RECOMMENDATION: Expand the AI Use Case Inventory by Limiting the 'Sensitive Law Enforcement' Exception

The National Artificial Intelligence Advisory Committee (NAIAC)
Law Enforcement Subcommittee (NAIAC-LE Subcommittee)

February 2024

NAIAC MEMBERS

Miriam Vogel, *Chair*
President and CEO of EqualAI

James Manyika, *Vice Chair*
Senior Vice President, Google, President for Research, Technology & Society

Amanda Ballantyne
Director of the AFL-CIO Technology Institute

Jack Clark
Co-founder of Anthropic

David Danks
Professor of Data Science and Philosophy at the University of California, San Diego

Victoria A. Espinel
President and CEO of BSA | The Software Alliance

Paula Goldman
Chief Ethical and Humane Use Officer at Salesforce

Susan Gonzales
Founder and CEO of AIandYou

Janet Haven
Executive Director of Data & Society

Daniel E. Ho
William Benjamin Scott and Luna M. Scott Professor of Law, Professor of Political Science, and Professor of Computer Science (by courtesy), Senior Fellow, Stanford Institute for Human-Centered AI, Stanford University

Ayanna Howard
Dean of Engineering at The Ohio State University

Jon Kleinberg
Professor in the Departments of Computer Science and Information Science at Cornell University

Ramayya Krishnan
W. W. Cooper and Ruth F. Cooper Professor of Management Science and Information Systems, Carnegie Mellon University

Ashley Llorens
Vice President, Distinguished Scientist, and Managing Director at Microsoft Research

Haniyeh Mahmoudian
Global AI Ethicist at DataRobot, Inc.

Christina Montgomery
Chief Privacy & Trust Officer and Vice President at IBM

Liz O'Sullivan
CEO of Vera

Fred Oswald
Professor and Herbert S. Autrey Chair in Social Sciences, Rice University

Trooper Sanders
CEO of Benefits Data Trust

Navrina Singh
Founder and CEO of Credo AI

Swami Sivasubramanian
Vice President for Data and Machine Learning Services at Amazon Web Services

Keith Strier
Vice President for Worldwide AI Initiatives at NVIDIA

Reggie Townsend
Vice President of Data Ethics at SAS Institute

RECOMMENDATION

Recommendation:
Expand the AI use case inventory by narrowing the 'sensitive law enforcement' exception.

A. Background:

Since 2020, the executive branch has required that federal agencies create and make public an inventory of how they are using AI.[1] These AI Use Case Inventories (UCIs) are meant to serve as a tool to support a national strategy of transparent and accountable AI use by the federal government.

At present, however, the public use case inventories published by federal law enforcement agencies are not fulfilling their transparency and accountability promise. For example, the Department of Justice's 2022 disclosures consisted of one page of information, listing a single use of AI by the FBI for a "threat intake processing system" to analyze crime tips.[2] This single page contained no information about the FBI's use of facial recognition technology despite the fact that the Bureau has been using this AI-powered technology for criminal investigations for almost a decade.[3] Likewise, there were zero disclosures for multiple other DOJ law enforcement agencies' use of facial recognition — from DEA to ATF to the U.S. Marshals — even though a recent Government Accountability Office (GAO) audit reported significant use of this technology by each of these agencies.[4] Although DOJ updated its disclosures in 2023 with a few additional use cases, these updates still did not include the use of facial recognition by any of these sub-agencies.[5] Nor are there any disclosures relating to use of license plate readers.

[1] Executive Order 13960 of December 3, 2020, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," Code of Federal Regulations, 78939-78943, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

[2] "2023 Agency Inventory of AI Use Cases," U.S. DOJ, https://www.justice.gov/open/page/file/1517316/download; Christie Lawrence, Isaac Cui, Daniel E. Ho, "Implementation Challenges to Three Pillars of America's AI Strategy," Stanford HAI, December 2022, https://hai.stanford.edu/sites/default/files/2022-12/HAIRegLab%20White%20Paper%20-%20Implementation%20Challenges%20to%20Three%20Pillars%20of%20America%E2%80%99s%20AI%20Strategy.pdf.

[3] Greta Goodwin, "Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains," GAO-19-579T, U.S. GAO, June 2019, https://www.gao.gov/assets/gao-19-579t.pdf.

[4] "Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties," GAO-23-105607, U.S. GAO, September 2023, https://www.gao.gov/products/gao-23-105607.

[5] "2023 Agency Inventory of AI Use Cases," U.S. DOJ.

This underreporting may be due to an expansive interpretation of an exception for "sensitive law enforcement" uses. The CIO Council's current guidance for UCIs contains vague and broad exclusionary language for "sensitive law enforcement" interests.[6] A recent GAO audit — this one specifically surveying agencies' AI use case reporting — confirmed federal law enforcement agencies' broad use of and reliance on this exclusionary language. Although GAO observed "instances of incomplete and inaccurate data across 15 agencies," it found that the DOJ had complied with all inventory requirements.[7] When asked to explain this finding, in light of significant DOJ use case omissions, GAO stated that the DOJ declined to include these programs because it deemed them "sensitive" and therefore properly subject to exclusion — a determination which the DOJ was able to make absent any external oversight.

In our view, such a broad exclusion undermines the transparency and accountability goals of the use case inventory. Importantly, transparency is not just a "foundational value of democracy," but it also is "essential to effective policing."[8]

To be sure, there will be some information that law enforcement agencies have a legitimate interest in keeping secret. For the most part, this is information that "could either substantially undermine ongoing investigations or put officers or members of the public at risk," such as specific operational details or investigatory tactics.[9] Disclosing the generalized use of an AI tool — such as an agency's use of facial recognition or license plate readers — is unlikely to rise to this level. In fact, it is hard to imagine a tool that is in use by law enforcement agencies (as opposed to national securities agencies) where the very existence of the tool (not all of its operational details) will undermine law enforcement investigations.[10] This is

[6] "Guidance for AI Use Case Inventories," U.S. CIO, 2023, https://www.cio.gov/assets/resources/2023-Guidance-for-AI-Use-Case-Inventories.pdf.

[7] "Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements," GAO-24-105980, U.S. GAO, December 2023, https://www.gao.gov/products/gao-24-105980.

[8] "Principles of the Law, Policing: Combined Revised Tentative Drafts," The American Law Institute, January 2023, § 1.05 Reporters' Notes, https://www.policingprinciples.org/wp-content/uploads/2023/01/Policing-Tentative-Draft_1-31-23.pdf.

[9] "Principles of the Law, Policing," The American Law Institute, § 1.06 Reporters' Notes.

[10] "Principles of the Law, Policing," The American Law Institute, § 1.06 Reporters' Notes; Barry Friedman and Maria Ponomarenko, "Democratic Policing," 90 NYU Law Review, (2015): 1827, 1884-85, discussing law enforcement objections to transparency and observing that "the need for secrecy is not nearly as acute as it may seem. . . ." and distinguishing between details related to specific investigations, which have a rightful claim to secrecy, and details related to use of tools or techniques which "can be made public and publicly debated without undermining law enforcement interests."

particularly so when federal law enforcement agencies already disclose some details in other public documents (such as privacy impact assessments).[11]

B. Recommendation:

To ensure law enforcement agencies produce more meaningful public inventories, we recommend that the CIO Council and OMB revise current guidance to narrow the "sensitive law enforcement" exemption. Every law enforcement use of AI should begin with a strong presumption in favor of public disclosure. An exception for disclosing sensitive law enforcement uses should be limited to information that either would substantially undermine ongoing investigations or would put officers or members of the public at risk, such as specific operational details or investigative tactics. It should not apply to information that sets out in general terms the existence of an AI technology and the general circumstances under which the technology may be deployed. Agency decisions that information is subject to exclusion should be documented, require approval of the agency's Chief AI Officer, and be subject to oversight.

[11] Erin M. Prest, "Privacy Impact Assessment for the Next Generation Identification-Interstate Photosystem," U.S. FBI, October 29, 2019, https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view (FBI disclosure of use and capabilities of facial recognition system as part of its interstate photo system); "Comment re: OMB Guidance," Brennan Center for Justice, December 5, 2023, https://www.regulations.gov/comment/OMB-2023-0020-0162 ("Public release undermines any argument for wholesale withholding information about a system based on practicability or protection of information.").

ACKNOWLEDGEMENTS

The NAIAC-LE Subcommittee participated in the preparation of this document.

Armando Aguilar
Assistant Chief of Police, Miami Police Department

Anthony Bak
Head of AI, Palantir

Amanda Ballantyne
Director of the AFL-CIO Technology Institute

Jane Bambauer
Director - Marion B. Brechner First Amendment Project, Brechner Eminent Scholar at the College of Journalism and Communications and at Levin College of Law, University of Florida

Esha Bhandari
Deputy Director of the American Civil Liberties Union’s Speech, Privacy, and Technology Project

Jennifer Eberhardt
Professor of Organizational Behavior and Psychology, Stanford University

Farhang Heydari
Assistant Professor of Law, Vanderbilt Law School

Benji Hutchinson
Chief Revenue Officer of Rank One Computing

Rashawn Ray
Vice-President and Executive Director of the AIR Equity Initiative

Cynthia Rudin
Professor of Computer Science, Electrical and Computer Engineering, Statistical Science, Mathematics, Biostatistics & Bioinformatics at Duke University

A quorum of the membership of NAIAC reviewed and approved this document.

ABOUT NAIAC-LE SUBCOMMITTEE

The Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee (NAIAC) has the responsibility to make recommendations and provide advice on matters relating to the development, adoption, or use of AI in the context of law enforcement.

The Subcommittee was established in Section 5104 (e) of the National Artificial Intelligence Initiative Act of 2020. It is charged with providing advice to the President, through recommendations that will be considered by the full NAIAC, on a range of legal and ethical issues that will arise as law enforcement increases its use of AI tools. These issues include AI bias, data security, adoption protocols, and legal standards. (Section 5104 (e) (2).)

The Law Enforcement Subcommittee was established in the summer of 2023 and began its work in August 2023.

ABOUT NAIAC

The National Artificial Intelligence Advisory Committee (NAIAC) advises the President and the White House National AI Initiative Office (NAIIO) on the intersection of AI and innovation, competition, societal issues, the economy, law, international relations, and other areas that can and will be impacted by AI in the near and long term. Their work guides the U.S. government in leveraging AI in a uniquely American way — one that prioritizes democratic values and civil liberties, while also increasing opportunity.

NAIAC was established in April 2022 by the William M. (Mac) Thornberry National Defense Authorization Act. It first convened in May 2022. It consists of leading experts in AI across a wide range of domains, from industry to academia to civil society. https://www.ai.gov/naiac/

###