epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 28, 2024

Mark Greene (mark.green2@usdoj.gov)
Office Director, Office of Technology and Standards
National Institute of Justice
810 7th Street NW, Washington, DC 20531

Re: Request for Input from the Public on Section 7.1(b) of Executive Order 14110

Mr. Greene:

The Electronic Privacy Information Center (EPIC) submits the comments below in response to the National Institute of Justice (NIJ or the Institute)'s Request for Input from the Public on Section 7.1(b) of Executive Order 14110. Our comments highlight three main points:

1. The promise of AI innovation too often serves as a smokescreen for negligent AI development and deployment, injecting harmful bias, errors, data security vulnerabilities, and other risks outlined below into core criminal justice processes.

2. To minimize harm, criminal justice AI applications require additional oversight and accountability mechanisms—including additional mechanisms to ensure compliance by law enforcement agencies.

3. Certain AI technologies, such as emotion recognition and one-to-many facial recognition, should be banned because they produce excessive racial bias, errors, and privacy risks across all use contexts.

For further details on EPIC's research, recommendations, and concerns around criminal justice AI and automated decision-making, we recommend the following non-exhaustive list of EPIC resources:

1. EPIC Report: *Generating Harms: Generative AI's Impact & Paths Forward* (May 2023)
2. EPIC Report: *Generating Harms II: Generative AI's New & Continued Impacts* (May 2024)
3. EPIC Report: *Liberty at Risk: Pre-Trial Risk Assessment Tools in the U.S.* (September 2020)
4. EPIC's Comments to OMB on Privacy Impact Assessments (April 2024)
5. EPIC's Comments to the NTIA on Dual Use Foundation Models (March 2024)
6. EPIC's Comments to DOJ and DHS on Law Enforcement Uses of AI (January 2024)
7. EPIC's Comments to OMB on Federal AI Risk Management (December 2023)

Respectfully submitted,

/s/ Grant Fergusson
Grant Fergusson
Equal Justice Works Fellow
fergusson@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL INSTITUTE OF JUSTICE

On its Request for Input from the Public on Section 7.1(b) of Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"

89 Fed. Reg. 31,771

May 28, 2024

The Electronic Privacy Information Center (EPIC) submits these comments in response to the National Institute of Justice (NIJ)'s Request for Input from the Public on Section 7.1(b) of Executive Order 14110, published on April 25, 2024.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] We advocate for a human rights-based approach to AI policy that ensures new technologies are subject to democratic governance.[3] Over the last decade, EPIC has consistently advocated for the adoption of clear, commonsense, and actionable AI regulations across the federal government.[4] EPIC has litigated cases against the U.S. Department of Justice to compel production of documents regarding "evidence-based risk assessment tools,"[5] against the U.S. Department of Homeland Security to produce documents about a program purported to assess the probability that

---

[1] 89 Fed. Reg. 31771 (Apr. 25, 2024).
[2] *About Us*, EPIC, https://epic.org/about/ (2024).
[3] *See, e.g.*, *AI and Human Rights*, EPIC, https://epic.org/issues/ai/ (2024); *AI and Human Rights: Criminal Legal System*, EPIC, https://epic.org/issues/ai/ai-in-the-criminal-justice-system/ (2024); EPIC, *Outsourced & Automated: How AI Companies Have Taken Over Government Decision-Making* (2023), https://epic.org/outsourced-automated/ [hereinafter "Outsourced & Automated Report"].
[4] *See, e.g.*, EPIC, Comments on the DOJ's and DHS's Request for Written Submission on Section 13(e) of Executive Order 14074 (Jan. 19, 2024), https://epic.org/documents/epic-comments-to-the-doj-dhs-on-law-enforcements-use-of-frt-biometric-and-predictive-algorithms/ [hereinafter "EPIC DOJ/DHS Comment"]; EPIC, Comments on the OMB's Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum (Dec. 5, 2023), https://epic.org/wp-content/uploads/2023/12/EPIC-OMB-AI-Guidance-Comments-120523-1.pdf.
[5] *EPIC v. DOJ*, 320 F. Supp. 3d 110 (D.D.C. 2018), *voluntarily dismissed*, 2020 WL 1919646 (D.C. Cir. 2020), https://epic.org/foia/doj/criminal-justice-algorithms/.

an individual will commit a crime,[6] and against the National Security Commission on Artificial Intelligence (NSCAI) to enforce its transparency obligations under the Freedom of Information Act and the Federal Advisory Committee Act.[7] EPIC has also published extensive research on emerging AI technologies like generative AI,[8] as well as the ways that government agencies develop, procure, and use AI systems around the country.[9]

EPIC submits these comments to raise three main points.

First, criminal justice AI and automated decision-making (ADM) use cases are uniquely high-risk and sensitive given the dire carceral consequences that result from inaccurate or biased decisions.[10] Effectively managing and mitigating these risks will be crucial for any criminal justice AI or ADM use case. These risks include, but are not limited to:

1. **Privacy risks:** Criminal justice AI and ADM systems raise at least two forms of data privacy risks—indiscriminate surveillance and commercial web scraping. First, many automated and real-time surveillance systems, such as ShotSpotter,[11] automated license-plate readers,[12] and even Ring camera footage,[13] collect a massive and indiscriminate array of personal and biometric data through real-time image, audio, and video recordings—including extensive data on individuals not being investigated or accused of a crime. Second, many predictive policing, risk scoring, and fraud detection systems are frequently built atop commercial web scraping, injecting unverified

[6] *See EPIC v. DHS – FAST Program*, EPIC, https://epic.org/documents/epic-v-dhs-fast-program/ (last visited May 20, 2024).
[7] *EPIC v. NSCAI*, 419 F. Supp. 3d 82, 86, 95 (D.D.C. 2019), https://epic.org/documents/epic-v-ai-commission/.
[8] EPIC, *Generating Harms II: Generative AI's New & Continued Impacts* (2024), https://epic.org/wp-content/uploads/2024/05/EPIC-Generative-AI-II-Report-May2024-1.pdf [hereinafter "EPIC GenAI Report II"]; EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* (2023), https://epic.org/gai [hereinafter "EPIC GenAI Report I"].
[9] Outsourced & Automated Report; EPIC, *Screened & Scored in the District of Columbia* (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf [hereinafter "Screened & Scored Report"].
[10] *See generally AI in the Criminal Justice System*, EPIC, https://epic.org/issues/ai/ai-in-the-criminal-justice-system/ (last visited May 22, 2024).
[11] *See, e.g.*, EPIC, Letter to Attorney General Garland Regarding ShotSpotter Title VI Compliance (Sept. 27, 2023), https://epic.org/documents/epic-letter-to-attorney-general-garland-re-shotspotter-title-vi-compliance/.
[12] *See* EPIC, Comments on the FTC's Proposed Trade Regulation Rule and Request for Comment on the Use of Customer Reviews and Endorsements 11–13 (Sept. 29, 2023), https://epic.org/documents/epic-comment-ftc-proposed-rule-on-consumer-reviews-and-endorsements/ (discussing Flock Safety license plate reader systems) [hereinafter "EPIC Endorsements Comment"]; Screened & Scored Report at 19 (discussing automated license plate readers).
[13] *See, e.g.*, EPIC Endorsements Comment at 8–11 (discussing law enforcement use of Amazon Ring data).

personal information from data brokers and social media websites into core criminal justice processes.[14]

2. **Accuracy and discrimination risks:** Relying on AI and ADM is a policy choice, and one that law enforcement agencies and courts frequently make without understanding the limitations of these systems.[15] Because AI and ADM systems make inferences about inputs—surveillance footage, personal records, etc.—based on average trends in their training data, AI and ADM outputs are generalized representations of the training data they used, rather than a reflection of reality. When training data includes inaccuracies, disparities, biased representations, or other mischaracterizations of the real world, any AI or ADM system trained on the data will tend to produce inaccurate and biased outputs. For example, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) system, a popular criminal risk assessment tool used in states like Florida, had an accuracy rate of only 20% for predicting future violent offenses; its inaccuracies flagged Black defendants as high recidivism risks twice as often as white defendants.[16] The result: Black defendants in Florida received higher bail amounts and longer jail sentences than other defendants, controlling for other factors.[17]

   These accuracy and discrimination risks can come from both facially inaccurate or biased data—such as inaccurate criminal records data—as well as facially neutral data that reflects trends of racial or other bias in housing, policing, and more.[18] Therefore, controlling for these risks requires not only data quality controls before and during AI development, but also post-development testing and red-teaming to ensure an AI or ADM system is accurate and unbiased for all intended use contexts.[19]

---

[14] *See* EPIC DOJ/DHS Comment at 64.
[15] *See* Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative for Machine Learning*, 34 Berkeley Tech. L.J. 781, 786 (2019).
[16] *See* Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. *See generally* EPIC, *Liberty at Risk: Pre-Trial Risk Assessment Tools in the U.S.* (2020), https://epic.org/documents/liberty-at-risk/.
[17] *Id.*
[18] *See* Screened & Scored Report at 23; Safiya Noble, Algorithms of Oppression: How Search Engines Reinforce Racism 1 (2018); Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, CDT (Jul. 7, 2021), https://perma.cc/L4ST-6C8D.
[19] *See, e.g.*, EPIC, Comments on NIST's Request for Information on its Assignments Under Sections 4.1, 4.5, and 11 of Executive Order 14110 3–6 (Feb. 2, 2024), https://epic.org/wp-content/uploads/2024/02/EPIC-Comment-on-NIST-AI-Executive-Order-Mandates-RFI-02.02.24.pdf; EPIC et al., Comments on OMB's Request for Information on Responsible Procurement of Artificial

3. **Accountability risks:** When a law enforcement agency, court, or other criminal justice actor relies on a privately developed AI or ADM system, it necessarily outsources part of its decision-making process to a private vendor and its technology.[20] What behavior is worth scrutinizing, which suspects are worth pursuing, which defendants should receive leniency, and more decisions are all filtered through AI and ADM recommendations, risk scores, and other screening processes. However, many AI vendors keep core features of their AI and ADM systems secret by claiming the software, training data, or underlying machine-learning models are "proprietary business information," making it difficult for even those with the knowledge and expertise to scrutinize and oversee AI and ADM systems to access the information they need to ensure systems are functioning properly.[21] The accountability risks of criminal justice AI and ADM applications come from the ways theses technologies displace traditional processes for holding our government accountable—and protecting individuals' rights throughout the criminal justice system. To effectively manage these systems and ensure explanations are available for core criminal justice decisions, government officials working in criminal justice need sufficient training, resources, access, and transparency to evaluate whether and when AI and ADM systems produce inaccurate or unreliable outputs.

4. **Data security risks:** AI and ADM systems rely heavily on data for their training and operation—often including sensitive, personal, and biometric data. Unlike databases, however, AI and ADM systems cannot easily remove inappropriate or illegally used training data or correct inaccurate training data; the AI training process leaves an indelible imprint of training data on the outputs an AI or ADM system produces.[22] For this reason, AI and ADM systems are particularly vulnerable to data leaks, data breaches, and other data security concerns. Law enforcement agencies and other criminal justice actors must therefore prioritize robust data security and privacy-

---

Intelligence in Government (Apr. 29, 2024), https://epic.org/wp-content/uploads/2024/04/Joint-Civil-Society-Comment-re-OMB-RFI-on-Responsible-Procurement-of-Artificial-Intelligence-in-Government.pdf.

[20] Outsourced & Automated Report at 21–25.

[21] *Id.* at 22.

[22] *See* Alison Snyder, *Machine Forgetting: How Difficult It Is to Get AI to Forget*, Axios (Jan. 12, 2024), https://www.axios.com/2024/01/12/ai-forget-unlearn-data-privacy; Jevan Hutson & Ben Winters, *America's Next "Stop Model!": Model Deletion*, 8 Geo. L. Tech. Rev. 125, 128–134 (Feb. 5, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225003.

protective measures like robust user authentication and differential privacy when using AI and ADM systems.[23]

Too often, private companies obscure negligent AI development and deployment practices through the language of AI innovation, thereby avoiding much-needed scrutiny for any harms that result when their technologies produce bias or errors in criminal justice contexts. For government actors to use any AI or ADM system in such sensitive and high-risk situations as policing, sentencing, and prison surveillance, they need *more* transparency, oversight, and risk management, not less. The United States has already seen remarkable technological innovation in highly regulated sectors like the automotive and energy industries; AI innovation should not be used as a reason to avoid regulation, but rather as a reason to formalize, implement, and innovate on key AI risk management and responsible development regulations. Mitigating AI risks and harms is fundamental to responsible AI innovation.

Second, even if government actors mitigate the risks inherent to AI and ADM systems through effective use of impact assessments, audits, and testing protocols, they must also ensure that law enforcement agencies, courts, and others working in criminal justice use these systems properly. Ineffective training, untested or unintended use cases, and intentional misuse of automated systems can all undermine responsible AI guardrails and harm the public. Over the last decade, for example, EPIC has uncovered several instances in which law enforcement agencies like the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Drug Enforcement Agency (DEA) failed to complete required privacy impact assessments (PIAs) under the E-Government Act of 2002[24] for activities implicating personal and sensitive data.[25] Without robust mechanisms to ensure compliance with AI risk management practices and oversee responsible AI use, law enforcement agencies and other government officials working in criminal justice may—intentionally or unintentionally—deploy AI and ADM systems in harmful ways across the criminal justice system.

Third, some AI and ADM technologies have been proven to cause serious harm across all use cases and thus cannot be used responsibly no matter the application. Relevant to the criminal justice system, provably harmful AI use cases include, but are not limited to, emotion recognition, biometric categorization, and one-to-many facial recognition. Emotion recognition systems rely

[23] *See, e.g.*, EPIC, Comments on OSTP's Request for Information on National Priorities for Artificial Intelligence 4–5 (July 7, 2023), https://epic.org/wp-content/uploads/2023/07/EPIC-OSTP-RFI-NationalPriorities.pdf; *cf.* EPIC, Comments on the NTIA's Request for Comment on Dual Use Foundation AI Models with Widely Available Model Weights 4–5 (Mar. 27, 2024), https://epic.org/wp-content/uploads/2024/03/EPIC_Comment_NTIA_Dual_Use_Foundation_Models_with_Appendix.pdf.

[24] 44 U.S.C. § 3501 note.

[25] *See* EPIC, Comments on the OMB's Request for Information on Privacy Impact Assessments 2–4 (Apr. 1, 2024), https://epic.org/documents/comments-of-epic-to-omb-on-privacy-impact-assessments/.

on the false premise that both universal emotions and a clear correlation between emotion and facial expression exist—a premise that has been repeatedly disproven.[26] Similarly, biometric categorization systems are based on the belief that certain physical characteristics can be linked to specific traits. This is fundamentally a form of digital phrenology.[27] Companies that provide these AI systems have claimed to be able to predict everything from the likelihood of terrorist leanings to sexuality based solely on the analysis of facial features.[28]

One-to-many facial recognition systems—also known as biometric identification systems—involve indiscriminate and ongoing privacy violations of millions of people in the hopes of identifying a single suspect. As Senators Wyden, Markey, Padilla, and Booker put it, "[n]ot only does this violate individuals' privacy, but the inevitable false matches associated with one-to-many recognition can result in [individuals] being wrongly denied desperately-needed services for weeks or even months as they try to get their case reviewed."[29] Further, one-to-many facial recognition systems have been shown to falsely identify people of color as criminals at rates as much as 100 times higher than those for people of Eastern European descent.[30] All of these AI use cases exhibit persistent and inherent inaccuracies, biases, and other harms that are inseparable from the AI systems' functionality; they cannot be corrected or managed in a way that mitigates harms

---

[26] Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-humanemotion/618696/; Lisa Feldman Barret et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 Ass'n for Psych. Sci., 1, 46 (2019), https://journals.sagepub.com/doi/pdf/10.1177/1529100619832930; *see also generally* Kuba Krys et al., *Be Careful Where You Smile: Culture Shapes Judgments of Intelligence and Honesty of Smiling Individuals*, 40 J. Nonverbal Behav. 101 (2016), https://link.springer.com/article/10.1007/s10919-015-0226-4; Charlotte Gifford, *The Problem with Emotion-Detection Technology*, New Econ. (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.

[27] *See* Blaise Aguera y Arcas et al., *Physiognomy's New Clothes*, Medium (May 6, 2017), https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a.

[28] *See* Sally Adee, *Controversial Software Claims to Tell Your Personality From Your Face*, New Scientist (May 27, 2016), https://www.newscientist.com/article/2090656-controversial-software-claims-totellpersonalityfrom-your-face/; *Researchers are Using Machine Learning to Screen for Autism in Children*, Duke Pratt Sch. of Eng'g (July 11, 2019), https://pratt.duke.edu/about/news/amazon-autism-app-video; Paul Lewis, *"I was Shocked it was so Easy": Meet the Professor Who Says Facial Recognition Can Tell if You're Gay*, Guardian (July 7, 2018), https://www.theguardian.com/technology/2018/jul/07/artificialintelligence-cantell-your-sexuality-politics-surveillance-paul-lewis; Madhi Hashemi & Margaret Hall, *Criminal Tendency Detection from Facial Images and the Gender Bias Effect*, 7 J. Big Data, 1, 1 (2020), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4 (since retracted); Luana Pascu, *Biometric Software that Allegedly Predicts Criminals Based on Their Face Sparks Industry Controversy*, Biometric Update (May 6, 2020), https://www.biometricupdate.com/202005/biometric-software-thatallegedlypredicts-criminals-based-on-their-face-sparks-industry-controversy.

[29] Letter from Senators Wyden, Markey, Padilla, and Booker to FTC Chair Lina Khan 1 (May 18, 2022), https://epic.org/wp-content/uploads/2022/05/Letter-to-FTC-on-ID.me-deceptive-statements-051822.pdf.

[30] *Id.*

while permitting the AI use case to continue. These systems are harmful by their very nature, and EPIC urges NIJ to explicitly call for their prohibition within its report under Executive Order 14110.

AI and ADM systems impose serious risks on the public, which can lead to inaccurate and biased decisions around whom to police, whom to arrest, whom to charge, and whom to release. As the NIJ develops its report on the use of AI and ADM in the criminal justice system, EPIC urges the Institute to take a critical and sociotechnical approach to these technologies, centering the myriad risks and harms from similar technologies used at the federal, state, and local levels. The United States cannot allow the potential of future AI innovation to obfuscate the real harms AI poses today and overtake the rights and safety of the American public. EPIC greatly appreciates this opportunity to comment on the NIJ's obligations under Executive Order 14110 and remains eager to continue engaging with NIJ further on any of the issues raised herein or in our prior work.

Respectfully submitted,

/s/ Grant Fergusson
Grant Fergusson
Equal Justice Works Fellow
fergusson@epic.org

/s/ Jeramie Scott
Jeramie Scott
EPIC Senior Counsel
scott@epic.org

/s/ Kara Williams
Kara Williams
EPIC Law Fellow
williams@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)