarily, by their impacts – especially on communities that have been historically marginalized. Transparency and oversight are imperative to ensuring that these systems promote just and equitable outcomes, and in many cases the best outcome is to not use automated tools in high-stakes decisions at all.

Preserving Constitutional Principles. Enforcement of constitutional principles such as equal protection and due process must keep pace with government use of technology. Search warrant requirements and other limitations on surveillance and policing are critical to protecting fundamental civil rights and civil liberties, especially for communities who have been historically marginalized and subject to disproportionate government surveillance. Moreover, governments should not compel companies to build technologies that undermine basic rights, including freedom of expression, privacy and freedom of association.

Ensuring that Technology Serves People Historically Subject to Discrimination Technology should not merely avoid harm, but actively make people's lives better. Governments, companies, and individuals who design and deploy technology should strive to mitigate societal inequities. This includes improving access to the internet and addressing biases in data and decision-making. Technologies should be deployed in close consultation with the most affected communities, especially those who have historically suffered the harms of discrimination

Defining Responsible Use of Personal Information and Enhancing Individual Rights. Corporations have pervasive access to people's personal data, which can lead to discriminatory, predatory, and unsafe practices. Personal data collected by companies also often end up in the hands of the government, either through the direct sale of personal data or through data-driven systems purpose-built for the government. Clear baseline protections for data collection, including both primary and secondary uses of data, should be enacted to help prevent these harms.

Making Systems Transparent and Accountable. Governments and corporations must provide people with clear, concise, and easily accessible information on what data they collect and how it is used. This information can help equip advocates and individuals with the information to ensure that technologies are used in equitable and just ways. Any technology that has a consequential impact on people's lives should be deployed with a comprehensive, accessible, and fair appeals process with robust mechanisms for enforcement, and governments and corporations must be accountable for any misuse of technology or data. When careful examination reveals that a new, invasive technology poses threats to civil rights and civil liberties, such technology should not be used under any circumstance.

The Leadership Conference

Evidence that facial recognition technology can impede civil and human rights has never been clearer. With respect to law enforcement use of one specific type of biometrics technology—facial recognition—the evidence of impact on civil and human rights has never been clearer. The Leadership Conference has spoken out against law enforcement use of facial recognition since 2016, highlighting the inherent bias of these tools and their disparate impact on marginalized communities that were already over-policed.[iii]

In June 2021, The Leadership Conference, along with Upturn and New America's Open Technology Institute, released "Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology," which was signed by 40 advocacy organizations.[iv] Additionally, The Leadership Conference, the ACLU, and more than 45 advocacy organizations wrote a letter to the Biden administration calling for a moratorium on the government use of facial recognition technology.[v]

Most recently, in July 2021 testimony[vi] before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, The Leadership Conference highlighted six of the most pressing civil rights concerns that advocacy organizations have with law enforcement use of facial recognition technology:

1. Regardless of technical accuracy, law enforcement use of face recognition systems could exacerbate the harms of policing in communities that are already targeted by the police.
2. Law enforcement use of face recognition threatens individual and community privacy by allowing invasive and persistent tracking and targeting.
3. Law enforcement use of face recognition can chill First Amendment-protected activities.
4. Law enforcement use of face recognition can easily violate due process rights and otherwise infringe upon procedural justice.
5. Face recognition systems used by law enforcement often rely on faceprints that have been obtained without consent.
6. In addition to racial bias in how law enforcement use face recognition, the technology itself poses disproportionate risks of misidentification for Black, Asian, and Indigenous people.

The Obama administration's big data reports provided important next steps for future administrations, Congress, and regulators to ensure that technology is used to enhance equal opportunity, not undermine it. And they acknowledged the important role that the civil rights community, and specifically, the Civil Rights Principles, played in informing this critical work. The Biden administration has a critical opportunity to continue this work and to ensure that biometric technologies serve the best interests of each of us. To accomplish this goal, civil rights must be a key part of any public policy framework. We urge you to ensure that the voices of the civil and human rights community are heard in this important, ongoing national conversation.

Thank you for your consideration of these views. If you have any questions, please contact Anita Banerji, Senior Program Director, Media and Tech, at [redacted]

The Leadership Conference

Sincerely,

[redacted]

Wade Henderson
Interim President and CEO

[redacted]

Jesselyn McCurdy
Executive Vice President of Government Affairs

---

[i] https://www.civilrightstable.org/civil-rights-principles-for-the-era-of-big-data/

[ii] https://www.civilrightstable.org/principles/

[iii] The Leadership Conference on Civil and Human Rights, Letter to Principal Deputy Assistant Attorney General Vanita Gupta (October 18, 2016), https://www.aclu.org/sites/default/files/field_document/coalition_letter_to_doj_crt_re_face_recognition_10-18-2016_1.pdf; The Leadership Conference on Civil and Human Rights, Letter to Committee on Oversight and Reform about Protests (June 30, 2020), https://civilrights.org/resource/letter-to-committee-on-oversight-and-reform-aboutprotests/; The Leadership Conference on Civil and Human Rights, Comments in Opposition to Proposed Rulemaking: Collection of Biometric Data from Aliens upon Entry to and Departure from the United States (December 21, 2020), https://civilrights.org/resource/comments-in-opposition-to-proposed-rulemaking-collectionof-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/; The Leadership Conference on Civil and Human Rights, Civil Rights Groups Urge Strong Ethical Review of Axon's Police Technology (April 26, 2018), https://civilrights.org/2018/04/26/civil-rights-groups-urge-strong-ethical-review-axons-police-technology/.

[iv] The Leadership Conference on Civil and Human Rights et al., Civil Rights Concerns Regarding the Law Enforcement Use of Facial Recognition Technology (June 3, 2021), https://newamericadotorg.s3.amazonaws.com/documents/FINAL_Civil_Rights_Statement_of_Concerns_LE_Use_of_FRT_June_2021.pdf

[v] American Civil Liberties Union, Facial Recognition Technology Letter to President Biden (February 26, 2021), https://www.aclu.org/sites/default/files/field_document/02.16.2021_coalition_letter_requesting_federal_moratorium_on_facial_recognition.pdf

[vi] http://civilrightsdocs.info/pdf/policy/testimony/2021/071321-WrittenTestimony-BertramLee-HouseJudiciary-FacialRecognition.pdf

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Thorn

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

THORN

Submission by Thorn, a Nonprofit Organization, in Response to the Office of Science and Technology Policy's Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

Exhibited and potential benefits of a particular biometric technology:

Thorn welcomes the opportunity to provide information to the Office of Science and Technology Policy (OSTP) on some of the beneficial uses of biometric technologies to help inform the legislative framework surrounding them. Thorn is a non-profit organization that exists to build global technological solutions and infrastructure to combat child sexual abuse online. We believe in the power and potential of government, NGOs, and tech companies working together to eliminate child sexual abuse material (CSAM) online. This goal cannot be achieved by just one of these entities alone, and we appreciate OSTP's collaborative national initiative to develop an Artificial Intelligence Bill of Rights.

As an organization with a mission to use technology as a force for good, one important consideration we want to ensure is taken into account as the Bill of Rights is crafted, is how these powerful technologies can be used to guard the privacy and safety of children. At Thorn, we believe that leveraging tailored and specific artificial intelligence-aided technology, on behalf of children, will help to ensure that they share in the benefits of technological innovation designed with their safety, privacy, and welfare in mind.

Unfortunately, anywhere there is a upload button, you will find users uploading child sexual abuse material. Online reports of this abuse material have increased by 15,000% over the last 15 years, and the privacy of child victims is violated every time content is shared.[1] At Thorn, we believe the only way to disrupt and end the proliferation of CSAM on the internet is through the proactive use of targeted technological solutions. To this end, we develop technological tools to stop the spread

[1] National Center for Missing & Exploited Children, Key Facts

of abusive content by quickly identifying, removing, and then reporting CSAM from online platforms.

In the space of child protection, there are well established technologies that have been tested and refined for over a decade, but many of the most cutting edge technologies still need the space for further innovation. These technologies have proven results of finding and saving children from online sexual exploitation. Tailored technological solutions in this space are the future of protecting children from online exploitation, and there needs to be a legislative framework that allows for this crucial work to continue. We understand the concerns that some AI applications could lead to the invasion of individual users' privacy, but child advocacy organizations have always worked towards surgical and balanced solutions in order to protect children online.

Technology constantly changes and improves with time, and we believe that any legislative framework must reflect this reality. If regulation becomes indiscriminate, or does not provide the necessary flexibility for this specific use case, it can create unintended consequences that could deter the development of new technologies with the potential to protect children online. Because of this, legislation around artificial intelligence must allow for innovation and growth of preventative tools and measures developed to safeguard children from online sexual abuse.

For example, through the use of targeted biometric technology, an investigator could potentially identify a child whose abuse images are circulating online, because that technology is capable of identifying the child's specific body markers. There have been cases of some of the most egregious child sexual abuse where a child or prepetator has been identified through distinct body marks - whether it be tattoos, birthmarks, etc. Without this flexibility to innovate, perpetrators will be able to utilize the most sophisticated technology to abuse children, while the child protection ecosystem falls behind.

Another example of how AI can be effective in this space is through the development and deployment of classifiers that are trained on data to make predictions and decisions on new data. And, as online platforms continue to share data, users can fine-tune the models to improve predictions over time.

Our image based classifier is deployed to find new and unknown CSAM. This classifier

is based on a machine learning algorithm we created, and has been trained on known CSAM, benign imagery, and adult imagery data sets in order to make it highly accurate and precise at identifying CSAM. Identifying new CSAM at scale ultimately helps in the identification and rescue of children and stops the viral spread of abuse on the open web.

Similarly, our text analysis classifier was developed to help prevent the grooming of a child for abuse. Through pairing the latest research from the child safety ecosystem with state of the art Natural Language Processing tools, our text-based classifier detects potential instances of grooming for sexual exploitation. This classifier is able to give predictions for specific lines in conversations that could indicate grooming, enabling quick review for human moderators, and empowering online platforms to automate the detection of grooming conversations in real time. Effective grooming detection is a crucial step in preventing child sexual abuse from happening in the first place. It can mean the difference between exploitation happening or not, again, intercepting before the abuse happens.

These targeted, surgical detection methods have been designed solely to combat child sexual abuse and grooming, and maintaining the use of these methods gives consumers the privacy that is expected without enabling bad actors and online predators. The spread of CSAM will never end if we are unable to create and deploy preventative tools and measures.

Child sexual abuse detection technologies are cutting edge and designed to protect the most vulnerable population in our society. Given this sensitivity, we acknowledge that safeguards and greater transparency are necessary for artificial intelligence technology used in this space. Any artificial intelligence regulation must find a balance that protects the general consumer's privacy while still allowing for technology designed to protect children. We must not allow offenders the ability to reverse engineer technologies designed to keep our children safe. Any enhanced transparency should not impede the development of technologies that are used to protect children online.

We recommend that artificial intelligence-aided child sexual abuse detection methods be preserved, prioritized, and future-proofed in any legislative proposals around these powerful technologies. Recognizing that much of the narrative surrounding these technologies often centers on the potential harms of artificial intelligence and

biometric technologies, we hope the Office of Science and Technology Policy will also prioritize the benefits of these technologies on behalf of our children. In the same way we want to ensure these technologies do not overstep or abuse the rights of any person, they also should be utilize to protect the basic rights of our children to not be sexually abused or harmed. They are the future.

Thorn looks forward to serving as a resource to the Office of Science and Technology Policy regarding how we use biometric technologies to help reduce the spread of child sexual abuse material and to prevent child sexual expoitation.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

U.S. Chamber of Commerce's Technology Engagement Center

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 14, 2022

Office of Science and Technology Policy
1650 Pennsylvania Avenue NW
Washington, DC 20502

Re: Request for Information on Public and Private Sector Uses of Biometric Technologies [Docket Number 2021-21975]; 86 FR 56300

To Whom It May Concern:

The U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC") appreciates the opportunity to submit feedback to the Office of Science and Technology Policy (OSTP) in response to its request for information ("RFI") on "Public and Private Sector Uses of Biometric Technologies." C_TEC appreciates OSTP's efforts to "understand the extent and variety of biometric technologies in past, current or planned use.[1]" Biometric technologies are not new. Their origins can be traced back to the 1960s. However, since that time, technology has steadily improved. Notably, the recent enhancements in underlying artificial intelligence ("AI") and computing power have advanced the technology. Biometric technology has multiple beneficial functional applications in both the public and private sectors. We believe it has enormous potential to enhance security and safety and enable innovation across various industries.

The Chamber has long been a fierce advocate for "promoting accountability and consistency[2]," which looks to elevate any "unanticipated misuse or harms[3]" around the use of artificial intelligence and biometric technology. Therefore, the Chamber has developed principles around the use of "artificial intelligence[4]" and "facial recognition[5]," which highlight the need for transparency. Furthermore, the Chamber stands committed to working with the Office of Science Technology Policy

[1] https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies
[2] https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies
[3] https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies
[4] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles
[5] https://www.uschamber.com/technology/us-chamber-of-commerce-releases-facial-recognition-policy-principles

around its work to develop an AI Bill of Rights that allows for the "equitable harnessing[6]" of the benefits of AI and Biometrics technology.

Many of the questions posed within the RFI are directed towards how organizations and businesses develop their products. Because C_TEC is comprised of companies from a wide array of sectors who use biometric technology and AI in many different ways, we will focus our feedback on topics five and six, which look to address the specific benefits of biometric technology as well as governing principles.

Topic five: Exhibited and potential benefits of a particular biometric technology

C_TEC is exceptionally excited about the past, current, and future uses of biometric technology, which will provide ample benefits to society. Some of the biometric modalities producing the most exciting benefits include voice, facial, fingerprint, palm, and iris. However, vendors and end-users are increasingly leveraging a wide variety of other biometric technologies in diverse public-sector and private-sector applications.

While C_TEC will highlight many of the great uses of biometric technology, we would like to highlight a concern that “biometric technologies” are not fully defined within the RFI, which does not allow us to address the question regarding the “scope.” C_TEC believes there is a need to thoughtfully define the term “biometric technology” to reduce any misinterpretations of the scope of the RFI and the work of the Office of Science Technology Policy.

Voice:

Regarding voice technology and biomarkers, there is already excellent utilization of this technology within the healthcare sector. Current examples of the use of this technology include Cedar-Sinai, and Boston Children's use to keep in touch with their families, connect with care team members, easily access news and information and play music. Additionally, artificial intelligence to interpret patient intent enables the message to be sent to the appropriate care team member using existing hospital communication systems. This technology utilization will allow for better and more streamlined care for patients.

Furthermore, vocal biomarkers can be used for health tracking, triage, risk prediction, and detecting emergencies. C_TEC is also excited about using "voice technology" for healthcare as a remote patient monitoring tool. This includes uses within one's home to help patients adhere to post-discharge instructions or a

[6] https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

diagnostic tool. This technology is currently being used for things such as reminding patients to take their medications and to be able to share post-surgical recovery data between a patient's home and the hospital. This technology can significantly reduce pressure placed on the medical system and staff by enabling real-time engagement and remote care of certain situations.

C_TEC sees the use of voice biomarkers to further improve human-to-human interaction, such as through in-person health visits, by capturing notes to support care teams. Combined with AI, voice technology may be able to leverage data from visits to expedite fact discovery and diagnoses, assist providers in developing care recommendations, and potentially support claims processing.

Fingerprint & Palm:

Fingerprint technologies are the oldest biometric technologies, and the FBI has been using fingerprint technologies to support law enforcement and forensics since the 1960s[7]. Today, biometric technology vendors produce fingerprint, latent print, ten print, and palm print technologies for use not only in law enforcement settings but also in a wide variety of public and private sector settings. These technologies not only help generate leads in criminal investigations, but they also help secure our borders, conduct background checks, and facilitate access control to various facilities and devices.

Facial Recognition:

C_TEC also would like to highlight the benefits facial recognition technologies, which analyze facial features, generate biometric templates of these features, and compare the template generated from a probe image to one (in the case of facial verification) or many (in the case of template and the gallery template(s). Facial recognition technologies, when used effectively and appropriately, can help expedite and improve the accuracy and security of authentication and access control. For instance, because of the uniqueness of and security protections built into biometric templates, leveraging facial recognition technology, alongside user consent to use and transparency around such applications, has become an increasingly popular way to log into phones and devices to securely access information and programs.

C_TEC member companies also provide facial recognition technologies for a variety of commercial applications that include theft prevention in the retail industry, fraud detection, ticketless entry to event venues, keyless and cashless resort experience, and face pay services to secure and enhance customer experience in

[7] https://www.nist.gov/programs-projects/biometrics

financial transactions. This includes applications such as "identity check mobile," which uses facial recognition to verify a cardholder's identity for payment. This use has been found to be secure and provide ease of access to an individual's financial data.

C_TEC also sees a bright future for the use of biometric technology in everyday commerce. One of the exciting and innovative uses is opt-in frictionless retail, which allows customers to quickly maneuver throughout a retail store and pick up merchandise that is being tracked through sensors and checkout remotely. The technology provides customers with a more streamlined shopping experience. Furthermore, the use of this technology will help reduce unnecessary contact with store surfaces, which will help reduce transmission of germs onto store goers.

We also see great value in using facial recognition technology for remote virtual proctoring. This technology provides students and work professionals the ability to take exams in remote locations while at the same time maintaining the integrity of the exam. The technology further allows students to continue studies at times that are more convenient for their schedules, allowing students obtain a better work/school balance.

C_TEC would also like to highlight further government applications of facial recognition technology, which include improving border security at airports and other points of entry, detecting and combatting (attempted) identity theft, and helping to generate leads in criminal investigations. An example includes the federal governments use of facial recognition to help solve a case which a man was stalking 30 high school women through various social media outlets. Federal law enforcement obtained a warrant and used facial recognition technology through the Mississippi Fusion Center to identify and arrest the suspect.[8]

Top-performing face recognition technologies are highly accurate overall[9] and across demographic groups[10], and when used properly by trained operators, is much more accurate than the average human's facial recognition capabilities. Given the potentially serious consequences of misidentifying individuals in situations involving international air travel, obtaining government-issued identity documents, and criminal investigations, using face recognition technologies to improve the accuracy of identifications can be especially beneficial in these settings.

---

[8] https://www.justice.gov/usao-sdin/pr/mississippi-man-faces-interstate-stalking-charges-five-year-long-crime-against

[9] https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing; https://mdtf.org/Downloads/MatchingSystemResults.pdf.

[10] NIST has found that top-performing algorithms have "undetectable" false positive error rate differences across demographic groups based on race and sex. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Any broad sweeping effort to limit biometric facial recognition technology within the federal government has the potential to harm innovation throughout the facial recognition ecosystem. Furthermore, it would undermine the implementation of a long-standing, bipartisan congressional mandate to apply one of the 9/11 Commission Report recommendations, namely, a biometrically enabled immigration exit system. Given the diverse uses and benefits of facial recognition technology, C_TEC believes that facial recognition regulation frameworks should calibrate any restrictions or limitations that they impose to address the risk of a specific facial recognition directly.

Iris Biomarkers:

Additionally, C_TEC would like to highlight the benefits of iris recognition technologies. Because these technologies can achieve accuracy rates of over 99%[11] and have become more commercially available, passengers around the world are choosing to participate in opt-in programs that leverage iris recognition technologies (in conjunction with face recognition technologies) to securely and accurately verify their identies and expedite their passage through airports.

Behavioral Biometrics:

Finally, C_TEC would like to highlight the opportunities related to "behavioral biometrics". The financial industry is gradually moving towards the use of authentication solutions that rely upon behavioral biometric data; i.e., characteristics about an individual's interaction with their computer or smartphone device, including the use of their keyboard, mouse and/or the way in which they hold and interact with their device.

Behavioral biometric data has several advantages over knowledge-based (i.e., PIN or passwords) authentication solutions. These include reduced risk of social engineering and fraud given behavioral biometrics are difficult to copy and/or replicate. Use of behavioral biometrics also leads to reduced transaction failure and abandonment rates, and consequently reduced harm to consumers, as they cannot be forgotten like passwords or PINs.

Topic six: Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case.

C_TEC firmly believes that safe, ethical, and effective use of AI-enabled biometric technology can provide tremendous benefits to society. However, we

[11] https://pages.nist.gov/IREX10/

understand that biometrics technologies are increasingly being developed and deployed within critical processes (e.g., healthcare, employment, judicial, policing, etc.) where there is a concern that such systems could pose a risk to safety, privacy, and human rights if not appropriately vetted. In particular, C_TEC recognizes that inaccurate biometric technologies can contribute to misidentifications that, if not subject to effective human review and oversight, could result in delays in accessing a workplace or an essential service and/or unnecessary contact with law enforcement.

C_TEC also realizes that even highly accurate biometric technologies in conjunction with surveillance cameras could lead to tracking individuals in a way that infringes on individual privacy. C_TEC encourages U.S. policymakers to develop use-case-specific governance frameworks that aim to mitigate the risks that biometric technologies can pose in specific settings without unduly limiting the public's ability to reap the multitude of benefits that biometric technologies can produce. In addition to domestic biometric technology governance framework, international governance frameworks that the United States develops in coordination with allied partner nations that have a shared commitment to human rights and democratic freedoms can serve an important role in promoting the ethical and appropriate use of these valuable technologies abroad, while also strengthening international partnerships that help advance global economic efficiency and innovation.

C_TEC believes that the following principles around the use of facial recognition are the appropriate framework for any specific governance structure around the use of facial recognition technology and may be useful starting point for developing broader biometric technology governance frameworks as well.

1. **PRIORITIZE TRANSPARENT USE OF FACIAL RECOGNITION TECHNOLOGY**: Commercial and government users should be transparent about when and under what circumstances the technology is used as well as the processes and procedures governing the collection, testing, processing, storage, use, and transfer of facial recognition data.

2. **PROTECT PRIVACY AND PERSONAL DATA:** Policymakers should look to the U.S. Chamber of Commerce's Privacy Principles as a guide for pursuing privacy rules that fosters innovation while protecting human rights and civil liberties.

3. **PROMOTE BENEFICIAL USES OF FACIAL RECOGNITION TECHNOLOGY WHILE MITIGATING RISKS**: Policymakers should acknowledge the benefits of facial recognition technology and not support overly burdensome regulatory regimes, such as moratoriums or blanket prohibitions.

4. **PURSUE A RISK-BASED AND USE-CASE SPECIFIC REGULATORY APPROACH**: Regulation of facial recognition technology should be risk and

performance-based, take into account specific use-cases, and consider the application of existing regulations and laws.

5. **ESTABLISH A SINGLE NATIONAL GOVERNANCE AND REGULATORY FRAMEWORK**: Congress should ensure a clear and consistent approach to the regulation and governance of facial recognition technology by developing a national framework governing the use of facial recognition technology.

6. **SUPPORT THE DEVELOPMENT OF RISK-BASED PERFORMANCE STANDARDS**: In accordance with existing law, the establishment of standards should be voluntary, industry-driven, and consensus-based and should be undertaken by existing, independent standard-setting bodies, such as the National Institute for Standards and Technology (NIST). Standards should be flexible, use-case and performance-based, and non-prescriptive.

7. **ENSURE FEDERAL INVESTMENTS IN TESTING AND BENCHMARKING**: To build public and consumer trust, policymakers should prioritize standardized testing and benchmark through existing independent entities, like NIST. Policymakers should ensure NIST is provided with sufficient and modern resources to support testing and benchmarking efforts.

Conclusion:

In conclusion, C_TEC believes that AI-enabled biometric technology has enormous potential to transform entire industries, providing innovative benefits to consumers and enhancing personal safety, security and privacy for all Americans. While there may be risks associated with these technologies, it is important to evaluate the level of risk posed by technologies and their intended applications to determine an appropriate course of action for mitigating risks. It is also important to work alongside industry stakeholders to determine appropriate applications and considerations for various biometric use cases. We firmly believe that biometric technology has a critical role in the advancement of our society. C_TEC looks forward to continuing to collaborate with OSTP on this important matter and encourage OSTP to continue to engage stakeholders on all matters that address biometric and artificial intelligence technology.

Sincerely,

[redacted]

Michael Richards
Policy Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Uber Technologies

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Uber

January 15, 2022

Dr. Eric Lander
Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

[Submitted electronically via email]

RE: Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

Dear Dr. Lander:

Uber Technologies, Inc. ("Uber") respectfully submits these comments in response to the Request for Information ("RFI") titled *Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies,* published by the White House Office of Science and Technology Policy ("OSTP") on October 8, 2021[1]. Uber appreciates OSTP's consideration of the important issues surrounding the development and use of biometric technologies.

At Uber, we prioritize the safety and privacy of all users on our platform. This is because we're not just connecting people online—we're connecting people in person, in real time, in the real world. As our Privacy Principles and ESG Report highlight, we are committed to doing the right thing by our users when it comes to how we collect and use their personal data. This includes our use of biometric technology; we only collect biometric data that is needed for defined and publicly disclosed safety and security purposes. To properly protect individuals' privacy rights, we embed privacy into the design and architecture of our facial recognition technology products from start to finish. In addition, we apply access controls and encryption mechanisms to protect biometric data against loss, unauthorized access, destruction, use, modification, or disclosure.

Facial recognition technology is an integral part of our safety measures. We've developed screening processes so that users feel comfortable putting trust in the person driving a vehicle or

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

delivering food. However, these screenings can only be useful if we can verify that the person driving passengers or delivering food is who they say they are.

One way we do this is by using a feature called Real-Time ID Check ("RTID"), which prompts drivers and delivery people to take a selfie to confirm that they're the same person who went through all the necessary screenings to drive or deliver on our platform. Selfies are matched against the account holder's profile picture, which in turn has been checked against the official identification document submitted during the onboarding process.

The uploaded selfie gets sent to our third-party vendor, Microsoft. Microsoft compares it against the profile photo, and if the photos are similar enough, the driver or delivery person passes the check and is able to log right into their account. Where Microsoft's tool detects a difference, three human reviewers are asked to review the pictures.

The use of facial verification technology is not a step we take lightly, so we have put in place a number of safeguards for responsible use of RTID. First, every case in which a variance is initially detected is ultimately decided by human review. No one can permanently lose access to the Uber platform based solely on technology. Second, users are able to appeal when they feel that something has gone wrong. We have also conducted internal fairness assessments to evaluate how the technology works for people with different skin complexions. Those assessments found no evidence that the technology is flagging people with darker skin complexions more often.

Uber supports conducting these types of fairness and bias assessments for all technologies that utilize biometric data to make sure they work as intended and do not create disparate impacts on underserved or underrepresented communities. Similarly, regulators should encourage the private sector to be vigilant for bias. They can do this by providing companies a safe harbor for engaging in good faith efforts to measure and mitigate bias.

We appreciate the opportunity to provide this input to OSTP and look forward to continued engagement on this important topic.

Sincerely,

CR Wooters
Head of Federal Affairs
Uber Technologies, Inc.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

University of Pittsburgh
Undergraduate Student
Collaborative

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

"Evidence, Pitfalls and Presumptions in Facial Recognition Technology"
Response to White House Request for Information (RFI) on Biometrics
University of Pittsburgh undergraduate student collaborative
October 26, 2021

Contents

White House Request for Information

On October 8, 2021, the U.S. White House Office of Science and Technology Policy released a "Request for Information" on biometric technology, calling on practitioners, experts, and members of the general public to submit comments regarding potential benefits, harms, and best practices relating to face recognition technology (FRT):

> The Office of Science and Technology Policy (OSTP) requests input from interested parties on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states. The purpose of this RFI is to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the

stakeholders that are, or may be, impacted by their use or regulation. OSTP encourages input on both public and private sector use cases.

Subsequent reporting highlights significance of the research area by framing the White House RFI as part of an effort by White House science advisor Eric Lander and OSTP deputy director Alondra Nelson to explore a "Bill of Rights" for AI.[1]

Executive Summary of Response

Research from an interdiciplinary undergraduate student collaborative at the University of Pittsburgh responds to the White House Request for Information (RFI) on biometrics through critical assessment of strengths, weaknesses, and best practices for use of facial recognition technology (FRT) in six domains: education, airport security, retail sales, law enforcement, medicine, and cellphone security. Critical approach to the assessment entailed collaborative research in an upper-level communication course, with six student teams using Zoom and Google Jamboard to collate, sift and share evidence regarding FRT in specific domains. Comparison across domains yields actionable insight linked to the RFI area prompts, especially "harms," "benefits," and "best practices" relating to FRT. Assessment scope is limited to FRT and the exercise does not address biometric technology such as gait detection or inference-to-emotion. The assessment highlights how conceptual terms such as presumption, burden of proof, pitfall and evidence inform choices articulated in the White House RFI, as well as the importance of transparency and addressing challenges posed by "off-purpose use" of FRT. One key finding

[1] Eric Lander and Alondra Nelson, "Americans need a Bill of Rights for an AI-powered world," *Wired,* October 8, 2021, https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/; see also Jim Nash, "Is it time for a Bill of Rights to keep AI in its place?," *Biometric Update,* October 11, 2021, https://www.biometricupdate.com/202110/is-it-time-for-a-bill-of-rights-to-keep-ai-in-its-place; and Aaron Boyd, "White House wants to know how biometrics like facial recognition are being used," *Nextgov,* October 12, 2021, https://www.nextgov.com/emerging-tech/2021/10/white-house-wants-know-how-biometrics-facial-recognition-are-being-used/186033/

is that establishing a presumption that FRT should *not be used* may reverse the prevailing burden of proof and require federal agencies to publicly articulate narrowly tailored uses for FRT, explain compelling interests justifying such use, and create guardrails to prevent harmful off-purpose use.

Background and Introduction to Domains of Analysis

This comment presents condensed content from the [redacted] created collaboratively during the research exercise, which took place during undergraduate class sessions in the Fall 2021 academic term, including approximately 33 students.[2] Following summaries of student findings in areas of education, airport security, retail sales, law enforcement, medicine, and cellphone security, the comment links student discussion with key topics of concern in the White House RFI.

Education

FRT **may be helpful** to students who have certain impairments, for example Listerine has supported a smartphone app for blind users that sends a message when a person in the camera's field of vision smiles.[3] Ellucian offers a suite of FRT tools designed to help gauge students'

[2] Offered through the University of Pittsburgh's Department of Communication the upper-level undergraduate course on "Evidence" explores types of evidence, methods for testing and evaluating evidentiary claims, and controversies about the evolving role of evidence in professional and public life. Students in a 2017 section of Evidence partnered with the "First Draft" fact-checking coalition to vet and polish its "CrossCheck" website, which was widely acknowledged as playing a key role in safeguarding the 2017 presidential election in France against Russian efforts to influence the election with targeted information disorder (see https://crosscheck.firstdraftnews.org/france-en/).

[3] Sarah Vizard, "Listerine helps blind people experience a smile," *Marketing Week,* September 1, 2015, https://www.marketingweek.com/listerine-shakes-up-oral-care-sector-with-app-that-lets-blind-people-experience-a-smile/

reactions to learning and support their engagement with the material.[4] One **potential danger** is that ubiquitous FRT could threaten privacy by normalizing surveillance of students and entrenching stereotype bias against certain demographics of students.[5] FRT information gathered in educational settings could possibly be passed to different agencies outside the classroom (child welfare, immigration, law enforcement), where such "off-purpose" use of facial images may pose risks to subjects.[6] **Best practices** may include work to improve diversity used in probe photo banks, limit the length of data retention, make people aware of how long their data is stored before deletion, be transparent to stakeholders about FRT use, and assert control over maintenance and management for FRT systems, i.e. don't let them "do their own thing."[7]

Airport Security

Potential benefits include ease of travel (boarding planes more quickly and easily) and a lower risk of COVID-19 (not having to take off masks to verify identity at the airport).[8] Although FRT accuracy has increased overall in airports, accurate identification of masked travelers for median systems is only 77%.[9] **Potential harms** include an invasion of privacy and an overreach of

[4] Ellucian, "Facial recognition can give students better service (and security)," Ellucian website, accessed October 14, 2021, https://www.ellucian.com/blog/facial-recognition-campus-benefits-security-risks

[5] John S. Cusick and Clarence Okoh, "Why schools need to abandon facial recognition, not double down on it," *Fast Company,* July 23, 2021, https://www.fastcompany.com/90657769/schools-facial-recognition

[6] Cusick and Okoh, "Why schools need to abandon."

[7] SAFR, "Privacy by design: Best practices for using facial recognition to support safer K-12 campuses," SAFR website, accessed October 14, 2021, https://safr.com/general/privacy-by-design-best-practices-for-using-facial-recognition-to-support-safer-k-12-campuses/

[8] Jeffrey N. Rosenthal, David J. Oberly, & Andrew H. Schrag, "Biometric privacy in the era of COVID-19: facial recognition compliance for airports and airlines," *Aviation Today,* February 8, 2021, https://www.aviationtoday.com/2021/02/08/biometric-privacy-era-covid-19-facial-recognition-compliance-airports-airlines/

[9] U.S. Department of Homeland Security, "Airport screening while wearing masks? Facial recognition tech shows up to 96% accuracy in recent test," News Release, January 4, 2021, https://www.dhs.gov/science-and-technology/news/2021/01/04/news-release-airport-screening-while-wearing-masks-test

government power/control. Benefit/harm calculations may be influenced by a "convenience trap," with privacy-invading technology being normalized with the idea of it being easier than passports.[10] During a pandemic it is safer to keep masks on, but this increases risk of inaccurate identification, especially in high trafficked areas. One important idea emerging from the literature is stress on the **safeguard** of being able to opt out of facial recognition.

Retail

Use of FRT in the retail sales context may **confer potential benefits** by helping stores customize the shopping experience, allowing employees to provide better customer service. FRT also can reduce shoplifting — the mere presence of surveillance may deter some customers from theft. According to the National Institute of Standards and Technology, facial recognition software was worse at identifying women and non-white people, **potentially leading to harmful** misidentification of people in retail settings.[11] Inequitable application of FRT may exacerbate these biases, for example Rite Aid uses facial recognition more in predominantly non-white neighborhoods and low-income neighborhoods.[12] Biometric information is protected as personal data in states with strong privacy laws. **Best practice** transparency may be achieved with conspicuous signs or statements of company policy on websites or in stores, this way people are always informed they are being recorded.

[10] Geoffrey A. Fowler, "Don't smile for surveillance: Why airport face scans are a privacy trap," *Washington Post,* June 10, 2019, https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/

[11] Drew Harwell, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," *Washington Post,* December 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[12] Dave Gershgorn, "Retail stores are packed with unchecked facial recognition, civil rights organizations say," *The Verge,* July 14, 2021, https://www.theverge.com/2021/7/14/22576236/retail-stores-facial-recognition-civil-rights-organizations-ban

Law Enforcement

Exhibited or potential benefits in this area include help in finding criminals.[13] Exhibited or potential harms in this area include the fact that the software itself is racist, as its programmed using white faces — Asian and African American people are up to 100 times more likely to be misidentified than White men, heightening privacy concerns and risks of faulty accusations.[14] **Best practices and safeguards** may include feed more faces into the systems, so more races are easily identifiable, and asking for consent and written release when using facial recognition systems.[15]

Medicine

FRT applications in medicine may yield **potential benefits** by expediting diagnosis for many (often rare) diseases or conditions, potentially lowering cost of care due to fewer hours / doctor visits needed for diagnosis.[16] One facial recognition app keeps all medical records and files in one place that can be accessible for patients. This app has "two different patient-provided verifications" to increase patient confidentiality and safety.[17] There may be **potential harms** of

[13] Craig McCarthy, "Facial recognition leads cops to alleged rapist in under 24 hours," *New York Post,* August 5, 2019, https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/

[14] Adi Robertson, "Detroit man sues police for wrongfully arresting him based on facial recognition," *The Verge,* April 13, 2021, https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest

[15] Martin Zizi, "How facial recognition needs to improve to be effective," *Forbes,* October 4, 2019, https://www.forbes.com/sites/forbestechcouncil/2019/10/04/how-facial-recognition-needs-to-improve-to-be-effective/?sh=541021302cdf

[16] Catherine Offord, "Deep-learning algorithms could help doctors narrow in on the causes of certain medical conditions, say researchers," *The Scientist,* January 8, 2019, https://www.the-scientist.com/news-opinion/ai-app-identifies-rare-genetic-disorders-from-photos-of-patient-faces-65295

[17] Byoungjun Jeon, et al., "A facial recognition mobile app for patient safety and biometric identification: design, development, and validation," *JMIR Mhealth Unhealth,* 7 (April 2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6475824/

over-reliance on FRT in medical settings when identification is not completely accurate. Health care providers might get a faulty diagnosis at first and keep going to prescribe incorrect treatments. Patients may give consent for their photos to be used, but they don't know the extent to which they're being used for. Apps may tend to work better for white patients, given the way FRT is trained on predominantly white faces, introducing potential racial inequality into the health care system. Finally, FRT in health care settings can increase rates of disease transmission and may be almost entirely inaccurate when the patient is unconscious.[18] Potential **best practices** include possible updates needed to HIPAA laws to include stored images of faces, requirements to disclose to patients all possible uses of the technology/their photos, and improving recognition of all faces, not just white ones.

Cellphone Security

FRT technology can be integrated into cellphones, providing a **benefit** of convenient, relatively accurate, security of personal and financial information. **Potential harms** include privacy concerns (where is the data being stored? is it shared with/sold to third parties?) and the fact that FRT could be vulnerable to hacking and exploitation, especially less sophisticated (2D) technology. **Best practices** for software companies may include keeping their algorithms updated to prevent hackers from learning how to override the algorithm and government regulation of selling data to third parties without explicit consent of users.

[18] Jeon, et al., "Facial recognition mobile app."

Conclusions

One common thread of analysis emerging across domains concerns spillover of FRT to off-purpose use. The student group focusing on education found FRT information gathered in educational settings could possibly be passed to different agencies outside the classroom (child welfare, immigration, law enforcement) where such 'off-purpose' use of facial images may pose risks to subjects. Likewise in medical contexts, patients may give consent for their photos to be used in therapeutic FRT, but they don't know the extent to which their images might migrate to other platforms and projects. Furthermore, with cellphone security, face images stored by cellphone companies for biometric security purposes may migrate and be monetized, presenting potential privacy harms to unsuspecting users.

Another prominent theme of analysis concerns importance of providing people with ways to opt-out of default FRT biometric systems. Yet opt-out routes only work if people are aware that FRT is being deployed to catch their image. Thus, the student group focusing on education cites SAFR's call to "be transparent to stakeholders about FRT use."[19] And the student group addressing retail cites calls for stores to make prominent displays signaling to shoppers that their faces may be under surveillance. Although measures to require FRT developers to disclose the source code underlying their applications may meet stiff resistance on grounds that such measures would require disclosure of trade secrets, transparency regarding FRT training processes (such as audits of images in the training pool and how they are used) may be easier to achieve, with potential to address the significant “garbage in, garbage out” problem facing FRT.[20]

[19] SAFR, "Privacy by design."

[20] Clare Garvie, "Garbage in, garbage out: Face recognition on flawed data," Georgetown Law Center on Privacy & Technology Brief, May 16, 2019, https://www.flawedfacedata.com

Student research in the airport security area amplified the powerful locution, "convenience trap" to describe uncritical appropriation of FRT in airports.[21] The trap here entails how easy it is to accept apparently minor privacy tradeoffs in the name of marginal convenience gains. One or two isolated decisions may seem inconsequential, yet multiplication of such decisions at scale can result in a pitfall where users feel trapped by an intrusive surveillance regime that was never vetted in its entirety. In evidence-based policy analysis, Giandomenico Majone develops the term 'pitfall' to describe "a conceptual error into which, because of its specious plausibility, people frequently and easily fall."[22] Possible remedies to the convenience trap pitfall may include providing users with clear convenience alternatives to FRT that informs their privacy decision-making.

Finally, two concepts from the field of communication may lend perspective on common threads emerging from this analysis. In argumentation theory, 'presumption' is defined by Richard Whately in *Elements of Rhetoric* as: "a predisposition to believe that a claim is correct until overwhelming evidence proves otherwise."[23] Closely related to presumption is the concept 'burden of proof,' which Whately says is "the obligation to offer reasons sufficient to overcome presumption."[24] A presumption that FRT is acceptable unless proven otherwise may make it difficult to track and control rapid development and diffusion of the technology, especially across domains and purposes. Conversely, a 'rebuttable presumption' against FRT use could spur clear guidelines that technology advocates would need to meet a burden of proof to overcome

[21] Fowler, "Don't smile."

[22] Giandomenico Majone, *Evidence, Argument and Persuasion in the Policy Process* (New Haven: Yale University Press, 1992): 52.

[23] Richard Whately, "From *Elements of Rhetoric, The Rhetorical Tradition,"* in *The Rhetorical Tradition: Readings from Classical Times to the Present,* ed. Patricia Bizzell and Bruce Herzberg (Boston: Bedford, 1990): 846-847.

[24] Whately, *Elements of Rhetoric,* 846-847.

such presumption. Such burden of proof standards may incorporate several of the best practices identified in this report, such as transparency, narrowly tailored uses for FRT, and defense of compelling interests justifying such use, as well as creation of durable guardrails to prevent drift to harmful off-purpose use and articulation of less invasive alternatives to achieve marginal convenience gains afforded by FRT.

Corresponding editor and comment filer: Gordon R. Mitchell, University of Pittsburgh

[redacted]

Corresponding student author: ?

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Upturn

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Upturn
Toward Justice in Technology

January 15, 2022

Office of Science and Technology Policy
Submitted via email to BiometricRFI@ostp.eop.gov

RE: Request for Information on Public and Private Sector Uses of Biometric Technologies (FR Doc. 2021-21975)

Thank you for the opportunity to respond to this Request for Information on Public and Private Uses of Biometric Technologies. Upturn is a research and advocacy group that works to advance equity and justice in the design, governance, and use of technology.

We write in support of the Office of Science and Technology Policy's efforts to protect people's fundamental rights and opportunities as powerful institutions continue to use data-driven technologies to shape key decisions about people's lives. These technologies, which include biometric technologies, often mirror and exacerbate historical racial and economic disparities in housing,[1] employment,[2] public benefits,[3] the criminal legal system,[4] and other areas of opportunity and wellbeing.

[1] A 2019 investigation of mortgage lending data found, for example, that Black people applying for loans were 80% more likely to be denied than white applicants. *See* Martinez, Emmanuel and Lauren Kirchner. "The Secret Bias Hidden in Mortgage-Approval Algorithms." *The Markup*. (Aug. 25, 2021). www.themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.
[2] In 2017, Amazon ended development of a machine learning tool to score job applicants after realizing that it lowered scores based on factors including the inclusion of the word "women's" and attending all-women's colleges. *See* Dastin, Jeffrey. "Amazon scraps secret AI recruiting tool that showed bias against women." *Reuters*. Oct. 10, 2018. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. An audit of another resume screening tool revealed that two of the factors identified by the model as predictive of good job performance were having the name Jared and playing high school lacrosse. *See* Gershgorn, Dave. "Companies are on the hook if their hiring algorithms are biased." *Quartz*. Oct. 22, 2018. https://qz.com/1427621/companies-are-on-the-hook-if-their-hiring-algorithms-are-biased/.
[3] McCormick, Erin. "What happened when a 'wildly irrational' algorithm made crucial healthcare decisions." *The Guardian*. (July 2, 2021). https://amp.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions.
[4] Robinson, David and Logan Koepke. "Stuck in a Pattern." *Upturn*. (Aug. 31, 2016). https://www.upturn.org/work/stuck-in-a-pattern/.

Across these areas, technologies are often used to make political decisions that can substantially affect people's material conditions, especially in the absence of careful attention and government regulation.[5] Over the past few decades, these technologies have undermined existing legal protections, including longstanding civil rights protections that have not kept pace with technology.[6]

1. **Biometrics are just one type of technology that are shaping people's rights and opportunities and deepening existing racial, economic, and other social disparities.**

Biometric technologies are among the latest in a long line of technologies that purport to measure people's attributes and predict future behavior, often with serious consequences. For decades, both governments and the private sector have used digital technologies to help determine people's access to social resources, such as housing and government benefits; economic opportunities, including jobs, credit, and education; and basic autonomy and wellbeing, including healthcare and public safety.

Today's terminology places all of these technologies in the frame of "AI," which confers more complexity and novelty than the issues often deserve. The most consequential technologies that are affecting people's rights and shaping their opportunities today are often not new — and the problems that these technologies exacerbate, such as racial, gender, disability, and other forms of discrimination and inequities, are longstanding. For instance, statistical risk assessment tools that states are adopting today for pretrial release decisions date back to at least the 1990s.[7] Consumer credit scoring algorithms, like FICO, emerged in the 1980s.[8]

The same concerns that animate today's call for a new Bill of Rights for an "AI-powered world" were raised during the Obama administration, under the frame of "big data,"

[5] For example, in 2017, Immigration and Customs Enforcement (ICE) quietly changed its risk assessment tool so that it no longer made any recommendations to release people awaiting deportation hearings. *Jose L. Velesaca v. Chad Wolf et al.* United States District Court for the Southern District of New York. 1:20-cv-01803. Feb 28, 2020. https://www.nyclu.org/en/cases/jose-l-velesaca-v-chad-wolf-et-al.
[6] *See, e.g.*, Solon Barocas and Andrew Selbst. "Big Data's Disparate Impact." 104 Calif. L. Rev. 671. (2016). https://www.californialawreview.org/print/2-big-data.
[7] For example, COMPAS, a hotly contested tool that many states have adopted to inform pretrial release decisions, was first developed in 1998. VPRAI, another widely-used pretrial risk assessment tool, was first developed in 2003. *See* https://pretrialrisk.com/the-basics/common-prai/.
[8] Hill, Adriene. "A brief history of the credit score." *Marketplace*. (Apr. 22, 2014). https://www.marketplace.org/2014/04/22/brief-history-credit-score/.

which was the fashionable term at the time.[9] While biometric technologies, particularly recent applications of face recognition, may be an attractive starting point, this administration must consider the impact of a broader scope of technologies and data practices, most of which are not biometrics or AI.

Consider a job applicant who is applying online for an hourly job. Many large employers in the U.S. now use multipurpose "applicant tracking systems" to manage their hiring processes, which often include background checks and a variety of online skills and personality screening tests. Some personality tests used in this context purport to assess people's trustworthiness and other traits, but in ways that reflect racist and ableist assumptions and anti-union motivations.[10] While these aren't complex technologies, they are among the ones that regulators like the Equal Employment Opportunity Commission should center in any examination of hiring discrimination and technology. To be sure, some vendors, like HireVue, have sought to introduce face or voice analysis technologies into employers' interviewing processes, but the practical impact of these applications today remains quite limited.[11]

Similarly in other areas, many well-entrenched technology and data practices continue to have adverse impacts on Americans' everyday lives: the use of eviction and criminal records in tenant screening tools,[12] increased digital tracking of families in the child welfare system[13] and of workers in home care,[14] law enforcement searches of people's

[9] *See* "Big Data: Seizing Opportunities, Preserving Values." Executive Office of the President. (May 2014). https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights." Executive Office of the President. (May 2016). https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[10] Rieke, Aaron; Urmila Janardan; Mingwei Hsu; and Natasha Duarte. "Essential Work." Upturn. (July 6, 2021). https://www.upturn.org/work/essential-work/.

[11] Knight, Will. "Job Screening Service Halts Facial Analysis of Applicants." *Wired*. (Jan. 12, 2021). https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/.

[12] Public Hearing on B23-149, Fair Tenant Screening Act of 2019, B23-498, Intersectional Discrimination Protection Amendment Act of 2019, B23-195, Michael A. Stoops Anti-Discrimination Amendment Act of 2019: Council of the District of Columbia Committee on Government Operations. October 27, 2020. (Testimony of Natasha Duarte and Tinuola Dada). https://www.upturn.org/static/files/2020-10-27-testimony-DC-fair-tenant-screening-act.pdf

[13] Roberts, Dorothy. "Child protection as surveillance of African American families." *Journal of Social Welfare and Family Law*. Vol 36. (2014). https://www.tandfonline.com/doi/abs/10.1080/09649069.2014.967991.

[14] Mateescu, Alexandra. "Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care." *Data & Society.* (Nov. 16, 2021). https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care.

cellphones,[15] and so on. Practices and systems like these have harmed people for decades — scrutiny cannot only be limited to emerging tools like biometrics or AI.

2. It's inadequate to address the harms of technology by examining technology in isolation. It's vital to consider the broader social, political, and historical context in which technology is used.

Technology tends to amplify structural power — and technology's impact depends not only on its design, but also on the broader social, political, and historical context in which it is used. While work to assess the statistical validity of a technology may provide important technical guideposts, additional perspectives are needed to more fully evaluate the potential effects of technology in various social contexts.

As a case in point, researchers and government agencies have worked to assess racial and gender disparities in popular face recognition programs.[16] These studies have been indispensable to understanding these programs' flaws. But even a technically "perfect" face recognition system would still perpetuate many social harms, including the harms of increased surveillance.[17] This is why, last year, over 40 civil society organizations called for an end to law enforcement's use of face recognition.[18] Due to the long history of racial discrimination and abuse by law enforcement in the United States, which continues to this day, the organizations concluded that "in the context of policing, face recognition is always dangerous—no matter its accuracy."[19]

In other cases, the use of a technology may benefit some people while at the same time harming others. For example, the use of face recognition to verify the identities of people

[15] Law enforcement uses mobile device forensic tools (MDFTs) to extract and search data on people's phones. The software includes face recognition capabilities for searching photos stored on the phone. Koepke, Logan; Emma Weil; Urmila Janardan; Tinuola Dada; and Harlan Yu. "Mass Extraction." *Upturn*. (Oct. 20, 2020). https://www.upturn.org/work/mass-extraction/.

[16] Buolamwini and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." (2018). http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.; Grother, Patrick; Mei Ngan; Kayee Hanaoka. "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects." *NISTIR 8280, National Inst. of Standards and Technology*. (December 2019). https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[17] Garvie, Clare; Alvaro Bedoya; and Jonathan Frankle. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *Georgetown Law Center on Privacy & Technology*. (Oct. 18, 2016). https://www.perpetuallineup.org/.

[18] New America's Open Technology Institute, The Leadership Conference on Civil and Human Rights, and Upturn, et al. "Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology." (June 3, 2021). https://www.newamerica.org/oti/press-releases/civil-society-coalition-releases-statement-of-concerns-regarding-law-enforcement-use-of-face-recognition-technology/.

[19] *Id.*

applying for unemployment benefits may speed up the process for those who have easy access to smartphones and for whom the software works, while creating barriers for others.[20] Technology can also shift and widen power imbalances, such as when landlords install face recognition to control access to their buildings.[21] The problems here are not only about the technology's accuracy or validity, but are largely tied to existing social inequities and harms that technology further amplifies.

For these reasons, policy debates about the merits of certain technologies need to be rooted in particular social contexts, not in a vacuum. To that end, Upturn, ACLU, the Leadership Conference on Civil and Human Rights, and a coalition of other organizations recently urged relevant federal agencies to step up their regulatory and enforcement activities to specifically address technology's role in discrimination in housing,[22] hiring,[23] and financial services.[24]

3. **Legal barriers such as trade secrets and non-disclosure agreements often hamper efforts to independently scrutinize the use of technologies. Even still, creating meaningful transparency is only the first step to addressing harms.**

Too often, it's difficult or impossible for researchers, advocates, investigative journalists, and communities to interrogate and challenge the use of technologies. While transparency alone will not mitigate the harms, it is an important baseline upon which people can begin to ask questions about how technologies are used and the potential ways they create or exacerbate inequities.

---

[20] Kenney, Andrew "'I'm shocked that they need to have a smartphone': System for unemployment benefits exposes digital divide." *USA Today*. (May 2, 2021). https://www.usatoday.com/story/tech/news/2021/05/02/unemployment-benefits-system-leaving-people-behind/4915248001/.

[21] Landlords are increasingly using technology to manage their interactions with current and potential tenants, *e.g.* https://antievictionmappingproject.github.io/landlordtech/. One high-profile example of tenant organizing to resist the use of biometrics happened in New York City in 2019, when the owner of a large rent-stabilized building attempted to install a face recognition system to control access to the building. *See* Durkin, Erin. "New York tenants fight as landlords embrace facial recognition cameras." *The Guardian*. (May 30, 2019) https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex.

[22] "Addressing Technology's Role in Housing Discrimination." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technologys-role-in-hiring.

[23] "Addressing Technology's Role in Hiring Discrimination." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technology-housing.

[24] "Addressing Technology's Role in Financial Services Discrimination." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technologys-financial.

One way that technology shifts power is through opacity. While opacity is often attributed to the complex nature of new technologies, such as machine learning models, opacity is often also created or furthered through legal and policy choices that put corporate interests above people's fundamental rights.

For instance, claims of trade secrecy have prevented criminal defendants from scrutinizing evidence created by potentially flawed probabilistic DNA analysis software used by law enforcement.[25] At least two courts have ordered disclosure of the software's source code to uphold the constitutional rights of criminal defendants to confront the evidence against them.[26] Such trade secrets claims have been made not only by private vendors like TrueAllele, but also by government agencies seeking to shield their decision-making tools from independent scrutiny.[27] In a similar vein, private vendors and government agencies have used non-disclosure agreements to hide the mere fact that certain technologies are in use.[28]

At the state level, one step forward has been Illinois's Biometric Information Privacy Act (BIPA), which requires companies to provide disclosure and obtain individual consent before collecting and using biometric information, and prohibits companies from selling

---

[25] Wexler, Rebecca. "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System." 70 Stanford Law Review 1343. (2018), 1368. https://www.stanfordlawreview.org/print/article/life-liberty-and-trade-secrets/.

[26] In February 2021, a New Jersey appeals court ruled that trade secrets can't be used to limit defense access to source code and other documentation for the DNA software used to analyze evidence in *State v. Pickett* (https://www.njcourts.gov/attorneys/assets/opinions/appellate/published/a4207-19.pdf?c=0qT). This was an important win in the ongoing fight to stop companies' intellectual property rights from infringing on defendants' constitutional rights. Upturn and Harvard's Cyberlaw Clinic submitted an amicus brief in the case, arguing for the need for independent and adversarial review of the software (https://www.upturn.org/work/amicus-brief-in-new-jersey-v-pickett/). That same month, the U.S. District Court for the Western District of Pennsylvania ordered disclosure of source code for the same software in *U.S. v. Ellis* (https://storage.courtlistener.com/recap/gov.uscourts.pawd.262237/gov.uscourts.pawd.262237.138.0_1.pdf).

[27] New York City's Office of the Chief Medical Examiner refused to share source code with defendants claiming that the software was "proprietary and copyrighted." A judge later ordered OCME to disclose the source code and an expert reviewer identified issues in the source code that could affect the software's assessment of the likelihood that a given person's DNA is in the mixture. Kirchner, Lauren. "Thousands of Criminal Cases in New York Relied on Disputed DNA Testing Techniques." (Sept. 4, 2017). *ProPublica* and *New York Times*. https://www.propublica.org/article/thousands-of-criminal-cases-in-new-york-relied-on-disputed-dna-testing-techniques.

[28] Wessler, Nathan Freed. "Documents in ACLU Case Reveal More Detail on FBI Attempt to Cover Up Stingray Technology." *American Civil Liberties Union*. (Sept. 24, 2014). https://www.aclu.org/blog/documents-aclu-case-reveal-more-detail-fbi-attempt-cover-stingray-technology.

or further sharing biometric data without consent.[29] While notice-and-consent can place undue burdens on individuals and may be insufficient to address systemic harms,[30] BIPA gave rise to a number of high-profile class action lawsuits and settlements seeking to control how biometrics are used.[31]

4. Regulators and enforcement agencies must actively measure, audit, and address systemic discrimination where technologies are used, and consider non-technological alternatives.

Inferential and other predictive technologies make probabilistic guesses and they inevitably make mistakes.[32] They also often fail for more prosaic reasons, due to inequities in access to or familiarity with smartphones and other technological requirements. When these technologies are used to mediate high-stakes decisions, such as determining access to crucial government services and benefits, these failures are not only frustrating and time-consuming but in some cases life-threatening. Even when these technologies work, they can introduce friction and rigidity to processes that ultimately hinder people's access to vital resources and opportunities. These barriers disproportionately harm people of color, poor people, disabled people, and others.

During the pandemic, as millions of workers sought unemployment benefits, many states began to adopt face recognition tools to verify people's identities. But this created significant burdens for many who either did not have access to smartphones, or for whom the software failed to match their identity.[33] Many were then required to wait on hold for

[29] Biometric Information Privacy Act, 740 ILCS 14 (2008). https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[30] One study estimated the time it would take people to read the privacy policies of all the sites they visit at 201 hours per year. Cranor, Lorrie Faith and Aleecia M. McDonald. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society.* 2008 Privacy Year in Review issue. http://www.is-journal.org/ (Accessed at https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf). On inadequacies of notice-and-consent *see, e.g.* Nehf, James P., "The Failure of 'Notice and Consent' as Effective Consumer Policy." (August 21, 2019). https://ssrn.com/abstract=3440816.

[31] *See ACLU v. Clearview AI*. https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint; and *Patel v. Facebook*. https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html. Facebook settled *Patel* for $650 million in February 2021. https://www.courthousenews.com/wp-content/uploads/2021/02/facebook-settle-approval-2.26.21.pdf.

[32] These mistakes can arise from false matches or non-matches when biometrics are used for identity verification. Other mistakes stem from false assumptions, or a fundamental lack of scientific grounding, when technology attempts to infer demographic traits, behavior, emotional state, or intent.

[33] Lyons, Kim. "Facial recognition software used to verify unemployment recipients reportedly doesn't work well." *The Verge*. (June 19, 2021). https://www.theverge.com/2021/6/19/22541427/facial-recognition-software-verify-unemployment-benefits-id-me.

hours to resolve issues[34] and some — without alternate options or timely redress — ended up abandoning the process altogether in frustration, giving up on the benefits that they deserved to receive.[35] Importantly, because of existing disparities across race, class, and geography in access to smartphones and broadband internet, these burdens too often fell on those who were most vulnerable and most in need of benefits.[36]

In another context, the growing popularity of e-proctoring software — from K-12 classrooms to bar examinations[37] — creates systems that often fail to verify the identities of Black students and other students of color,[38] arbitrarily and unfairly flag some students for cheating, and set up rigid behavioral rules that punish students for getting up to use the bathroom or looking around the room.[39] While these are problems for any student, such software can impose much worse effects on disabled students, "which can also exacerbate underlying anxiety and trauma."[40] Black students and other students of color,

[34] One woman in Colorado tried and failed 60 times to take a suitable picture on her older smartphone to verify her identity. *See* Kenney, Andrew. "'I'm shocked that they need to have a smartphone': System for unemployment benefits exposes digital divide." *USA Today*. (May 2, 2021). https://www.usatoday.com/story/tech/news/2021/05/02/unemployment-benefits-system-leaving-people-behind/4915248001/.

[35] One person applying for unemployment benefits in California spent months submitting paperwork and calling a hotline before being asked to use face recognition to verify their identity. After multiple attempts, the system couldn't match their face and they eventually stopped trying to access unemployment benefits. *See* Sato, Mia. "The pandemic is testing the limits of face recognition." *MIT Technology Review*. (Sept. 28, 2021). https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition/.

[36] White Americans are more likely to have a computer and broadband internet than Black or Hispanic Americans. *See* Atske, Sara and Andrew Perrin. "Home broadband adoption, computer ownership vary by race, ethnicity in the U.S." *Pew Research Center*. (July 16, 2021). https://www.pewresearch.org/fact-tank/2021/07/16/home-broadband-adoption-computer-ownership-vary-by-race-ethnicity-in-the-u-s/.

[37] Kelley, Jason. "Bar Applicants Deserve Better than a Remotely Proctored 'Barpocalypse.'" *Electronic Frontier Foundation*. (Oct. 9, 2020). https://www.eff.org/deeplinks/2020/10/bar-applicants-deserve-better-proctored-barpocalypse

[38] Johnson, Kari. "ExamSoft's remote bar exam sparks privacy and facial recognition concerns." *VentureBeat*. (Sept. 29, 2020). https://venturebeat.com/2020/09/29/examsofts-remote-bar-exam-sparks-privacy-and-facial-recognition-concerns/.

[39] Brown, Lydia X. Z. "How Automated Test Proctoring Software Discriminates Against Disabled Students." *Center for Democracy & Technology*. (November 16, 2020) https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/.

[40] *Id.*

who are already more likely to face punishment in school, are especially vulnerable to long-lasting negative effects of increased monitoring.[41]

Rarely are there alternatives that allow students or unemployed people to opt-out of these mainstream processes and avoid the coercive effects of technology. These are systemic harms that require systemic interventions, but it's often difficult for individuals who encounter harms to show broader discriminatory patterns. It's necessary for regulators and enforcement agencies to play a stronger and more active role to assess whether technologies are exacerbating existing inequities in key areas of justice and opportunity. One way to do this is by using demographic data to measure and audit systems for disparate impact. These are long-standing civil rights enforcement measures that can also be used to assess the impact of new technologies.

Conclusion

These are urgent issues that the Biden administration must address. In July 2021, Upturn wrote a letter to the Office of Science and Technology Policy (OSTP), together with 26 other groups, urging OSTP to work across the federal government to "identify how technology can drive racial inequities, and help agencies devise new policies, regulations, enforcement activities, and guidance that address these barriers."[42] Attached to the letter were three memos sent to federal agencies outlining concrete recommendations to address technology's role in housing,[43] hiring,[44] and financial services[45] discrimination. While some progress has been made at the agency level, much more remains to be done. OSTP must work to support the administration in developing a proactive and coordinated policy agenda to tackle these challenges.

Thank you for considering these comments. We welcome further conversations on these important issues. If you have any questions, please contact Emily Paul (Project Director, [redacted]) and Harlan Yu (Executive Director, [redacted]).

---

[41] *See, e.g.* Del Toro, Juan and Ming-Te Wang. "The Roles of Suspensions for Minor Infractions and School Climate in Predicting Academic Performance Among Adolescents." *American Psychologist*. (Oct 2021). https://www.apa.org/news/press/releases/2021/10/black-students-harsh-discipline.
[42] "Centering Civil Rights in Artificial Intelligence and Technology Policy." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technologys-role-in.
[43] "Addressing Technology's Role in Housing Discrimination." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technologys-role-in-hiring.
[44] "Addressing Technology's Role in Hiring Discrimination." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technology-housing.
[45] "Addressing Technology's Role in Financial Services Discrimination." (July 13, 2021). https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technologys-financial.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

US Technology Policy
Committee of the Association of
Computing Machinery

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 13, 2022

Dr. Eric S. Lander, Director
Office of Science and Technology Policy
1650 Pennsylvania Avenue, NW
Washington, DC 20502

Re: Request for Information on Public and Private Sector Uses of Biometric Technologies (Document Number: 2021-21975)

Dear Dr. Lander:

The non-profit Association for Computing Machinery (ACM), with more than 50,000 U.S. members and approximately 100,000 worldwide, is the world's largest educational and scientific computing society. ACM's US Technology Policy Committee (USTPC), currently comprising more than 150 members, serves as the focal point for ACM's interaction with all branches of the US government, the computing community, and the public on policy matters related to information technology. As such, the Committee strives to serve as an apolitical source of expert information.

USTPC commends OSTP for its inquiry in the above-captioned proceeding and concurs that the specific inquiries it poses are critical to the development of comprehensive and coherent federal policy with respect to all aspects and applications of biometric technologies. USTPC wishes at this time, however, to underscore the urgent need to develop widely supported uniform norms and practices for the development and deployment of AI-assisted facial recognition technologies. To that end, and in the hopes that it will prove useful in this proceeding, we are pleased to attach for OSTP's consideration USTPC's June 2020 Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies.

We look forward to contributing to the work of the present proceeding in the future and stand ready to assist you with it, and the development of facial recognition policy, as may be most useful to your Office. To access the expertise of ACM's members, please contact our Director of Global Policy and Public Affairs, Adam Eisgrau, at [redacted].

Sincerely,

[redacted]

Alec Yasinsac, Vice Chair

ACM U.S. Technology Policy Committee
1701 Pennsylvania Avenue, NW Suite 200
Washington, DC 20006

[redacted]
www.acm.org/public-policy/ustpc

June 30, 2020

STATEMENT ON PRINCIPLES AND PREREQUISITES FOR THE DEVELOPMENT, EVALUATION AND USE OF UNBIASED FACIAL RECOGNITION TECHNOLOGIES

The ACM U.S. Technology Policy Committee (USTPC) has assessed the present state of facial recognition (FR) technology as applied by government and the private sector. The Committee concludes that, when rigorously evaluated, the technology too often produces results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems. The consequences of such bias, USTPC notes, frequently can and do extend well beyond inconvenience to profound injury, particularly to the lives, livelihoods and fundamental rights of individuals in specific demographic groups, including some of the most vulnerable populations in our society.

Such bias and its effects are scientifically and socially unacceptable.

For both technical and ethical[1] reasons – pending the adoption of appropriately comprehensive law and regulation to govern its use, oversee its application, and mitigate potential harm – ***USTPC urges an immediate suspension of the current and future private and governmental use of FR technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights***.

Specifically, USTPC finds that:

- Though powerful today and likely to improve in the future, FR technology is not sufficiently mature and reliable to be safely and fairly utilized without appropriate safeguards against adversely impacting individuals, particularly those in vulnerable populations;

- Their potential to help meet significant societal needs, as well as political and marketplace forces, have driven the adoption of FR systems by government and industry ahead of the development of principles and regulations to reliably assure their consistently appropriate and non-prejudicial use;

[1] The Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct counsels computing professionals to avoid harm, be cognizant of the public good, and thoroughly evaluate the impacts and risks of computing systems before deploying them. While written for ACM members and other computing professionals, these core precepts of the Code also may be employed by policy makers assessing how to effectively regulate the development and use of facial recognition technologies.

ACM U.S. Technology Policy Committee
1701 Pennsylvania Avenue, N.W. #200
Washington, D.C. 20006

[redacted]
www.acm.org/public-policy/ustpc

- While FR technology can be benign or beneficial in its application, its use has often compromised fundamental human and legal rights of individuals to privacy, employment, justice and personal liberty;

- Policy makers should thus immediately enjoin the use of FR technology by corporations and governments pending the creation and adoption of legal standards for its accuracy proportional to the potential harm such systems may cause to misidentified or non-identified individuals;

- Universal principles for the accurate and just use of FR technology, and for its principled regulation, must be developed without delay; and

- Relevant standards and regulations must address the accuracy, transparency, governance, risk management, and accountability of FR systems.

To these ends, USTPC offers the following guiding principles:[2]

ACCURACY[3]

- Before an FR system is used to make or support decisions that can seriously adversely affect the human and legal rights of individuals, the magnitude and effects of such system's initial and dynamic biases and inaccuracies must be fully understood.

- As the impact of each type of error is context dependent, context must be expressly identified and addressed in standards that set legally "acceptable" error rates.

- When error rates are reported, they must be disaggregated by sex, race, and other context-dependent demographic features, as appropriate.

- The accuracy of every FR system must be fully auditable over time to support third party monitoring and robust government oversight.

---

[2] Primary contributors to this Statement and its constituent principles were USTPC Chair Jim Hendler, Vice Chair Alec Yasinsac, and Committee members Ricardo Baeza-Yates, Jeremy Epstein, Simson Garfinkel, Arnon Rosenthal, and Stuart Shapiro.

[3] The Committee also urges that practices, policies, rules and statutes governing the development and deployment of all FR technology be consistent with its *Statement on Algorithmic Transparency and Accountability* and *Statement on the Importance of Preserving Personal Privacy*. The former highlights the need to understand the consequences of software errors. (In particular, it warns of potential biases in training data and resulting potentially discriminatory harms.) The latter underscores the importance of ensuring appropriate data quality, particularly its accuracy.

TRANSPARENCY

- An FR system should be activated only after some form of meaningful advance public notice of the intention to deploy it is provided and, once activated, ongoing public notice that it is in use should be provided at the point of use or online, as practicable and contextually appropriate.

- Such notices should at minimum contain:

  - A description of the data used to develop and train the FR algorithm;

  - Sufficient detail about the algorithm's implementation so that experts can understand its performance characteristics, accuracy, and limitations;

  - A report of the algorithm's performance relative to a standardized benchmark; and

  - A clear statement of:

    - How the algorithm will be used (including particularly its role in any decisions affecting individuals and whether those decisions are to be taken automatically or by a human supported by the FR technology); and

    - The role that humans will play in application of the system.

GOVERNANCE

- No FR system should be deployed prior to establishing appropriate policies governing its use and the management of data collected by the system.

- All such policies, to the maximum extent possible, should be subject to public input, scrutiny, and oversight.

- Data retention policies and practices should be legally compliant, transparent to the public, and limit data retention to what is strictly necessary for the specific purpose for which the data was collected.

- Systems should be designed to minimize the quantity and richness of any data retained.

- FR system governance mechanisms should pay particular attention to the risks posed to, and consequently necessary protections for, vulnerable individuals and populations; the more significant the potential harm, the stricter risk management protocols should be.

RISK MANAGEMENT

- The benefits of deploying a given FR system to the deploying organization, the public, and to vulnerable subgroups should be proportional to the risks posed by its use.

- Key risks to consider must include those related to security, privacy, and safety in general, as well as to the potential for negative and discriminatory practical, legal and public policy impacts on protected and vulnerable populations.

- Organizations that use FR should empower and enable an appropriately constituted advisory board, similar to a Civilian Oversight Board or an academic Institutional Review Board, to assess whether a proposed FR system can be employed ethically before approving or deploying it for a particular proposed use.

- Such reviews should include a proactive, multi-factor impact assessment and risk analysis.

- No FR system should be made available or deployed unless its relevant material risks to vulnerable populations, or to society as a whole, can be sufficiently eliminated or remediated.

ACCOUNTABILITY

- Developers, operators, and users of any FR system must be accountable within their organization and to external stakeholders for the consequences of such systems' use and misapplication.

- When harm results from the use of such systems, the organization, institution, or agency responsible for its deployment must be fully accountable under law for all resulting external risks and harms.

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Virginia Puccio

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

From: [redacted]
To: MBX OSTP BiometricRFI
Subject: [EXTERNAL] RFI Response: Biometric Technologies
Date: Monday, December 13, 2021 7:54:30 PM

Hello,

I support regulations to help AI maximize benefit and minimize harm, and the president's endorsement is an important step. That said, I wonder: Would an Electricity Bill of Rights have made sense 100 years ago? I urge regulators to focus not on AI as a whole but on applications in vertical areas such as surveillance, advertising, consumer software, health care, law enforcement, social media, and many other areas.

Thank you for your consideration.

Best regards,
Virginia Puccio

--
Virginia Puccio
[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

Visar Berisha and Julie Liss

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

Speech and language analytics for assessment of human health

RFI Respondents:

Visar Berisha, PhD
Associate Professor
Arizona State University (Academic Institution)

Julie Liss, PhD
Professor and Associate Dean
Arizona State University (Academic Institution)

I. Introduction

Speaking is a deceptively complicated activity. We must think of the words to convey our message, organize the words in compliance with the rules of our language, and activate the muscles that allow us to produce intelligible speech. This process requires coordination across multiple regions of the brain and precise activation of more than 100 muscles. If there is a disturbance to any of these regions of the brain or the physical apparatus itself, it becomes apparent in the resulting speech. *What we say* and *how we say* it is actually a window into our health.

The potential for extracting clinically-rich information from such an easy-to-acquire signal has generated considerable excitement in the digital health and wellness communities, and speech has been referred to as the newest *vital sign* [1]. The promise is that any neurological, mental health, or physical disturbances that impact the speech production process can be passively detected from patients' speech patterns. To that end, there has been significant interest in different academic communities and in industry in developing artificial intelligence (AI) models for diagnosis, prognosis, and tracking of different clinical conditions using only speech (e.g. see [2], [3] for mental health, [4], [5] for cognition, [6] for motor disease, [7] for emotion recognition, etc.).

The potential of this technology is undeniable, however these models are not yet ready for prime time. An easy-to-access vital sign that provides signal across multiple conditions has the potential to extend clinical reach into underserved rural communities [8], speed up diagnosis in conditions where early intervention can be beneficial [9], and expand participation in clinical research [10]. However, there is a gap between the potential of the technology and the current reality. Our work has shown that reported accuracy results from published clinical AI models in speech are overoptimistic and that these models would likely not fare well if they were to be deployed [11]. Furthermore, published clinical AI models are heavily biased demographically, with 71% of the training data coming from only three states in the US: California, Massachusetts, and New York [12]. This biased sampling is likely to leave a massive blind spot in the models that would not be obvious until after deployment [11].

In addition to the performance of these AI models, there are important security and privacy risks. Every time we email, make a call, write a Facebook message, post a YouTube video, or record a Snap on Snapchat, we are providing indirect evidence of our health. By one estimate, people spend an average of four hours per day on their smartphones [13]. This data can be accessed by providers of this technology and there exists a risk of them gleaning personal health information (PHI) about their users without their user's consent. Or the data exists in the public domain and can be used by anyone for the same purpose. We have demonstrated that it's possible to do this by analyzing speech available online for several public figures: Ronald Reagan prior to his Alzheimer's diagnosis [14], Muhammad Ali prior to his Parkinsonism diagnosis [15], and players in the National Football League to assess cognitive-linguistic changes [16].

In this RFI response we aim to provide a realistic overview of the potential of clinical speech analytics, the risks associated with this technology - both due to inaccurate validation of models and security risks, and a path for moving forward responsibly with these methods. To that end, we provide a response to the following areas of interest:

- **Descriptions of use of biometric information for recognition and inference:** an explanation of what types of clinical information can be gleaned from the speech signal and current approaches to this problem.
- **Procedures for and results of data-driven and scientific validation of biometric technologies:** an explanation of some of the pitfalls of the current methods for validating speech-based clinical AI tools and an overview of a thorough framework for validation.
- **Exhibited and potential benefits of a particular biometric technology:** a discussion of the benefits of speech-based assessments in clinical research and in clinical applications.
- **Security considerations associated with a particular biometric technology; and exhibited and potential harms of a particular biometric technology:** an overview of the risks of clinical speech analytics due to inaccurate validation of models and privacy concerns.

We are uniquely qualified to provide a response to this RFI. Berisha and Liss have collaborated for over 10 years on clinical speech-based AI models. Berisha's background[1] is in artificial intelligence applied to healthcare, with contributions to fundamental AI theory and applications to clinical speech analytics. Liss' background[2] is in speech neuroscience, with contributions in clinical speech science spanning multiple neurological conditions. Since the inception of their collaboration, their work has been funded by the National Institutes of Health, the National Science Foundation, the Office of Naval Research, the Department of Defense, industry partners, and foundations. In addition, they have founded a company[3] together and have first-hand experience of the challenges associated with translating clinical AI models to practice.

II. Descriptions of use of biometric information for recognition and inference

In this section we provide an overview of the utility of speech as a vital sign - a marker of human health across several different conditions. We first describe the complexities of the human speech production process. Then we overview the types of clinical information that can be gleaned from speech. Finally, we describe the two current approaches to clinical speech analytics.

1. The human speech production mechanism and its complexities

The production of spoken language is a complex, multi-stage process that involves high levels of memory, cognition, and sensorimotor function. The three distinct stages are [17]:

1) *Conceptualization*: formation of abstract ideas about the message to be communicated
2) *Formulation*: forming the exact linguistic construction of the utterance to be spoken
3) *Articulation*: producing words via synergistic movement of the speech production system, *i.e.* lungs, glottis, larynx, vocal tract, *etc*.

These stages are visually represented in the block diagram in Figure 1, and the figure legend explains the stages in more detail for the interested reader.

Clinical conditions may affect any of these stages, but broadly, they can be captured through analysis of "content" (*what is said*) and "form" (*how it is said*). Indeed, the tools used to characterize content and form of speech are agnostic to the underlying condition. It is the constellation of speech characteristics and abnormalities that point to the underlying condition. For example, speech that lacks coherence of ideas and jumps from topic to topic (impaired content), and is produced very rapidly and without pauses (impaired form), would point toward a thought or mood disorder, such as schizophrenia or mania. A person with dementia may present with restricted vocabulary size (impaired content), and frequent lengthy pauses (impaired form).

[1] https://scholar.google.com/citations?user=MQBn718AAAAJ&hl=en
[2] https://scholar.google.com/citations?user=z6uGtv4AAAAJ&hl=en
[3] http://www.auralanalytics.com

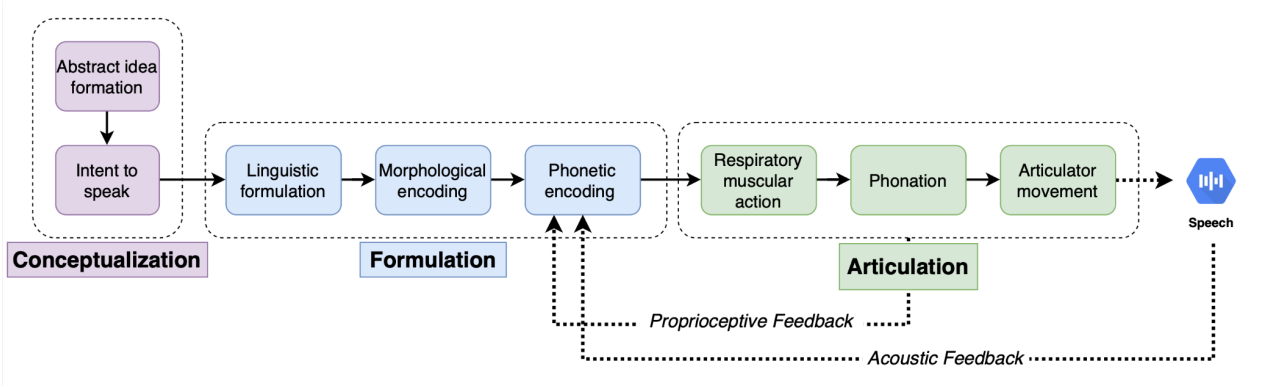


Figure 1: A high-level overview of the three-stage speech production process. During the *Conceptualization* stage, the speaker has an abstract idea that they want to verbalize (*Abstract idea formulation*) and the intention to share through speech (*Intent to speak*). During the *Formulation* stage, they select the words that best convey their idea and sequence them in an order allowed by the language (*Linguistic formulation*). Then they plan the sequence of phonemes and the prosodic pattern of the speech to be produced (*Morphological encoding*). Next, they program a sequence of neuromuscular commands to move speech structures (*Phonetic encoding*). Finally, these commands are executed to produce speech (*Articulation* stage). During this stage, respiratory muscles produce a column of air that drives the vocal folds (*Phonation*) to produce sound. This sound is shaped by the *Articulator movements* to produce speech. Two feedback loops (*Acoustic feedback* and *Proprioceptive feedback*) refine the neuromuscular commands produced during the *Phonetic encoding* stage over time. Adapted from Levelt (1989) [17].

2. What clinical information can be gleaned from speech and language?

Spoken language contains measurable dimensions that provide insight into various aspects of health. These include movement disorders (*e.g.* Parkinson's disease, amyotrophic lateral sclerosis (ALS), Huntington's disease); cognitive impairments (*e.g.* MCI, dementia, Parkinson's disease, AD, chronic traumatic encephalopathy (CTE)); mental health conditions (*e.g.* schizophrenia, depression, bipolar disorder); and respiratory conditions (e.g. COVID, asthma, COPD, etc.).

A large body of work in clinical speech analytics is based on textual language analysis, either by manual or automatic transcription of speech. For example, consider the "*Linguistic formulation*" area within the formulation stage in Fig. 1. Neurological thought disorders affect one's ability to form complex thoughts and sentence structures, and may manifest as poverty of speech or disorganized speech. Therefore, we examine thought content density, complexity of sentence syntax, semantic coherence, and sentiment analysis as they relate to these conditions.

Analysis of acoustic speech content provides additional insight for characterizing the health state of an individual, as impairments can affect *how* speech is produced. For example, speaking depends upon the cognitive capacity to conceptualize and formulate stages of speech production. Cognitive disorders can result in abnormalities in motor coordination and reduced proprioceptive feedback that impacts speech acoustics [18]. Acoustic features that capture temporal characteristics and prosody (*e.g.* pause rate, phonation rate, periodicity of speech, *etc.*) and those related to frequency analysis (*e.g.* mel-spectral coefficients) contain complex information about the cognitive state of the individual. For other conditions, such as respiratory system involvement, the impact on speech acoustics is simpler to characterize. A patient with reduced breath support will pause frequently to catch their breath in between words [19]. Table 1 provides examples of speech symptoms present in different types of conditions.

	Content - "*what is said*" *Natural Language Processing*	**Form - "*how it is said*"** *Acoustic Analysis*
Motor disorders (e.g. Parkinson's, ALS, Huntington's)	Reduced speech output, reduced volition to participate in conversation	Slurred, slow speech, atypical rhythm, reduced prosodic variation, poor phonation quality
Cognitive disorders (e.g. Alzheimer's, FTD)	Low lexical complexity, simple syntax, simple vocabulary,	Long pause length between words, slow speech
Mental health conditions (e.g. depression, schizophrenia, bipolar)	Reduced speech output, incoherent speech, atypical sentence structure	Atypical prosody, increased pause rate
Respiratory conditions (e.g. COVID, asthma, COPD, etc.)	Short sentences	Frequent breaths, increased pause rate

Table 1: A high-level overview of the speech symptoms present in different types of conditions. Clinical analytics that characterize *Content* typically rely on natural language processing after transcription of the words spoken by the patient. Clinical analytics that characterize *Form* typically analyze the raw acoustic signal.

3. How have speech and language been used in clinical applications?

Broadly speaking, there exist two approaches to clinical speech analytics. The first approach, which we call *model-driven*, relies on developing and validating analytical tools to automatically measure clinically-relevant speech symptoms, some of which are listed in Table 1. The second approach, which we call *data-driven*, uses existing AI processing pipelines to develop diagnostic models for different diseases based on speech. To date, the second set of approaches have dominated the scientific literature on this topic. We provide a brief overview of both approaches.

Model-driven clinical speech analytics: The first approach to clinical speech analytics involves the automation of existing tools for automatically and reliably measuring clinically-relevant parameters from speech. There is a long and rich history in speech neuroscience and clinical speech science analyzing the relationship between different health conditions and the speech signal [20]. Until recently, this work required manual analysis (by listening) and annotation of speech from individuals with different disorders. Model-driven approaches aim to develop algorithms that codify this know-how in algorithms for analyzing speech. In the review in [18], we provide an overview of clinically-relevant features that can be extracted for cognitive and mental health conditions and we describe how these features map on the framework in Fig. 1.

One of the perceived "limitations" of this approach is that it provides a measurement of speech symptoms and not a binary speech-only diagnostic decision. We view this as a strength and not a limitation as the constellation of measured symptoms must be considered within a broader context (that may include other data) by clinicians or AI algorithms. Reliable assessment of the domains shown in Fig. 1 is likely to improve the accuracy of downstream diagnostic decisions.

Data-driven clinical speech analytics: The second set of approaches are data-driven and aim to use the speech signal to automatically diagnose patients. In contrast to the relatively small body of work focusing on model-driven clinical speech analytics, the data-driven literature is abundant. These approaches use labeled clinical datasets to learn a relationship between characteristics of the speech signal and a given condition. For example, using speech to diagnose patients with cognitive impairment or Alzheimer's disease [9]; using speech to diagnose patients with mental health conditions [2], [21]; or using speech to diagnose patients with COVID-19 [22]. Speech is a data-rich signal sampled at tens of thousands of times per second. To wrangle with this volume of data for clinical AI applications, algorithm designers that adopt this approach transform the raw speech

samples into high-dimensional feature vectors that range from hundreds to thousands of features; the expectation is that these features contain the complex information relevant for clinical diagnoses. However, clinical speech databases are quite small in comparison to the large feature sets, often on the order of tens or hundreds of patients with only a few minutes of speech per person [11]. This leads to considerable problems as we will discuss in section III.1.

III. Procedures for and results of data-driven and scientific validation of biometric technologies

The abundant optimism surrounding biometrics in the academic literature is at odds with the real-world performance of these models once deployed in-clinic. There are several notable examples of models with impressive reported accuracy results that fail when deployed in clinical settings [23], [24]. We posit that this is due to incomplete validation of these tools in the academic literature. In this section, we provide evidence of the limitations of current approaches to clinical validation and describe a more thorough approach, focusing on clinical speech analytics.

1. Limitations of current approaches to clinical model validation

As we described, most published methods are data-driven. In two recent papers [11], [25], we highlight several significant limitations with the validation of these approaches. Below we provide an overview of some of these issues and refer the reader to [25] for an in-depth discussion on validation of features and to [11] for an in-depth discussion on validation of models.

Feature validation: Working with the raw speech signal can be challenging as it's a high-volume data stream (sampled at thousands of times per second). To make the problem easier, algorithm designers typically transform the raw signal into high-dimensional feature vectors (ranging from hundreds to thousands of features per sample). The expectation is that there is clinically-relevant information within the measured feature set.

In most published work in this space, the features used to drive AI data-driven models are derived from open source speech analysis packages that have been developed for other purposes (*e.g.* automatic speech recognition). As such, these features have not been subjected to the validation rigor typically required for clinical applications. To develop reliable clinical models using speech, it is important to distinguish natural variation in speech production from disease-related change in the measures of interest. An individual undergoing repeated measurements will show natural variation such that the scores vary across different days (and even within the same day). When the natural variation is large, it becomes difficult to detect when there is an important disease-related change. For example, in Parkinson disease, weakness of muscles used in speaking causes a decrease in loudness; however, many factors unrelated to Parkinson disease can also impact day-to-day speaking loudness. The more loudness variation is exhibited by healthy individuals, the harder it becomes to detect a true loudness decline due to Parkinson disease progression. Even in cross-sectional studies, high-variance features combined with small sample sizes increase the risk of overfitting to a dataset. Therefore, it is important to understand the typical natural variation of speech features if speech is to be used as a biomarker. In our work in [25], we studied the repeatability of several thousand speech features most commonly used in clinical speech applications. The results indicated that the average test-retest reliability across all features is 0.35. This is considered very low for clinical applications [26].

AI Model validation: While the number of features in clinical speech models can be very high, clinical speech databases are quite small in comparison - often on the order of tens or hundreds of patients with only a few minutes of speech per person [11]. High-dimensional data combined with a relatively small sample size used to model a very complex phenomenon (human health) can lead to overfit models with overoptimistic estimates of accuracy.

We studied whether there was evidence of this in the existing literature in a recent publication [11]. When building clinical-AI models, one would expect that as additional training data is added to a properly-trained model, the accuracy of the model should either remain the same or improve. That is, AI models are expected to *learn from data*. However, we found exactly the opposite trend in published models. In Fig. 2, we characterize the relationship between accuracy and sample size for speech-based classification models of cognitive impairment from 55 studies published in the literature. It is common practice in the speech analytics literature to extract hundreds or thousands of features from speech samples elicited under different conditions to learn models for classifying between a control group and an impaired group. We plot the reported accuracy vs. total sample size for 51 classifiers from the literature, considering two types of models: (1) speech-based models for classifying between a control group (Con) and patients with a diagnosis of Alzheimer's disease (AD) and (2) speech-based models for classifying between a control group and patients with other forms of cognitive impairment (CI). As the figure shows, there is an unexpected negative association between sample size and reported accuracy. This same trend appears with other data modalities (*e.g.* neuroimaging, eye tracking) in studies involving several neurological disorders, including schizophrenia, MCI, Alzheimer's disease, major depressive disorder, autism spectrum disorder, and attention deficit hyper-activity disorder [27], [28].

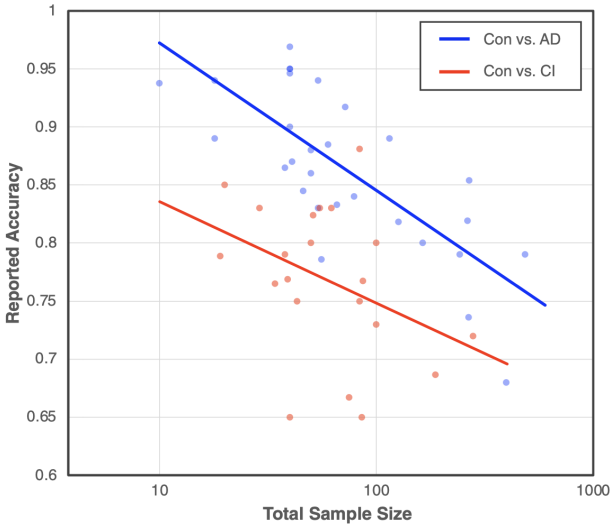


Figure 2: The negative relationship between sample size and reported accuracy as evidence of overoptimistic models in the literature. This analysis considers two types of models: (1) speech-based models for classifying between a control group and patients with a diagnosis of Alzheimer's disease (Con vs. AD; blue plot) and (2) speech-based models for classifying between a control group and patients with other forms of cognitive impairment (Con vs. CI; red plot). The total sample size is the sum of the number of subjects in the control group and the clinical group. The y-axis is in linear scale and the x-axis is in log scale as it spans multiple orders of magnitude. From Berisha et al (2020) [11].

As we noted in [11], this negative trend may result from overfitting during model development by repeatedly using the same training and test set, or they are the result of the so-called file drawer effect seen in other research areas [29]. Either way, there is converging evidence of overoptimism in the reported accuracy results in clinical AI studies and these results should be viewed with caution.

2. A framework for thorough validation of speech-based biomarkers

The gold standard validation procedure for any analytical tool, be it model-driven or data-driven, is a prospective study that demonstrates **V**erification of hardware, analytical **V**alidation, and clinical **V**alidation (V3). The V3 framework [30], introduced in 2020, provides a framework for thorough validation of biometric monitoring technologies. We interpret the three stages of the V3 framework for speech-based digital biometrics as follows:

- **Verification** evaluates the fidelity of the raw sample data produced by the sensor technology used to acquire it in the environment in which it is to be used. For speech, this could include

evaluation of the microphones used to acquire the data and the environmental conditions that ensure the collected samples are of sufficient fidelity for downstream processing.

- **Analytical validation** evaluates the performance of the algorithms that process the raw sensor data to produce physiological or behavioral metrics. For speech, this requires validation of individual features automatically estimated from the raw speech samples. Implicit in this step is the requirement that features extracted from speech be interpretable and reliably measurable using other means. Examples of interpretable features that can be manually validated include speaking rate (calculated manually), articulatory precision (rated perceptually by speech language pathologists), semantic relevance (scored manually), etc.
- **Clinical validation** demonstrates that models track with a quantifiable clinically-relevant ground truth or a clinically accepted measure. For speech, this means evaluating whether the features that are analytically validated - or some combination of them via statistical modeling - track with an acceptable clinical ground truth. Depending on the application, this may require separate cross-sectional and longitudinal validation studies.

3. Validation results: Speech-based assessment of cognition, motor control, and respiration

We have applied the V3 approach to several speech-based models for assessment of cognition, motor control, and respiration. Below we describe sample results from three relevant publications [5], [31], [32].

Speech-based assessment of cognition: In [5][4], we developed and evaluated an automatically extracted measure of cognition (semantic relevance) using automated and manual transcripts of audio recordings from healthy and cognitively impaired participants describing the Cookie Theft picture from the Boston Diagnostic Aphasia Examination. We developed the measure on one dataset and evaluated it on an external database (over 2000 picture descriptions) by comparing accuracy against a manually calculated metric (Analytical Validation) and evaluating its clinical relevance (Clinical Validation). Prior to validating the measure, we verified that the hardware used to acquire the data provided speech samples of sufficient quality for accurate transcription for speech samples collected with supervision in-clinic and independently at-home (Verification).

The fully-automated measure was accurate (r = .84), had moderate to good reliability (ICC = .73), correlated with Mini Mental State Exam (MMSE) and improved the fit in the context of other automatic language features (r = .65), and longitudinally declined with age and level of cognitive impairment. To our knowledge, this is the largest speech-based study conducted in dementia.

Speech-based assessment of motor control: In a recent paper [31], using a cohort of N = 65 patients diagnosed with amyotrophic lateral sclerosis (ALS), we demonstrated that it is possible to remotely detect early motor speech changes and track motor speech symptom progression in ALS via automated algorithmic assessment of speech. We assessed two speech features - articulatory precision and speaking rate - that change as a result of imprecise speech motor secondary to bulbar deterioration in ALS. We first established the analytical validity of both features by comparison against clinical labels obtained from a speech language pathologist. Next we established the clinical validity of the features by comparing against the clinical standard in ALS. Prior to validating the features, we verified that the hardware used to acquire the data provided speech samples of sufficient quality for accurate feature estimation.

Speech-based assessment of respiratory function: In the paper in [32], we present and provide validation data for a tool that predicts forced vital capacity (FVC) from speech acoustics collected remotely via a mobile app without the need for any additional equipment (e.g. a spirometer). We

[4] This paper is in press and not currently publicly available. We have provided a current draft of the manuscript as supplementary material.

trained a machine learning model on a sample of healthy participants and participants with reduced respiratory function to learn a mapping from speech acoustics to FVC and used this model to predict FVC values in an external sample from a different study of participants. To elicit the speech, we asked each participant to take a deep breath and say “ahhhh” for as long as possible until they run out of breath - this is called a sustained phonation task.

Prior to building the model, we verified that the microphone types used to acquire the data did not impact data quality for assessing sustained phonations (Verification). We validated that the features used to drive the model were correctly extracted by comparing against manually-tagged features (Analytical Validation). Finally, we evaluated the cross-sectional accuracy of the model and its sensitivity to within-subject change in FVC (Clinical Validation). We found that the predicted and observed FVC values in the test sample had a correlation coefficient of .80, that the model was able to detect longitudinal decline in FVC, and that it was highly repeatable.

IV. Exhibited and potential benefits of a particular biometric technology

Mobile technology has changed the way we communicate and it will change the way we monitor our health and well-being. Speech-based assessment tools will play an important role in this new ecosystem and have the potential to provide benefits both in clinical research and in-clinic. One can argue that existing speech-based solutions (e.g. a phone call/Zoom call with a provider) have already helped improve connectivity between patients and clinicians; however, in this section our aim is to provide an overview of the benefits of *automated speech-based biomarkers* and not existing speech technologies for better transcription or improved connectivity.

1. Benefits of speech-based digital health tools in clinical research

Most clinical trials are very burdensome for participating patients and costly for the sponsor. To determine whether an intervention is effective, patients must be evaluated several times during a trial. This is typically done in-clinic with long and exhaustive test batteries and requires intensive training of clinicians to ensure reliable measurement of outcomes. This is especially problematic in conditions (*e.g.* neurodegenerative disorders) where patients may have ambulatory constraints.

- **Reduced clinical trial costs by decreasing sample sizes:** Our previous work [10] and the work of others [33] has demonstrated that digital tools, including those that assess speech, are more sensitive to changes in patients’ health and can help reduce the size and cost of clinical trials through shorter trials or trials with smaller sample sizes.
.
- **Reduced patient burden through simple remote monitoring solutions**: In contrast to existing clinical assessment tools, speech-based assessments can be administered very efficiently. For example, in Alzheimer’s disease clinical trials, existing neuropsychological tests can take hours to administer. The speech-based assessments take anywhere between 1 to 2 minutes. For example, for the results highlighted in the previous section (Assessment of cognition), the picture description task used to elicit speech requires only 90 seconds to administer and can be done remotely without the need to bring patients in-clinic.
.
- **Improve diversity in clinical trials**: There is a well-documented need for increased patient diversity in clinical trials [34]. One of the rate-limiting factors in attracting a more diverse participant pool is the burden and time commitment. Assessments in clinical trials can take all day once the drive time and in-clinic assessment times are taken into account. Proliferation of speech-based digital health outcomes in clinical trials have the potential to increase participation because they remove the need for in-person assessment. This enables patients to participate remotely (without taking time off, without having to make long drives to clinics, etc.)

1. Benefits of speech-based digital health tools for clinical care

Speech-based digital health tools have the potential to provide clinicians with a more complete view of their patient's cognitive, motor, mental, and respiratory health; and the potential to provide patients more control over their own health. All this is done in service of improving outcomes through earlier diagnosis, better prognosis, and better management of chronic conditions. Below we outline some of the potential future benefits of this technology:

- **Reduce inefficiencies:** Speech-based tools have the potential to improve operational inefficiencies (*e.g.* via automatic generation of clinical notes, remote assessment of vital signs), giving the clinician more time to spend with patients [35].
- **Improved access to care:** Speech-based assessments can be administered remotely, thereby increasing clinical reach into rural communities with reduced access to specialized care.
- **Reduce costs:** Speech-based tools that don't require clinical supervision can be administered at a very low cost.
- **Increase quality:** Across many conditions, diagnosis in the early stages is very challenging for clinicians. This is especially true in neurology with misdiagnosis rates of nearly 50% for early stages of Parkinson's disease, and ~30% for Alzheimer's disease [36], [37]. Automated speech-based tools can contribute to AI models for diagnosis and potentially improve on these misdiagnosis rates.
- **Empowering patients:** These tools can be downloaded on patients' personal devices allowing them to track their health and well-being and giving them control over their own data.
- **Make medicine more personalized for patients:** No two patients have exactly the same manifestation of a condition, yet interventions are typically the same for everyone. Speech-based tools can help identify strata for which specific intervention types are more or less effective. One of the very exciting future use-cases is the combination of digital therapeutics with digital speech-based assessments for precision intervention [38].

V. Security considerations associated with a particular biometric technology and exhibited and potential harms of a particular biometric technology

While this technology is promising, there are risks associated with deploying these models prior to sufficient validation and privacy risks related to PHI disclosure. We describe these below.

1. Risks and harms associated with premature deployment of inaccurate models

A primary risk of prematurely-deployed models is that they will provide clinically inaccurate output. As discussed in Section III.1, current strategies to validate AI models are insufficient and produce overoptimistic estimates of accuracy. However, reported accuracy metrics carry much weight when presented to the public - for example, see the press article claiming diagnosis of pre-clinical Alzheimer's disease with up to 75% accuracy using language samples [39]. In many cases, these papers become the foundation for new companies, new investments, or large-scale implementations. There is real risk that these models will fail if deployed and potentially harm patients, as we have already seen in other clinical applications [23], [24].

This problem is compounded by the homogeneity of the data used to train these models. Published clinical AI models are heavily biased demographically, with 71% of the training data coming from only three states: California, Massachusetts, and New York, with 34 of the states not represented at all [12]. It becomes impossible to know how these models would perform on data from demographic groups for which they were not trained.

2. Security and privacy considerations

Speech and language data is widely available and, as we continue to interact with our mobile devices, we generate an ever-growing personal footprint of our health status. This data (emails, voice searches, phone calls, comments, etc.) can be accessed by companies providing the underlying technology to uncover personal health information (PHI) without their users' permission. However, some of this data also exists in the public domain and is accessible to anyone. For example, the speeches of political figures, lectures from instructors and academics, interviews with actors and actresses, etc. can be analyzed by anyone for the purpose of health analytics. Easy access to PHI without permission has obvious deleterious downstream implications.

There are several published use cases from our work that demonstrate this is possible. In a series of three studies, we analyzed publicly-available interviews of public figures for longitudinal changes in cognitive-linguistics. We describe the studies below:

President Ronald Reagan and Alzheimer's Disease: Changes in some lexical features of language have been associated with the onset and progression of Alzheimer's disease. In work from 2014 [14], we described a method to extract key features from discourse transcripts, which we evaluated on non-scripted news conferences from President Ronald Reagan, who was diagnosed with Alzheimer's disease in 1994, and President George Herbert Walker Bush, who had no known diagnosis of Alzheimer's disease. Key word counts associated with cognitive decline were extracted and regression analyses were conducted. President Reagan showed a significant reduction in the number of unique words over time and a significant increase in conversational fillers and non-specific nouns. There was no significant trend in these features for President Bush.

Muhammad Ali and Parkinsonism: In a 2017 paper [15], we use YouTube interviews from Muhammad Ali from 1968 to 1981, before his 1984 diagnosis, to determine whether there were measurable speech changes consistent with parkinsonism. We measured changes in speech from the Ali interviews and analyzed these changes relative to a coded registry of hits he received in each of his boxing matches over time. Multivariate analyses revealed changes in prosody and articulation consistent with hypokinetic dysarthria over time, and a relationship between reduced speech intonation and the amount of time elapsed since the most recent fight preceding the interview.

National Football League (NFL) players and cognitive-linguistic changes: Reduced spoken language complexity is associated with the onset of cognitive disorders. In 2015 [16] we analyzed language complexity in professional football players who are at risk for CTE, using publicly available interview transcripts. We compared these measures with those taken from interview transcripts of coaches and NFL executives who never played professional football. Statistical analysis revealed that exposure to the high-impact sport (vs no exposure) was associated with an overall decline in language complexity scores over time. This trend persists even after controlling for age as a potential confounder.

For the Reagan and Ali studies, the analysis and publication was completed posthumously. For the NFL study, the identities of the players and coaches were kept confidential. A fourth study not described here has not been published based on a request from the public figure.

The risks to privacy of this type of analysis if used outside of academic research is considerable. While none of the studies above used social media platforms, there is evidence that similar analyses can be conducted using data from Facebook, Twitter, Reddit, etc. [40]. We should consider whether there should be bounds on what the companies that provide these services can do with gleaned PHI data. In addition, there can be national and international political ramifications of this type of analysis. Internally, political adversaries can advance a potentially false narrative on the health of candidates. Furthermore, geopolitical adversaries could explore this as an additional dimension of influence in elections.

References:

[1] J. Nosta, "Voice As The New Vital Sign," *Forbes, 2018*. https://www.forbes.com/sites/johnnosta/2018/10/23/voice-as-the-new-vital-sign/ (accessed Jan. 10, 2022).
[2] N. Cummins, S. Scherer, J. Krajewski, S. Schnieder, J. Epps, and T. F. Quatieri, "A review of depression and suicide risk assessment using speech analysis," *Speech Commun.*, vol. 71, pp. 10–49, Jul. 2015, doi: 10.1016/j.specom.2015.03.004.
[3] T. F. Quatieri and N. Malyska, "Vocal-source biomarkers for depression: A link to psychomotor activity," 2012.
[4] K. C. Fraser, J. A. Meltzer, and F. Rudzicz, "Linguistic Features Identify Alzheimer's Disease in Narrative Speech," *J. Alzheimers Dis. JAD*, vol. 49, no. 2, pp. 407–422, 2016, doi: 10.3233/JAD-150520.
[5] Stegmann, Gabriela *et al.*, "Automated Semantic Relevance as an Indicator of Cognitive Decline: Out-of-sample Validation on a Large-Scale Longitudinal Dataset," *Alzheimers Dement.*, 2022.
[6] A. Zhan *et al.*, "Using Smartphones and Machine Learning to Quantify Parkinson Disease Severity: The Mobile Parkinson Disease Score," *JAMA Neurol.*, vol. 75, no. 7, p. 876, Jul. 2018, doi: 10.1001/jamaneurol.2018.0809.
[7] K. Wang, N. An, B. N. Li, Y. Zhang, and L. Li, "Speech Emotion Recognition Using Fourier Parameters," *IEEE Trans. Affect. Comput.*, vol. 6, no. 1, pp. 69–75, Jan. 2015, doi: 10.1109/TAFFC.2015.2392101.
[8] R. F. Mufioz, G. M. Gonzfilez, and J. Starkweather, "Automated Screening for Depression: Toward Culturally and Linguistically Appropriate Uses of Computerized Speech Recognition," *Hisp. J. Behav. Sci.*, vol. 17, no. 2, pp. 194–208, May 1995, doi: 10.1177/07399863950172004.
[9] Filiou et al., "Connected speech assessment in the early detection of Alzheimer's disease and mild cognitive impairment: a scoping review," *Aphasiology*, 2020, Accessed: Jan. 11, 2022. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/02687038.2019.1608502
[10] S. B. Rutkove *et al.*, "Improved ALS clinical trials through frequent at-home self-assessment: a proof of concept study.," *Ann. Clin. Transl. Neurol.*, 2020.
[11] Berisha, Visar, Krantsevich, Chelsea, Hahn, P. Richard, Dasarathy, Gautam, Turaga, Pavan, and Liss, Julie, "Digital medicine and the curse of dimensionality," *Nat. Digit. Med.*, vol. 4, 2021, Accessed: Jan. 10, 2022. [Online]. Available: https://www.nature.com/articles/s41746-021-00521-5
[12] A. Kaushal, R. Altman, and C. Langlotz, "Geographic Distribution of US Cohorts Used to Train Deep Learning Algorithms," *JAMA*, vol. 324, no. 12, pp. 1212–1213, Sep. 2020, doi: 10.1001/jama.2020.12067.
[13] "How Much Time Do People Spend on Their Mobile Phones in 2018?" https://www.textrequest.com/blog/how-much-time-people-spend-mobile-phones-2017/ (accessed Jan. 11, 2022).
[14] V. Berisha, S. Wang, A. LaCross, and J. Liss, "Tracking Discourse Complexity Preceding Alzheimer's Disease Diagnosis: A Case Study Comparing the Press Conferences of Presidents Ronald Reagan and George Herbert Walker Bush," *J. Alzheimers Dis.*, vol. 45, no. 3, pp. 959–963, Mar. 2015, doi: 10.3233/JAD-142763.
[15] V. Berisha, J. Liss, T. Huston, A. Wisler, Y. Jiao, and J. Eig, "Float Like a Butterfly Sting Like a Bee: Changes in Speech Preceded Parkinsonism Diagnosis for Muhammad Ali," in *Interspeech 2017*, Aug. 2017, pp. 1809–1813. doi: 10.21437/Interspeech.2017-25.
[16] V. Berisha, S. Wang, A. LaCross, J. Liss, and P. Garcia-Filion, "Longitudinal changes in linguistic complexity among professional football players," *Brain Lang.*, vol. 169, pp. 57–63, 2017.
[17] W. J. M. Levelt, *Speaking: From intention to articulation*. Cambridge, MA, US: The MIT Press, 1989, pp. xiv, 566.
[18] R. Voleti, J. M. Liss, and V. Berisha, "A Review of Automated Speech and Language Features for Assessment of Cognitive and Thought Disorders," *IEEE J. Sel. Top. Signal Process.*, vol. 14, no. 2, pp. 282–298, Feb. 2020, doi: 10.1109/JSTSP.2019.2952087.
[19] L. Lee et al, "Speech Breathing in Patients with Lung Disease," *Am. Rev. Respir. Dis.*, vol. 147, no. 5, pp. 1199–206, May 1993.
[20] Darley, Frederic, Aronson, Arnold, and Brown, Joe, "Differential Diagnostic Patterns of Dysarthria," *J. Speech Hear. Res.*, pp. 246–269, 1969.
[21] G. Bedi *et al.*, "Automated analysis of free speech predicts psychosis onset in high-risk youths," *Npj Schizophr.*, vol. 1, no. 1, pp. 1–7, Aug. 2015, doi: 10.1038/npjschz.2015.30.
[22] T. Quatieri et al, "A Framework for Biomarkers of COVID-19 Based on Coordination of Speech-Production Subsystems," *IEEE Open J. Eng. Med. Biol.*, pp. 203–206, May 2020.
[23] C. Ross and I. Swetlitz, "IBM's Watson supercomputer recommended 'unsafe and incorrect'cancer treatments, internal documents show," *Stat News Httpswww Statnews Com20180725ibm-Watson-Recomm.-Unsafe-Incorrect-Treat.*, 2018.
[24] Ross, Casey, "Epic's AI algorithms, shielded from scrutiny by a corporate firewall, are delivering inaccurate information on seriously ill patients," *STAT*, Jul. 26, 2021. Accessed: Jan. 11, 2022. [Online]. Available:

https://www.statnews.com/2021/07/26/epic-hospital-algorithms-sepsis-investigation/
[25] G. Stegmann et al., "Repeatability of Commonly Used Speech and Language Features for Clinical Applications," *Digit. Biomark.*, vol. 4, no. 3, 2020, Accessed: Jan. 11, 2022. [Online]. Available: https://www.karger.com/Article/FullText/511671
[26] Portney, Leslie Gross, *Foundations of Clinical Research: Applications to Practice*. F.A. Davis Company, 2015. Accessed: Jan. 11, 2022. [Online]. Available: https://www.fadavis.com/product/physical-therapy-foundations-clinical-research-portney-3
[27] M. R. Arbabshirani, S. Plis, J. Sui, and V. D. Calhoun, "Single subject prediction of brain disorders in neuroimaging: Promises and pitfalls," *NeuroImage*, vol. 145, no. Pt B, pp. 137–165, Jan. 2017, doi: 10.1016/j.neuroimage.2016.02.079.
[28] A. Vabalas et al, "Machine learning algorithm validation with a limited sample size," *PLOS ONE*, Nov. 2019, Accessed: Jan. 11, 2022. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0224365
[29] R. Rosenthal, "The file drawer problem and tolerance for null results," *Psychol. Bull.*, vol. 86, no. 3, pp. 638–641, 1979, doi: 10.1037/0033-2909.86.3.638.
[30] J. C. Goldsack *et al.*, "Verification, analytical validation, and clinical validation (V3): the foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs)," *Npj Digit. Med.*, vol. 3, no. 1, pp. 1–15, Apr. 2020, doi: 10.1038/s41746-020-0260-4.
[31] G. M. Stegmann *et al.*, "Early detection and tracking of bulbar changes in ALS via frequent and remote speech analysis," *NPJ Digit. Med.*, vol. 3, p. 132, 2020, doi: 10.1038/s41746-020-00335-x.
[32] G. M. Stegmann *et al.*, "Estimation of forced vital capacity using speech acoustics in patients with ALS," *Amyotroph. Lateral Scler. Front. Degener.*, vol. 22, no. sup1, pp. 14–21, 2021, doi: 10.1080/21678421.2020.1866013.
[33] H. H. Dodge, J. Zhu, N. C. Mattek, D. Austin, J. Kornfeld, and J. A. Kaye, "Use of High-Frequency In-Home Monitoring Data May Reduce Sample Sizes Needed in Clinical Trials," *PLOS ONE*, vol. 10, no. 9, p. e0138095, Sep. 2015, doi: 10.1371/journal.pone.0138095.
[34] L. T. Clark *et al.*, "Increasing Diversity in Clinical Trials: Overcoming Critical Barriers," *Curr. Probl. Cardiol.*, vol. 44, no. 5, pp. 148–172, May 2019, doi: 10.1016/j.cpcardiol.2018.11.002.
[35] Topol, Eric, *Deep medicine: how artificial intelligence can make healthcare human again*. Hachette UK, 2019.
[36] C. H. Adler *et al.*, "Low clinical diagnostic accuracy of early vs advanced Parkinson disease: clinicopathologic study," *Neurology*, vol. 83, no. 5, pp. 406–412, 2014.
[37] T. K. T. Phung, B. B. Andersen, L. V. Kessing, P. B. Mortensen, and G. Waldemar, "Diagnostic evaluation of dementia in the secondary health care sector," *Dement. Geriatr. Cogn. Disord.*, vol. 27, no. 6, pp. 534–542, 2009.
[38] A. Dang, D. Arora, and P. Rane, "Role of digital therapeutics and the changing future of healthcare," *J. Fam. Med. Prim. Care*, vol. 9, no. 5, pp. 2207–2213, May 2020, doi: 10.4103/jfmpc.jfmpc_105_20.
[39] Kolata, Gina, "Alzheimer's Prediction May Be Found in Writing Tests," *The New York Times*, Feb. 01, 2021.
[40] E. Seabrook et al., "Journal of Medical Internet Research - Predicting Depression From Language-Based Emotion Dynamics: Longitudinal Analysis of Facebook and Twitter Status Updates," *J. Med. Internet Res.*, vol. 20, no. 5, May 2018, Accessed: Jan. 12, 2022. [Online]. Available: https://www.jmir.org/2018/5/e168/

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

XR Association

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

January 15, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Document # 2021-21975; Document Citation 86 FR 56300

Dear Office of Science and Technology Policy:

The XR Association is pleased to submit comments in response to the Office of Science and Technology Policy's Request for Information on Public and Private Sector Uses of Biometric Technologies.

The XR Association (XRA) represents the broad ecosystem of the XR industry including headset manufacturers, technology platforms, component and peripheral companies, internet infrastructure companies, enterprise solution providers, and corporate end-users. The founders of XRA are Google, HTC Vive, Microsoft, Meta Platforms, Inc. (formerly Oculus by Facebook), and Sony Interactive Entertainment. XRA is leading the way for the responsible development and adoption of XR – virtual reality (VR), augmented reality (AR), and mixed reality (MR) – by convening stakeholders, developing research and best practices, and advocating on behalf of our members and the broader XR industry. Our mission is to champion the thoughtful advancement of XR solutions that foster positive societal outcomes.

While immersive experiences have in the past typically been associated with entertainment and gaming, XR technology has come a long way and is now widely considered to be the next major computing platform.[1] Indeed, XR technology is rapidly being adopted across industries as an enterprise solution, particularly as companies look to technology to help them weather and recover from the COVID-19 pandemic.[2] While the technology is still emerging, the importance of biometric data to XR's success cannot be understated, as it ensures users can realize the benefits and experiences made possible by XR. Without biometric data, XR programs will simply not work as designed.

Immersive experiences in XR may utilize a variety of human body characteristics and related data, depending on the platform, program, and intended experience or use case. XR may include sensors for eye-tracking, eye movement detection, and pupil dilation; facial recognition; head position; gait tracking; and sometimes heart rate and skin response, such as sweating. Some of these characteristics are considered biometric technologies in the sense that they may be used for identification, while others are not. The XR industry has been a leader in the advancement of biometric technologies, while also intensely focused on developing measures to ensure the data created in connection with XR technologies is not misused. As XR continues to mature, there is a deep commitment to consult with

[1] "Accelerating the Next Computing Platform," Medium.com, Jan. 28, 2020. https://michaeltefula medium.com/accelerating-the-next-computing-platform-fb3ed88d01e1
[2] "XR-Based Workforce Training Identified As Key Tool In Addressing America's Employment Crisis," XRA Association Survey, Nov. 4, 2021. https://xra.org/xr-workforce-training-addressing-americas-employment-crisis/

[redacted]

various stakeholders and, through consultation and innovation, advance the practice of "privacy by design" to the greatest extent possible.

We believe that, if properly incubated and supported here in the United States, the advantages of biometrics can and will overcome the risks. Indeed, biometric technology promises significant benefits across the board including sophisticated healthcare; navigation assistance; identification efficiency; U.S. defense and public safety advantages; enriched social and educational experiences; and outstanding entertainment, among many others. In the interest of brevity with respect to this comment however, we will focus on workforce training and safety, and the unparalleled benefits provided to the disabled community.

Benefits of XR for People with Disabilities

XR technology offers tremendous benefits to people with disabilities - whether at home, at school, at work, or in social settings. The safe, responsible use of biometric data is essential to ensuring XR can be used by people of all abilities, including people with both cognitive and physical challenges. Some have even suggested that XR can "democratize technology" for people with disabilities by providing them with experiences and interactions that they may be unable to experience in the physical world without the aid of VR, AR, and MR.[3] For example, immersive experiences have allowed people with low vision to see more clearly;[4] given those with mobility challenges the ability to surf or climb mountains;[5] given amputees a more effective way to exercise and strengthen their muscles;[6] and allowed individuals with autism to navigate challenging social situations in a virtual setting, thereby learning new skills and gaining confidence.[7]

XR technology is also being explored for use in pain management as an alternative to opioid prescriptions;[8] in treating mental health disorders, such as post-traumatic stress disorder in U.S. military veterans;[9] in diagnosing and treating people with Alzheimer's disease;[10] and in complimenting traditional therapies for stroke patients and individuals with neurodegenerative diseases.[11]

[3] "What the Future of Virtual Reality Means for Accessibility," Bureau of Internet Accessibility, June 23, 2020. https://www.boia.org/blog/what-the-future-of-virtual-reality-means-for-accessibility
[4] "A Rare Disease Robbed Me Of My Sight. VR Brought It Back," Alex Lee, *Alphr*, March 27, 2018. https://www.alphr.com/virtual-reality/1008932/vr-vision-loss-sight-blindness/
[5] "Affordable Virtual Reality Opens New Worlds For People With Disabilities," Lindsey Hoshow, *NPR*, Oct. 22, 2015. https://www npr.org/sections/health-shots/2015/10/22/450573400/affordable-virtual-reality-opens-new-worlds-for-people-with-disabilities
[6] "VR games open new doors for people with disabilities," Yoon So-Yeon, Korea JoongAng Daily, Dec. 15, 2020. https://koreajoongangdaily.joins.com/2020/12/15/culture/gamesWebtoons/VR-game-recovery/20201215193206600.html
[7] "Virtual Reality Training Improves Social Skills of Individuals on the Autism Spectrum," Center for Brain Health at University of Texas, Sept. 18, 2016. https://centerforbrainhealth.org/article/virtual-reality-training-improves-social-skills-of-individuals-on-the-autis
[8] Virtual Reality for Pain Management in New York: An Alternative to Opioids, Miranda Felde, MHA, CPHRM, Vice President, Patient Safety and Risk Management, the Doctors Company, December 2018. https://www.thedoctors.com/articles/virtual-reality-for-pain-management-in-new-york-an-alternative-to-opioids/#7
[9] Virtual reality exposure therapy for posttraumatic stress disorder: a meta-analysis, European Journal of Psychtraumatology, August 2019. https://www ncbi.nlm nih.gov/pmc/articles/PMC6713125/
[10] Use of Immersive Virtual Reality in the Assessment and Treatment of Alzheimer's Disease: A Systematic Review, Journal of Alzheimer's Disease, April 2020. https://www ncbi nlm nih.gov/pmc/articles/PMC7306888/
[11] Virtual reality-based rehabilitation for recovery of stroke and neurodegenerative disease patients, reviewed by Emily Henderson, B.Sc., News Medical, December 2020, available at https://www news-medical.net/news/20201214/Virtualreality-based-rehabilitation-for-recovery-of-stroke-and-neurodegenerative-disease-patients.aspx

[redacted]

The XR industry has been working with accessibility advocates, industry, and non-profits, such as XR Access, to ensure that as new XR technologies emerge, they are inclusive by design. Working with these partners, the XR Association developed and published a chapter for the XRA Developers Guide entitled "Accessibility & Inclusive Design in Immersive Experiences."[12] The guide offers a set of industry-backed best practices for developing inclusive platforms and software that can provide enhanced experiences for all users. In 2021, the XR Association also collaborated with the Department of Labor's Partnership on Employment & Accessible Technology (PEAT) to draft a white paper entitled "Inclusive XR in the Workplace."[13] The paper details how accessible XR technology can help employers upskill and diversify their workforce with employees with disabilities. The XR industry believes that inclusive XR can help expand job opportunities for people with disabilities, and we have been working diligently toward that goal.

Benefits of XR in the Workplace: Worker Safety and Job Training

The use of XR job training programs has been increasing in recent years. ABI Research predicts that by 2025 upwards of 60 million people will use XR training applications, and that the industries likely to see the greatest adoption of XR training include healthcare, logistics, Architecture, Engineering, and Construction (AEC), and manufacturing.[14] U.S. companies, particularly manufacturers, are quickly becoming reliant on XR technology to increase worker safety, increase productivity, and train employees. With XR applications, inexperienced personnel can be trained in low-risk environments without the need for expensive additional resources. What's more, by digitally simulating production processes, dangerous maneuvers can be identified in advance for even the most experienced individuals. Success stories include Tyson Foods, where 89% of workers said they felt more prepared for their jobs after VR training,[15] and Ford Motor Company, which reduced the injury rate for its more than 50,000 U.S. "industrial athletes" by 70%.[16] Lockheed Martin and Boeing are using XR for space and aircraft manufacturing, and even astronaut training.[17] [18] [19]

Other industries are embracing XR as well. In 2018, construction giant Bechtel announced it was using a variety of XR products to train crane operators and improve the quality of safety procedures on its construction sites.[20] And XR training programs for firefighters are helping to reduce cancer exposure

[12] XRA'S Developers Guide, Chapter Three: Accessibility & Inclusive Design in Immersive Experiences, October 2020. https://xra.org/research/xra-developers-guide-accessibility-and-inclusive-design/
[13] Inclusive XR in the Workplace, PEAT and XRA. https://peatworks.org/pdfs/InclusiveXRWhitePaper_PEATandXRA.pdf
[14]AR Remote Expertise and Training Applications to have Almost 60 Million Active Users by 2025, ABI Research, Oct. 14, 2020. https://www.abiresearch.com/press/ar-remote-expertise-and-training-applications-have-almost-60-million-active-users-2025/
[15] Tyson Foods reduces worker injuries, illnesses with VR safety training, Riia O'Donnell, *HR Dive*, Sept. 18, 2018. https://www hrdive.com/news/tyson-foods-reduces-worker-injuries-illnesses-with-vr-safety-training/532452/
[16] Ford Reduces Production Line Injury Rate By 70 Percent For Its More Than 50,000 'Industrial Athletes,' Ford Motor Company release, July 16, 2015. https://media ford.com/content/fordmedia/fna/us/en/news/2015/07/16/ford-reduces-production-line-injury-rate-by-70-percent html
[17] Lockheed Martin Embraces AR on the Factory Floor, *Assembly* magazine, Aug. 27, 2019. https://www.assemblymag.com/articles/95163-lockheed-martin-embraces-ar-on-the-factory-floor
[18] Boeing Conducts First-Ever Astronaut Training in Virtual Reality using Varjo Headsets, Boeing release, June 11, 2020. https://www.boeing.com/global/boeing-in-europe/news/2020/boeing-conducts-first-ever-astronaut-training-in-vr.page
[19] Boeing Tests Augmented Reality in the Factory, Boeing release, Jan. 19, 2018. https://www.boeing.com/features/2018/01/augmented-reality-01-18.page
[20] Using Extended Reality to Improve Safety on Construction Sites, Bechtel, Nov. 8, 2018. https://www.bechtel.com/blog/innovation/november-2018/using-extended-reality-improve-safety-construction/

and other significant hazards attending live fire trainings by allowing new and veteran firefighters to prepare in safe environments, while learning the skills they need to fight real world fires.[21]

Privacy By Design

In late 2021, the Institute of Electrical and Electronics Engineers (IEEE) published a comprehensive report detailing privacy concerns related to biometric data generated by XR users. As the report notes, biometric data is intrinsic to the functioning of XR technology and the benefits it can provide:

> *This pervasive capture of personal "sensitive" data is unique to XR relative to other consumer technologies, but fundamentally necessary. Such sensing underpins much of the core functionality that makes this technology, and the software that runs on it, so compelling to futurists. It drives the capability to create more usable spatial interactions, enables new applications that better address accessibility needs, and enhances understanding of the user's context, behavior, and needs that drive better AI assistants. For example, an XR headset* without *sophisticated optical sensing would feature greatly degraded performance in all use cases. Many current consumer devices would lose the ability to accurately track its position and orientation in the world, meaning it would be unable to render the exocentric (world-fixed) spatial virtual content that underpins immersive virtual and augmented reality experiences.*[22]

The XR industry places a premium on the need to safeguard sensitive biometric data. Indeed, the industry ideal is the concept of privacy by design, in which XR hardware and applications are engineered with privacy protections in mind from the start. Examples of privacy protections already available on XR platforms include on-device encrypted computing and the ability to opt-in or opt-out of specific data collection features, among other things.

Still, the industry's commitment to privacy by design aims to go even further. It must be recognized, however, that privacy by design involves significant engineering challenges that are not easily solved. As an emerging technology, the XR industry needs the regulatory space to create and experiment in a way that will not stifle innovation as it works toward enhanced privacy protections and other technical features.

The Importance of U.S. Competitiveness in XR

XR is and will continue to be an integral part of the future technology ecosystem. As noted, XR is considered the next major computing platform (predecessors being the personal computer in 1984; the World Wide Web in 1993; and the smart phone in 2007), and the U.S. must be at the forefront of designing and creating it. XR will be the vehicle used for accessing the next iteration of the internet - what is often referred to as "the metaverse," currently. The U.S. Senate recently recognized the impact of XR when it included immersive technologies in its list of "key technology focus areas" to be prioritized for research and development in the United States Innovation and Competition Act of 2021 (S. 1260).

[21] "XR a 'Tool for the 21st Century Firefighter', Execs Say," Demond Cureton, *XR Today*, Aug. 12, 2021. https://www xrtoday.com/mixed-reality/xr-a-tool-for-the-21st-century-firefighter-execs-say/

[22] Extended Reality (XR) and the Erosion of Anonymity and Privacy, IEEE Industry Connections Report, November 2021. https://ieeexplore.ieee.org/document/9619999

[redacted]

U.S. tech luminaries have built ambitious strategies around the development and adoption of XR. Mark Zuckerberg announced his newly renamed company, Meta Platforms, Inc., would be investing $10 billion in AR, VR, and related hardware in 2021 alone, saying during the company's 2021 3rd quarter earnings call that "the metaverse will be a successor to the mobile internet. … It will unlock a massively larger creative economy [...] than what exists today."[23] Microsoft, through its HoloLens hardware and its cross-platform development tools (Azure, Mesh, etc.) has been aggressive in the enterprise space[24]. HTC, Sony, Valve and others are continuing to make significant advancements in hardware and software.[25] And Apple, Google, and Unity have each built substantial AR development platforms in pursuit of democratizing consumer access to AR technologies.

But U.S. companies are not alone in pursuing advances in immersive technology innovations. Foreign powers are rapidly advancing on the U.S.'s historical domination in the field. China recognized the outsized potential of immersive technology years ago and has taken impressive steps towards controlling its future. XR is featured prominently in the CCP's Made in China 2025 strategy, and the Ministry of Industry and Information Technology, the National Development and Reform Commission, the Ministry of Science and Technology, the Ministry of Culture and the Ministry of Commerce have all released detailed strategies concerning XR. In addition, Chinese provincial and municipal local governments are proactively building industrial parks and labs to promote the development of local VR industries.[26]

Harvard University's Belfer Center for Science and International Affairs recently highlighted China as a "full-spectrum peer competitor" to the U.S. in the technology race.[27] And China is not the only nation investing heavily in XR. Countries that had early 5G commercialization strategies, including Japan and South Korea, planned for VR as a key 5G application field. Governments worldwide are generously funding XR research and development, and XR-related inventions are increasing exponentially.[28]

Still, China remains the United States' chief rival in terms of defining the future of technology. China aims to control the technical and ethical standards for those technologies it believes will be both foundational and ubiquitous in the 21st Century,[29] including XR.

In order to ensure that technologies that rely on biometric technology are imbued with U.S. cultural values, we must promote their development here in America where regulations are predominantly

[23]"Facebook's metaverse spending will top $10 billion this year," Janko Roettgers, *Protocol*, Oct. 25, 2021. https://www.protocol.com/bulletins/facebook-metaverse-10-billion-dollars

[24] "With Apple and other rivals in the wings, mixed reality is Microsoft's race to lose, Daniel Rubino, Windows Central, April 2, 2021 (https://www.windowscentral.com/microsofts-bet-hololens-paying)

[25] "The AR, VR future coming in 2022: What we leanred from CES" Scott Stein, CNET, January 10, 2022 (https://www.cnet.com/tech/computing/vr-and-ar-looked-to-the-metaverse-at-ces-2022/)

[26] "Virtual Reality/Augmented Reality White Paper," China Academy of Information and Communications Technology (CAICT), 2017. https://www-file huawei.com/-/media/corporate/pdf/ilab/vr-ar-en.pdf

[27] The Great Rivalry: China vs. the U.S. in the 21st Century, Graham Allison, Harvard University Belfer Center for Science and International Affairs, Dec. 7, 2021. https://www.belfercenter.org/publication/great-rivalry-china-vs-us-21st-century

[28] Allies like the United Kingdom are taking a strategic approach to XR. The Digital Catapult is the British government innovation agency for the digital and software industry, developed in conjunction with Innovate UK. Digital Catapult explicitly lists immersive technology as one of its three specialty areas for provision of assistance. This focus is accompanied by extensive grants and investments in R&D by the UK government to support the immersive technology sector in the UK. See also https://www.digicatapult.org.uk/technologies/immersive/virtual-reality

[29] China Task Force Report, Michael T. McCaul, Chairman, U.S. House of Representatives, September 29, 2020.

[redacted]

influenced by U.S. legislation. What's more, U.S.-based companies' commitment to privacy is a key advantage that should be leveraged, experts say. In a presentation to the National Academies of Sciences, Engineering, and Medicine in 2020, Jason Matheny, founding director of the Center for Security and Emerging Technology, said that "new advancements in privacy technology and a 'commitment to privacy protection' may also offer strategic advantages."[30]

The Belfer Center report also notes the U.S. tech industry's commitment to both innovation and transparency:

> *The U.S. continues to have many advantages, including a greater number of top research universities;* ***tech companies that are more accountable to the public****; a more transparent form of government allowing for popular participation; a wider range of technology partnerships abroad; a persistent appeal to high-skilled migrants; an unparalleled advantage in emerging technologies including aeronautics, medicine, and nanotech; and a tradition of protecting and enabling blue-sky innovators.*

U.S. leadership in XR development is needed to ensure the technology advances in alignment with cultural values that place a premium on freedom of thought and expression, learning, cooperation, and other standards of an open and flourishing society. Technology reflects the culture and values of the people who create it.[31] America's competitiveness will quickly wither if the U.S. prematurely limits the use of biometric data - a situation that would stifle innovation, negatively impact economic growth, and prevent U.S.-based companies from providing leadership on issues of privacy and security.

Conclusion

It is not a question of if, but when, XR technology will become ubiquitous and replace our current modes of computing, and no one doubts that technologies that employ biometric data will be developed to push that movement forward. What remains to be decided is whether that innovation will happen here in the U.S., where companies are more accountable to the public and have a stronger commitment to privacy and security, or on the other side of the world where individual rights are not afforded the same level of respect.

To ensure that the U.S.-based XR industry can continue to lead, innovate, and provide benefits to consumers, workers, people with disabilities, and our national security, we must resist the impulse to place stringent restrictions on the development of biometric technologies. While legitimate concerns exist about the use of biometric data, the U.S. XR industry is committed to developing their products with privacy by design. And only in the U.S. can that goal become a reality.

For additional discussion of XR's benefits to industry, society, and U.S. technological advancement overall, please see XRA's 2021 white papers "The Integrated Technology Landscape of the Future and

[30] "The Future of Data Science," Jason Matheny, keynote speech at the National Academies of Sciences, Engineering, and Medicine, Nov. 4, 2020. https://cset.georgetown.edu/article/the-future-of-data-science/
[31] "China's AI tech leaves aside questions of ethics," Yasu Ota, *Nikkei Asia*, August 23, 2020. https://asia nikkei.com/Spotlight/Comment/China-s-AI-tech-leaves-aside-questions-of-ethics

the Synergistic Effect of Immersive Technologies,"[32] and "Immersive Technology and Infrastructure: Building America's Future,"[33] as well as our 2020 letter to the Department of Health and Human Services on the use of XR technology to reach aging, underserved populations.[34]

We hope the information above helps the Office of Science and Technology Policy to better understand why biometric technologies are essential to the functioning of XR technology; the tremendous societal benefits this technology provides; the industry's commitment to continuing to develop the principles, practices, and policies governing their use; and the stakeholders that may be impacted by their use or regulation. We welcome further discussion on this topic and are glad to answer any questions you may have.

Sincerely,

[redacted]

Elizabeth Hyman, CEO

XR Association

[32] "The Integrated Technology Landscape of the Future and the Synergistic Effect of Immersive Technologies," XR Association, 2021. https://xra.org/wp-content/uploads/2021/04/EFA-White-Paper-Final.pdf

[33] "Immersive Technology and Infrastructure: Building America's Future," XR Association, 2021. https://xra.org/wp-content/uploads/2021/06/XRA_Immersive-Technology-and-Infrastructure_Whitepaper-1.pdf

[34] Letter to Dr. Leith States, Chief Medical Officer, Office of the Assistant Secretary for Health U.S. Department of Health and Human Services, December 2020, Document # 2020-25328; Document Citation 85 FR 73280. https://xra.org/wp-content/uploads/2020/12/HHS-RFI-Final.pdf

[redacted]

Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

XR Safety Initiative

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.

RFI Response: Biometric Technologies

Respondents:

- Kavya Pearlman - Founder and CEO XR Safety Initiative, XR Safety Initiative (XRSI)
- Marco Magnano - Cofounder and Executive Director of Communications, XR Safety Initiative (XRSI)
- Rachel Michelon - Medical XR Advisory Council Lead, XR Safety Initiative (XRSI)
- Ryan Cameron - Medical XR Adviser and Co-chair Medical XR Privacy & Safety Framework, XR Safety Initiative (XRSI)

Respondent Type: Non-Profit Research Organization registered in California, USA

About XR Safety Initiative (XRSI)

XR Safety Initiative (XRSI) is a 501(c)(3) worldwide not-for-profit Standards Developing Organization(SDO) that promotes privacy, security, and ethics in immersive environments. XRSI's mission is to help build safe and inclusive experiences so that XR stakeholders can make informed and pragmatic decisions. XRSI does this by discovering novel cybersecurity, privacy, and ethical risks and proposing potential new solutions to mitigate them. XRSI, being the first such global effort, is uniquely positioned to provide impartial, practical information about XR and Spatial Computing-related risks and opportunities to individuals, corporations, universities, government agencies, and other organizations worldwide. XRSI launched the first novel XRSI Privacy Framework for the XR and SpatialComputing domain to address the impact of Biometric Inferences via Special Data Type consideration. The framework has been well received and has been a point of discussion among XR stakeholders and many regulatory entities worldwide.

SUMMARY

Even though XRSI specifically focuses on Immersive Technologies and Metaverse-related use cases, we have discovered that Biometric Inferences impact most of the technology landscape and, in turn, humans. With the significant focus on the Metaverse globally, amplified by the pandemic, the use of Immersive Technologies such as XR[1] and its intersections that utilize Biometric data and inferences must not be ignored. If anything, XR use cases are the perfect testing ground for classifying and handling the potential risks and opportunities stemming from Biometric inferences.

The domains in which these technologies are being used: XR and Metaverse related Technologies and their intersections, e.g., Artificial Intelligence, Robotics, Decentralized Ledger Technologies, Brain-Computer Interfaces, etc.

The entities making use of them: Big tech companies like Meta, Microsoft, Google, Niantic, Snap, Netflix, Amazon, Neuralink, and a large number of Metaverse-focused organizations.

Current principles, practices, or policies governing their use are lacking when it comes to inferences. From a policy perspective, most companies can only address Biometric Data per state laws or European specific General Data Protection Regulation (GDPR) within the context of Privacy laws. None of the laws, including GDPR, currently address inferences and their impact. XRSI analyzed these laws within the United States and found no mention, indication, or guidance on the inferences application or use.

[1] Extended Reality (XR) is a fusion of all the realities – including Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) – which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures. Source: https://xrsi.org/definition/extended-reality-xr

Topic 1. Descriptions of use of biometric information for recognition and inference

Information about planned, developed, or deployed uses of biometric data, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

XR Safety Initiative (XRSI) is serving as a subcontractor to Cyber Bytes Foundation (CBF) to create natural authentication methods for First Responders using Augmented Reality (AR) Systems in the context of a NIST Grant award. XR technologies can be valuable tools to Public Safety Organizations (PSOs) in doing their jobs and accomplishing their missions.

First Responders often have to utilize multiple disconnected databases in the line of duty to gain critical information such as juvenile status or identification verification.

AR can provide a means to have this information directly in the line of sight, but the AR device must be authenticated due to the sensitive nature of the data it would be displaying. This prevents equipment and sensitive data from falling into the wrong hands in often chaotic situations.

The issue is further amplified when PSOs operate in limited settings such as unreliable network coverage, sensitive situations like an active shooter, etc.

By using Biometric Inferences (Natural Authentication) to reduce or eliminate cognitive load during authentication to the AR device at hand, first responders can remain focused on their duty.

The research work focuses on identifying PSOs' requirements such as form factor, usability, and other pertinent factors to identify and validate authentication methods as probable.

These methods are tested and validated further to develop secure and safe authentication methods through actual PSOs participation.

During the research, companies are identified as using AR, and existing authentication methods that authenticate users to AR devices are identified. Existing AR devices and sensors that provide Biometric Inferences are also identified.

Topic 2. Procedures for and results of data-driven and scientific validation of biometric technologies

Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting in error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies, when deployed in a specific societal context, is also welcome.

The work from previously mentioned natural authentication methods for First Responders using Augmented Reality (AR) Systems via NIST Grant award[2] is planned to include prototype development that records several biometric data streams to train a Machine Learning algorithm and then the result will be used to identify the subject in an appropriate context. These biometric data streams could be used by themselves or in combination with others and would consist of data such as voice audio samples, EKG, EEG, body movement patterns, gaze patterns, galvanic skin response, bio capacitance, and any others we can include within the scope of the project. As first responders are authenticated, cognitive load, as well as other attention metrics, will be measured and compared to a baseline so it can be determined whether the method truly is Natural Authentication. The end goal is to ensure that the device is authenticated as close to real-time as possible without impacting the awareness of the subject, as well as being resilient against environments and challenges faced by first responders in the line of duty.

Topic No. 3. Security considerations associated with a particular biometric technology.

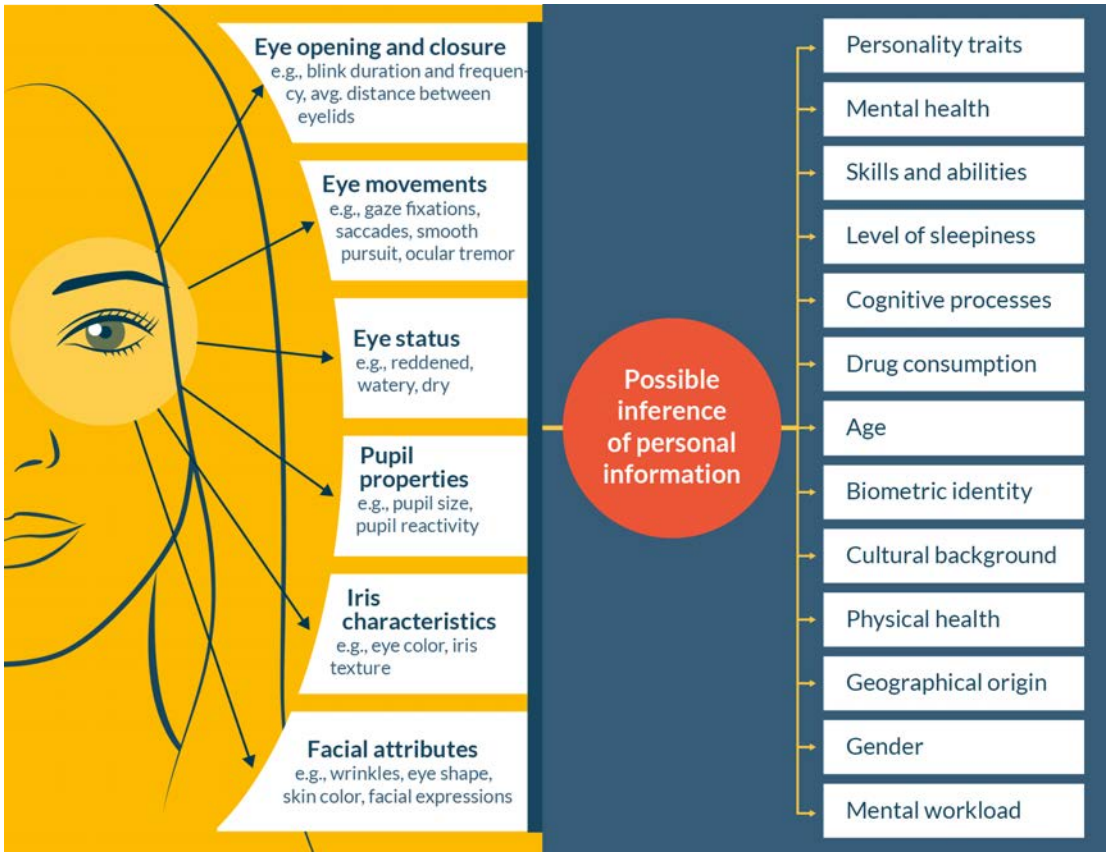
Information about validation of the security of biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally-identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end-users, and impacted communities.

[2] Natural Authentication methods for First Responders using Augmented Reality (AR) SystemsNIST Grant Award
https://xrsi.org/cyber-bytes-foundation-and-xrsi-announce-grant-award-to-create-natural-authentication-methods-for-first-responders-using-augmented-reality-systems

XRSI has developed a Privacy and Safety Framework for XR and Spatial Computing Domain[3] specifically focusing on Biometric Inferences. Many organizations are developing immersive technologies to build all-day wearable glasses that are spatially aware with the goal of delivering AR and VR experiences more immersive and integrated into the physical world serving as the baseline for the Metaverse. In order to achieve this outcome via the use of AI algorithms, a large amount of data collection is necessary. The concerns for excessive data collection are heightened because of a large amount of real-time data collection and the potential inferences that are possibly made. While some inferences are necessary and even welcomed by individuals such as curated and customized shopping preferences many others such as Biometrically-Inferred Data (BID) are not and may cause harm to humans.

Biometrically-Inferred Data (BID)[4] is a collection of datasets resulting from information inferred from behavioral, physical, and psychological biometric identification techniques, and other nonverbal communication methods. For example, XR devices can lead to inferences such as biometric and gender identity, mental workload, mental health status, cognitive abilities, religious and cultural background, physical health, geographic origin, and many other skills, abilities, personality traits, and more. Based in different jurisdictions, organizations may be mandated to protect BID and require adopting a data governance framework like XRSI's. This will prevent excessive and unwarranted data collection at the hardware, operating system, API, and software levels, leading to responsible research and innovation in the XR domain. Below are a few examples of the data tracked and collected by and for XR devices.

[3] XRSI Privacy and Safety Framework for XR and SPatial Computing Domain http://www.xrsi.org/psf11
[4] Biometrically Inferred Data https://xrsi.org/definition/biometrically-inferred-data-bid



The emergence of the Metaverse has led to the convergence of various technologies such as XR, Brain-Computer Interfaces (BCI), Artificial Intelligence (AI), etc. The citizens must be protected from these technologies that are capable of mind control, mind-reading, or any other nefarious interference with human brains. While such concerns used to be relegated to conspiracy-theory chat rooms and science fiction, now they're subject to debate by senators.

At the end of 2021, in fact, a constitutional amendment was passed by the National Congress of Chile and signed by the president, the people of Chile as the first in the world to be granted a new kind of human rights—"neuro-rights"—which are made necessary to protect human agency and autonomy from advances in neurotechnology and the convergences leading up to the Metaverse.

XR Safety Initiative (XRSI) has been investigating these rights and the way to facilitate them via their Medical XR-focused Privacy and Safety Framework. These conversations need to happen at a global regulatory level and more efforts are needed to ensure we do not lose human agency and autonomy as we move fast toward and our dependence on Metaverse focused technologies grows. BID provides a legal foundation to classify

and protect health inferences as well facilitate neuro rights policy directives to be discussed at the regulatory level. XRSI conducted additional research (resulting in the Securing the Metaverse Research Paper) and presented it at the Simulation Interoperability Standards Organization - SISO Symposium in 2021.[5]

Topic 4. Exhibited and potential harms of a particular biometric technology

Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

XR in healthcare presents unique opportunities for patient harm that otherwise did not exist. When a person is fully immersed in a new reality, simple things like ensuring there is a visual representation of a floor, a horizon, or lighting that we often take for granted can really cause serious harm to a patient if not implemented properly. People can stumble, walk into windows or off a balcony, injure their head if the environment is poorly designed. On top of that, VR can introduce psychological trauma because it is just so immersive. This is seen in experiments carried out at various universities where VR has been shown to be so immersive, it can replace pain medication for pregnant patients, or enhance and replace cognitive behavioral therapy that traditionally utilizes psychedelic drugs. In terms of biometrics, VR cameras that display for the user can be moved/angled by software to accommodate vision alignment issues, but bad actors could use this to cause severe eye strain or double/blurred vision to injure subjects.

Given these unique harms, it is simply critical that regulatory oversight that is steeped in research is applied not only in the medical device space but wherever XR is utilized for any purpose. This regulatory oversight needs to address these unique concerns and XRSI Medical Privacy and Safety Framework[6] is being developed to address these issues. See medical.xrsi.org for more information.

[5] Securitng the Metaverse Research by https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=52969&PortalId=0&TabId=105

[6] XRSI Medical Privacy and Safety Framework https://medical.xrsi.org/

Cyber XR Coalition for advocacy and rights : The mission is to actively address social and technical biases in emerging technologies that foster a sense of belonging while helping to ensure a safe experience for all. The coalition advocates to address the impact resulting from the misuse of biometric inferences and from algorithmic biases potentially undermining the human rights of minorities and others. The coalition uses this knowledge to inform global standards for Accessibility, Ethics, Inclusion, and Safety for immersive technologies. CyberXR advocates the use of technologies to create an equitable future with the benefits of scientifically valid technologies with appropriate contexts and proposes global standards to implement safeguards against anticipated and unanticipated misuse or harm.

Topic 6. Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case

With the newly-emerged focus on the Metaverse, which is going to be the confluence of various technologies such as XR, AI, BCI, Robotics and more it is imperative to extend data protection beyond just PII (Personally Identifiable Information or Personal Data and understand the context for putting better safeguards in place. XRSI commenced its mission in early 2019 and immediately started researching and investigating these matters via the XR Data Classification Public Working Group.[7]

a. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;
   XRSI began conducting a series of closed roundtables last year. The goal of the roundtables is to connect stakeholders, technologists, and human rights experts in a dialogue sharing their insights, research, data, experiences, and concerns to address the implications of enormous amounts of data being collected and shared in the immersive ecosystems. Through the multidisciplinary roundtables XRSI is able to collaboratively map the classification contexts and schemes that enable and drive the adoption of various augmented reality (AR) and virtual reality (VR) technologies.

b. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;
   The magnitude and scale of XR data make it challenging to categorize in a simplified manner. Regardless, an attempt must be made to look through and analyze such a large amount of data with a filter of Information Security, privacy and safety principles.

[7] XR Data Classification Public Working Group https://dc.xrsi.org/working-group/

Since XR has the potential to record all new kinds of user information (from eye movements and emotions to the movement of a user's entire body through space), ensuring that this data is managed in a responsible way has become paramount for virtual XR researchers and commercial entities alike.
XRSI's Medical XR Advisory Council is currently studying various use cases and as preliminary research to discover potential areas of concern for patient harm and privacy violation unique to XR.

c. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;
The development of Data Classification guidance, common vocabularies, and Data sets will certainly contribute to the understanding of potential risks associated with XR data.

d. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;
The outcome and framework from the data classification will serve as the foundation to further build safeguards for the immersive technology domain via XRSI Privacy and Safety Frameworks

e. Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);
Planned for further development of XRSI Privacy and Safety Framework version 2.0

f. Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);
Planned for further development of XRSI Privacy and Safety Framework version 2.0

g. Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems;
Currently in development via XR Data Classification Public Working Group

h. Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.
Planned for further development of XRSI Privacy and Safety Framework version 2.0