May 28, 2024

National Institute of Justice
810 7th St. NW,
Washington, D.C. 20531

Re: 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"; Comments on 89 Fed. Reg. 31771 (Apr. 25, 2024)

The undersigned racial justice, civil rights, human rights, technology policy, and privacy groups submit this comment to urge the National Institute of Justice ("NIJ") to consider the following recommendations regarding the use of artificial intelligence ("AI") in the criminal justice system. Black people and other people of color face significant civil rights harms resulting from law enforcement's use of AI. The best practices identified in the forthcoming report are crucial for addressing these harms and ensuring that any AI technologies developed, procured, used, or funded by law enforcement agencies do not cause or contribute to discrimination.[1] The report and its findings should be made public upon completion.

Long-term racial disparities in the criminal justice system fuel the systemic over-policing of Black communities and other communities of color.[2] Algorithmic technologies used by law enforcement agencies replicate and reinforce existing racial bias and discrimination; policing technologies such as facial recognition, risk assessments, and predictive policing tools often enable and accelerate this trend.[3]

These discriminatory effects stem from biases baked into the development and deployment of the technologies themselves. First, algorithmic tools used by law enforcement may exhibit racial bias based on their design and training data. Algorithmic systems, such as those used to predict crime rates, are trained using vast troves of data that are rife with inaccuracies and reflect existing societal biases and inequities in the criminal justice system.[4] Algorithmic systems that blindly rely on such data often

---

[1] *See* Executive Order 14110: Safe, Secure and Trustworthy Development and Use of Artificial Intelligence (October 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[2] *See* Press Release, White House, *Fact Sheet: President Biden to Sign Historic Executive Order to Advance Effective, Accountable Policing and Strengthen Public Safety* (May 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/25/fact-sheet-president-biden-to-sign-historic-executive-order-to-advance-effective-accountable-policing-and-strengthen-public-safety/.

[3] Simone Browne, *Dark Matters: On the Surveillance of Blackness* 50 (2015); Andrea Dennis, *Mass Surveillance and Black Legal History*, ACS Expert F. (Feb. 18, 2020), https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/.

[4] *See* Jane Chung, *Racism In, Racism Out: A Primer on Algorithmic Racism*, Public Citizen (2022), https://www.citizen.org/article/algorithmic-racism/; Weihua Li et al., *See if Police in Your State Reported Crime Data to the FBI*, Marshall Project (Aug. 3, 2023), https://www.themarshallproject.org/2022/08/15/see-if-police-in-your-state-reported-crime-data-to-the-fbi; Jeff Asher, *NIBRS Noncompliance Has Become More of a Small Agency Problem*, Jeff-alytics Substack, March 25, 2024, https://jasher.substack.com/p/nibrs-noncompliance-has-become-more; and William S. Isaac, *Hope, Hype, and Fear: The Promise and Potential Pitfalls of the Big Data Era in Criminal Justice*, 15 Ohio St. J. Crim. L. (2017).

replicate past discrimination. Second, law enforcement agencies may deploy algorithmic technologies in ways that reinforce existing human biases. For instance, a recent report found that the New Orleans Police Department disproportionately used facial recognition technology ("FRT") to identify Black individuals; they deployed the technology on Black people over 90 percent of the time. One city councilmember described the police department's use of FRT as "wholly ineffective and pretty obviously racist."[5]

Many AI systems used by law enforcement have been shown to result in, or have the potential to result in, discriminatory outcomes. For instance, the use of FRT by law enforcement has resulted in multiple wrongful arrests of Black people—including a Black woman in Detroit who was wrongfully arrested for a recently committed crime when she was eight months pregnant, even though the suspect was not pregnant, and a Black man in Georgia who had never been to Louisiana but was arrested for a crime that occurred in Louisiana.[6]

In another example, a popular crime prediction algorithm disproportionately predicted crime in neighborhoods that had higher populations of Black, Latino, and low-income residents, often predicting little to no crime in wealthier, whiter neighborhoods.[7] The system was based on data of previously reported crimes, reflecting racial disparities in crime reporting and statistics. Available data also indicated higher arrest and use-of-force rates by police in neighborhoods with higher prediction rates, suggesting that the software reinforces existing disparities.[8]

Predictive tools used by courts in bail and sentencing decisions and by parole authorities in parole decisions also create significant risks to human and constitutional rights. These tools, known as "risk assessments," assign risk scores to individuals, including defendants.[9] These risk scores influence determinations about defendants' freedoms; from bond amounts to parole eligibility and sentencing lengths. Researchers obtained seven thousand individuals' risk scores from 2013 and 2014 and investigated whether those individuals were charged with committing any new crimes in the subsequent

---

[5] *See* Alfred Ng, *'Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing*, Politico (Oct. 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

[6] *See* Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/technology/facial-recognition-false-arrest.html; John Simerman, *JPSO Used Facial Recognition Technology to Arrest a Man. The Tech Was Wrong.*, NOLA.COM (Jan. 2, 2023), https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html; *see also, e.g.*, Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED (Feb. 28, 2023), https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/; Patrick Grother et al., *Facial Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM. 2, 7, 47 (NISTIR 8280, Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[7] Aaron Sankin et al., *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, THE MARKUP (Dec. 2, 2021), https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[8] *Id.*

[9] Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Ames Grawert and Patricia Richman, Brennan Ctr. for Just., *The First Step Act's Prison Reforms* 3–6 (Sept. 23, 2022), https://www.brennancenter.org/our-work/research-reports/first-step-acts-prison-reforms.

two years.[10] Researchers found that the predictive algorithm was "particularly likely to falsely flag black defendants as future criminals, wrongly labeling them [as greater crime risks] at almost twice the rate as white defendants."[11]

Such harms are compounded by the fact that law enforcement's use of AI often lacks transparency, explainability, or public accountability. Shrouded in secrecy, law enforcement agencies use AI technologies – ranging from police surveillance to suspect identification and prison-management tools – without meaningful public input or oversight. As a result, impacted communities frequently lack transparency about when, why, and how law enforcement uses AI. Without this transparency, law enforcement denies individuals recourse to contest errors or defend their rights.

When police use AI during a criminal case, law enforcement and prosecutors often fail to disclose critical information about use and performance of these technologies to defendants and defense attorneys. Without access to such information, criminal defendants have no way to assess the accuracy of technologies used to implicate them.[12]

In order to address the civil rights risks and discriminatory harms stemming from law enforcement's use of AI, it is critical that the NIJ's forthcoming report assess policies and practices that can accomplish the following goals:

Law enforcement's use of racially discriminatory technologies, including FRT and predictive policing tools, should be prohibited. Research has repeatedly shown that FRT and predictive policing tools are racially discriminatory. Because of this, all federally funded law enforcement uses of these technologies should be prohibited by default as presumptively discriminatory and in violation of Title VI of the Civil Rights Act of 1964. Limited waivers, on a case-by-case basis, could be granted, but only when there is clear and convincing evidence that a specific technology, used by a specific law enforcement agency strictly in adherence with specific policies and procedures, is affirmatively shown to be not discriminatory on the basis of protected characteristics. In all cases where a waiver is granted, law enforcement agencies should be required to disclose the use of such technologies and to complete pre- and post-deployment audits.[13]

The use of algorithmic surveillance tools should be prohibited in public places and in any setting that could chill the exercise of First Amendment rights. The proliferation of surveillance technologies – such as aerial drones and FRT-enabled surveillance cameras – enables law enforcement's overbroad, intrusive, and discriminatory surveillance of Black people and other people of color. These

[10] *Id.*
[11] *Id.*
[12] *See*, generally, Rebecca Wexler, Life Liberty and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 STAN. L. REV. 1361 (2018).
[13] Critically, the Office of Management and Budget's recent guidance on agency use of AI defines all law enforcement uses of AI as presumptively safety-impact and rights-impacting. *See* Office of Management and Budget, Executive Office of the President, M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Mar. 28, 2024) [hereinafter "AI M-Memo"], https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

technologies sweep up large amounts of data about individuals' lives and are often used by police to target racial justice protestors and other activists. Because of the acute threat that these technologies pose to First Amendment rights, their use for public surveillance should be prohibited, and any data collected through these means should be securely deleted to prevent any future exploitation or misuse that could result from retaining sensitive information.

Independent pre- and post-deployment audits of AI technologies used for law enforcement purposes should be required. Vendors to law enforcement agencies, such as those providing risk assessment tools, should be required to engage an independent auditor to conduct pre-deployment risk evaluations and annual post-deployment impact assessments designed to identify, prevent, and mitigate racial discrimination and other forms of bias in algorithmic technologies used for law enforcement purposes.[14] Vendors should provide independent auditors with the data they need to evaluate whether these systems are safe, effective, and nondiscriminatory based on their intended use. Outcomes of these audits must include the possibility of law enforcement not using this system or removing a system if it is already in use. Law enforcement agencies must not use these systems if they have not been evaluated. The outcome of such audits should be transparent and publicly accessible.[15]

Law enforcement use of AI technologies should be disclosed to defendants in criminal cases. To address the current lack of transparency around the use of AI in criminal proceedings, prosecutors and law enforcement should be required to promptly disclose all use of algorithmic technologies in criminal cases to defendants and defense attorneys. Prosecutors and law enforcement should provide this information to defendants and defense attorneys in clear and accessible plain language, and data should be available in machine-readable formats for easy analysis. Explanations must include sufficient information for an independent expert to evaluate whether such technologies cause racial discrimination. Additionally, prosecutors and law enforcement should keep defendants and defense attorneys reasonably apprised of any changes made to AI systems that might impact the outcome of their proceedings.

Thank you for your attention to and consideration of these recommendations. Please do not hesitate to contact Hauwa Ahmed (Senior Policy Analyst, Center for American Progress) at hahmed@americanprogress.org or Quinn Anex-Ries (Policy Associate, Lawyers' Committee for Civil Rights Under Law) at qanex-ries@lawyerscommittee.org if you have any questions.

Sincerely,

Asian Americans Advancing Justice - AAJC
Black Women's Roundtable
Center for American Progress
Color Of Change
Electronic Privacy Information Center (EPIC)
Fight for the Future

[14] The AI M-Memo, for instance, requires all agencies deploying safety- and rights-impacting AI, including law enforcement applications, to conduct similar pre-deployment impact assessments and post-deployment monitoring.
[15] *See* Lawyers' Committee for Civil Rights Under Law, *Online Civil Rights Act* (model legislation) § 102 (Dec. 2023), https://www.lawyerscommittee.org/wp-content/uploads/2023/12/LCCRUL-Model-AI-Bill.pdf.

Free Press
Government Information Watch
Kapor Center
Lawyers' Committee for Civil Rights Under Law
League of Women Voters of the United States
NAACP
National Coalition on Black Civic Participation
National Disability Rights Network
Secure Justice
Surveillance Technology Oversight Project (S.T.O.P.)