U.S. Commission on Civil Rights

Public Briefing: Civil Rights Implications of the Federal Use of Facial Recognition Technology

Friday, March 8th, 2024

Washington, DC

Submitted by:

Katie Kinsey
Chief of Staff/Technology Policy Counsel
The Policing Project at NYU School of Law
40 Washington Square South
New York, NY 10012

Thank you to the Commission for inviting me to testify on the topic of the civil rights implications of federal agency use of facial recognition technology (FRT).

My remarks today focus on the domestic federal law enforcement context. I want to make four overarching points:

(1) Facial recognition systems must be tested in real-world contexts to know how well or poorly they work, but this type of testing has not been conducted for law enforcement use.

(2) Federal law enforcement use of facial recognition suffers from a lack of transparency.

(3) Without transparency and real-world testing, it is impossible to evaluate any public safety benefit and understand the full scope of civil rights implications from law enforcement use of this technology.

(4) There is a better way: sound governance is necessary to ensure law enforcement use of facial recognition actually promotes public safety and protects people's civil rights.

I. Background for testimony

I am Chief of Staff and Technology Policy Counsel at the Policing Project, a nonprofit, nonpartisan center at New York University School of Law dedicated to promoting public safety through transparency, equity, and democratic accountability. We conduct research and also do work on the ground all over the country, with policing agencies and with the communities they serve, with the federal, state, and local governments, and with technology vendors, to promote democratically-accountable and equitable policing. Core to our mission is promoting "front-end, or democratic accountability," which means that there are democratically-ratified policies or regulations in place, *before* policing agencies use novel practices or emerging technologies, governing how they do so.[1]

Over the past several years, we have spent countless hours researching and discussing policing technologies with racial justice and civil liberties advocates, technologists, and law enforcement agencies themselves. Much of this work has focused specifically on facial recognition technology:

⇒ In 2021, we convened a series of closed-door conversations conducted under a modified Chatham House Rule, with a diverse set of stakeholders from civil society, law enforcement, and technology companies to discuss regulating law enforcement use of facial recognition. From these conversations, we developed several resources to guide lawmakers looking to develop regulation on this issue, including a federal legislative checklist that establishes a baseline of necessary regulatory safeguards.

⇒ From 2019–2022, we staffed the Axon AI Ethics Board, an independent review board that guided and advised Axon, the developer of TASERS and the country's largest producer of body-worn cameras, around ethical issues related to the development and deployment of AI-driven policing technologies. One of the Board's first major actions was to recommend that

[1] Our Mission, Policing Project, https://www.policingproject.org/our-mission.

Axon **not** develop facial recognition products for its body-worn cameras. Axon agreed to this recommendation and as a result, most police body-worn cameras do not have this capability today.

My remarks draw on our deep study and past work on policing technology and our fundamental belief that adoption and use of these tools must be guided by democratic legitimacy, a commitment to racial justice, and an imperative to minimize harm.

II. Facial recognition is untested in real-world law enforcement contexts

No matter what you might hear from other panelists today or read in press releases from facial recognition vendors, here's the truth: **there is *no* publicly-available, independent testing of facial recognition technology as it is actually used by law enforcement for criminal investigations**.

As we have explained in a research brief on this issue, without public, real-world testing, we do not know how well or poorly these systems perform. In its recent draft guidance on federal agency use of artificial intelligence (AI), the Office of Management and Budget likewise made clear that if federal agencies want to use AI like facial recognition, they "must conduct adequate testing to ensure the AI . . . will work in its intended real-world context," which means "[t]esting conditions should mirror as closely as possible the conditions in which the AI will be deployed."[2]

For facial recognition, real-world testing requires evaluating the entire facial recognition system – the computer software and the human operator – on the types and quality of images searched in the actual use context. Image quality alone has a major impact on facial recognition accuracy, with low-quality images producing much higher error rates.[3] Law enforcement face recognition searches often use low-resolution or grainy images from sources like CCTV cameras.[4] Today, there is no publicly available testing of actual law enforcement FRT systems and the photos they search.

Proponents of law enforcement use of facial recognition often claim that algorithm testing conducted by the National Institute of Standards and Technology (NIST) provides sufficient independent validation of system performance. This is false. Although NIST's testing provides an

[2] Shalanda D. Young, Office of Management and Budget, Proposed Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence § 5(c)(iv)(B) (Nov. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf [hereinafter "OMB Guidance"].

[3] *See, e.g.*, Patrick Grother et al., Face Recognition Technology Evaluation Part 2: Identification, NIST 8 (Feb. 21, 2024), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (explaining that image quality impacts error rates for face recognition algorithms and finding that "error rates are much higher, often in excess of 20% even with the more accurate algorithms" for lower quality images); *see also* 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 ("Poorer-quality images are known to contribute to mismatches.").

[4] *E.g.*, Jake Laperruque, Limiting Face Recognition Surveillance: Progress and Paths Forward, Ctr. for Democracy & Tech. (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward.

important benchmark of algorithms' technical capabilities, NIST doesn't test these algorithms on the actual, low-quality images used by law enforcement.[5]

To understand why NIST testing isn't sufficient, consider the testing required for another human-machine system: a Formula 1 racecar. NIST's algorithm testing would be the equivalent of just testing a Formula 1 car's engine in isolation. If you own a Formula 1 racecar, you might start with engine testing, but you don't stop there. You're also going to test how the engine performs in the actual car, with a driver, on a race track. In other words, you're going to test your racecar in real-world conditions.

When it comes to law enforcement use of facial recognition, this type of independent, real-world testing simply does not exist. Or if it does, it has not been made public. And without this kind of testing, there is no way for the public to know how accurate or biased these systems are for law enforcement use.

III. Federal law enforcement use of facial recognition suffers from a lack of transparency

Federal law enforcement agencies have rushed ahead to deploy facial recognition technology with little transparency. Despite over a decade of use and the allocation of tens of millions of taxpayer dollars by both the Department of Justice (DOJ) and Department of Homeland Security (DHS), the public lacks any comprehensive accounting of basic information about these agencies' use.[6] Fundamental questions – such as how often agencies run searches, for what types of crimes, on what demographics, and to what result – remain unanswered. What little public information does exist about federal law enforcement use stems largely – sometimes exclusively – from investigative reporting or is scattered across federal auditor reports – and not, as it should, from agencies' affirmative commitments to transparency, publicly available policies, or democratically-enacted legislation.

The FBI provides an instructive example. The Bureau started piloting FRT in 2011 and had a fully operational system by 2015.[7] Today, the FBI still has no publicly available use policy establishing the basic terms of its use. And despite a federal mandate to publicly disclose any uses of artificial

[5] *Cf.* Patrick Grother et al., Face Recognition Vendor Test Part 3: Demographic Effects, NIST 3 (Apr. 18, 2021), https://pages.nist.gov/frvt/reports/demographics/nistir_8280.pdf (observing that while its face recognition algorithm benchmark testing can be informative, there is a need to "specifically measure accuracy of the operational algorithm on the operational image data" to adequately assess accuracy).

[6] *See, e.g.*, U.S. Gov't Accountability Off., GAO-21-526, Facial Recognition Technology: Current and Planned Uses by Federal Agencies 59, 66 (Aug. 2021), https://www.gao.gov/assets/gao-21-526.pdf (reporting that DHS obligated over $70 million in funding for fiscal year 2020 for three of its FRT systems and FBI obligated $17 million for its biometrics contract which includes facial recognition services); Tonya Riley, Feds' spending on facial recognition tech expands, despite privacy concerns, CyberScoop (Jan. 10, 2022), https://cyberscoop.com/feds-spending-on-facial-recognition-tech-continues-unmitigated-despite-privacy-concerns (identifying over 20 federal law enforcement contracts totaling over $7 million that included facial recognition services).

[7] U.S. Gov't Accountability Off., GAO-19-579T, Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains 2 (June 2019), https://www.gao.gov/assets/gao-19-579t.pdf.

intelligence in an annual use case inventory, the FBI has never included its FRT system as part of these disclosures.[8]

A series of auditing reports from the U.S. Government Accountability Office (GAO), has revealed the following concerns:

- By 2016 – half a decade after its pilot began – the FBI had only limited information on the accuracy of its system and needed to "improve transparency and oversight to better safeguard privacy."[9]

- Three years later, a GAO follow-up audit found that the FBI still had not fully complied with its transparency and accuracy recommendations, despite having run over 200,000 searches on a database containing over 40 million photos from 2015-2019.[10]

- A 2020 audit found that the FBI – along with 12 other federal agencies that use FRT – had no way to track its employees' use of external FRT systems and as a result, could not "fully assess the risks of using these systems."[11]

- Just last year, another GAO audit found that the FBI lacked any policies or guidance "specific to facial recognition technology that address civil rights and civil liberties," and that only 5% of FBI staff members with access to the system had completed any training.[12]

To sum up, despite the fact that the FBI has dedicated millions of dollars to its facial recognition system and conducted hundreds of thousands of searches of a database containing over 40 million photos of American citizens, it has failed to comply with general federal privacy law requirements; hasn't adequately assessed the accuracy of its system; lacks any publicly available use policy or any policy whatsoever to protect citizens' civil rights and civil liberties; has failed to train the vast majority of its staff who have access to this system; and has no mechanism in place to track employee use of external FRT systems.

These transparency issues also extend to state and local agencies that receive significant federal funding for their facial recognition systems. Take Pinellas County, Florida as one example. In that

[8] *See* 2023 Guidance for AI Use Case Inventories, U.S. CIO, https://www.cio.gov/assets/resources/2023-Guidance-for-AI-Use-Case-Inventories.pdf (setting out guidelines for annual artificial intelligence use case inventory required by Executive Order 13960); AI Use Case Inventory Submission on Open Data, U.S. Dep't of Justice (2023), https://www.justice.gov/open/file/1305831/dl?inline=.

[9] U.S. Gov't Accountability Off., GAO-16-267, FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 18-19 (June 2016), https://www.gao.gov/products/gao-16-267.

[10] *See generally* U.S. Gov't Accountability Off., GAO-19-579T, Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains (June 2019), https://www.gao.gov/assets/gao-19-579t.pdf; U.S. Gov't Accountability Off., GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks 48 (June 2021), https://www.gao.gov/assets/gao-21-518.pdf.

[11] *See* GAO-21-518, *supra* note10, at 27-28.

[12] U.S. Gov't Accountability Off., GAO-23-105607, Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Polices for Civil Liberties (Sept. 2023), https://www.gao.gov/assets/gao-23-105607.pdf.

county, the sheriff's office has been running a facial recognition program for over 20 years.[13] The system initially was stood up with $3.5 million of federal funding and received a total of $15 million in federal grants through 2014.[14] Hundreds of law enforcement agencies have access to Pinellas' system which runs searches on a database containing "more than 30 million images, including driver's licenses, mug shots and juvenile booking photos."[15] Despite the longstanding use and significant cost of this program, the "most comprehensive" public accounting of this system's use comes from documents obtained through an open records request submitted by the *New York Times* and not agency policy or auditing.[16]

The lack of transparency over federal law enforcement use of facial recognition is undemocratic, and it erodes trust in law enforcement, which in turn hampers effective policing. The American Law Institute's Policing Principles put it plainly: transparency is both a "foundational value of democracy," and "essential to effective policing."[17] The President's Task Force on 21st Century Policing likewise emphasized that transparency in law enforcement is essential "to build public trust and legitimacy."[18] As the legal scholars who founded the Policing Project have explained, "without transparency there is no hope of democratic governance."[19]

IV. Without transparency and real-world testing, it is impossible to evaluate actual public safety benefit and understand the full civil rights implications of law enforcement's facial recognition use

At the Policing Project, our evaluation of any policing technology starts with a basic question: will the public benefit from the use of this tool? We start here because as any good economist would tell you in doing cost-benefit analysis, there is no need to evaluate costs until you are certain there are benefits. The problem with federal law enforcement use of facial recognition is that in the absence of transparency and real-world testing, we have no meaningful ability to determine the public safety benefits of this use. And deploying this technology without adequate proof of benefit simply is unacceptable – and a recipe for harm.

Of course, it is not hard to envision the potential benefits of law enforcement use of this technology. It promises to enable law enforcement to identify criminal suspects more quickly and efficiently.[20] There also is the promise that it might help exonerate the wrongly accused.[21] Proponents of facial

[13] 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.
[14] *Id.*
[15] *Id.*; Pinellas County Sheriff's Office, EFF, https://atlasofsurveillance.org/search?agency=Pinellas+County+Sheriff%27s+Office.
[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] Am. Law Instit., Principles of the Law, Policing § 1.05 Reporters' Notes, https://www.policingprinciples.org/wp-content/uploads/2023/01/Policing-Tentative-Draft_1-31-23.pdf.
[18] President's Task Force on 21st Century Policing, Final Report of the President's Task Force on 21st Century Policing, Dep't of Justice 12 (May 2015), https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.
[19] Barry Friedman & Maria Ponomarenko, Democratic Policing, 90 NYU L. Rev 1827, 1835 (2015).
[20] Nat'l Academies of Sciences, Engineering, & Medicine, Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance 15 (2024) [hereinafter "NAS Report"].
[21] Kashmir Hill, Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands, N.Y. Times (Sept. 18, 2022), https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html.

recognition technology are quick to provide specific anecdotes of successful use cases. By now we all have heard of federal agencies using this technology to identify individuals involved in the January 6, 2021 U.S. Capitol riots.[22] Vendors are especially wont to highlight their tool's successful use in sex trafficking or child exploitation cases.[23]

These examples are no doubt real and we should take seriously the claim about the value of facial recognition to solve serious crimes and facilitate exonerations. Law enforcement at all levels of government often face a difficult and exhausting task when they try to identify an unknown criminal suspect. Likewise defense attorneys – particularly those representing indigent clients – often have little time and even fewer resources to prove the innocence of their clients. A technology that could aid both tasks – finding the truly guilty, exonerating the truly innocent – should receive due consideration.

But the problem with these claimed benefits is that we only have isolated examples to support them, when what we truly need is representative data. In the absence of adequate transparency and testing, we have no idea if these handful of success stories represent the tip of the iceberg or the entire story. And the government should not be investing public resources in facial recognition – and risking individuals' civil rights and liberties – if it cannot gauge the expected benefits of use.[24]

Even though any decent economist would say we need not delve into costs on such an insufficient public record of benefits, we know that law enforcement use of facial recognition has caused real harm to individuals. And we know this despite the veil of secrecy that has defined law enforcement use of this technology. We and many others have written about these harms extensively and a subsequent panel will address them in depth so I will not belabor them here. The point is simple – whether it is false arrests that have only affected Black individuals; the chilling of First Amendment rights from police using facial recognition at protests; or due process concerns from failures to disclose facial recognition use to the accused – law enforcement use of this technology has come with real costs.[25]

V. Sound governance is needed

What is needed instead of the current opaque, rush-to-deploy model for law enforcement use of facial recognition is rigorous study, stepwise adoption, public accounting of this technology's benefits and costs, enforceable safeguards to mitigate risks to civil rights, racial justice, and civil liberties, and a commitment to abandoning systems and tools that do not advance public safety and

[22] *E.g.*, James Vincent, FBI used facial recognition to identify a Capitol Rioter from his girlfriend's Instagram posts, The Verge (Apr. 21, 2021), https://www.theverge.com/2021/4/21/22395323/fbi-facial-recognition-us-capital-riots-tracked-down-suspect.

[23] *E.g.*, Skylor Hearn, Clearview AI Powers Sex Trafficking Investigation That Takes Down a Most Wanted Man, Clearview AI (July 28, 2022), https://www.clearview.ai/post/clearview-ai-powers-sex-trafficking-investigation-that-takes-down-a-most-wanted-man; Child Exploitation, Clearview AI, https://www.clearview.ai/child-exploitation.

[24] OMB Guidance § 5(c)(iv)(A)(2).

[25] Tesfaye Negussie, Lawsuit: Man claims he was improperly arrested because of misuse of facial recognition technology, ABC News (Oct. 3, 2023), https://abcnews.go.com/US/lawsuit-man-claims-falsely-arrested-misuse-facial-recognition/story?id=103687845#:~:text=And%20we%20know%20that%20it,Black%20or%20African%2DAmerican%20people; GAO-21-518, *supra* note 8 at 17-18; Khari Johnson, The Hidden Role of Facial Recognition Tech in Many Arrests, WIRED (Mar. 7, 2022), https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests.

equity. In other words, what is needed is a model of sound governance that establishes rules, **on the front end**, for how police can and cannot use facial recognition.

The federal government is an essential locus for this work both because federal law enforcement agencies make extensive use of this technology and because there is a need for national standards and guidelines for appropriate use and evaluation. Luckily, Congress and federal agencies need not start from scratch. Good models establishing what sound governance of facial recognition requires already exist. They include the Policing Project's own federal legislative checklist; the OMB Guidance discussed above; and a recent Consensus Study Report from the National Academies on this very topic.[26] These resources contain sound policy solutions to the problems presented by the current unmitigated use of facial recognition. All that's left is for Congress and federal agencies to actually take action.

In the remainder of my remarks, I want to highlight a few key safeguards found in these models.

- **Democratic authorization**

Our checklist begins, as it must, with the requirement of democratic authorization for law enforcement use of facial recognition. As the National Academies study recognizes, there simply must be a federal regulatory framework in place for law enforcement use of facial recognition.[27] It is a significant failing of Congress that it has allowed federal agencies to use such a powerful technology with absolutely no specific legislative authorization.

- **Meaningful transparency**

Meaningful transparency is essential to support any evaluation of benefits and costs from use of FRT. To start, this means agencies must be required to develop publicly available use policies.[28]

It also requires careful data collection on, and disclosure of, agencies' facial recognition use so that the public gains answers to basic questions about use: how often, for what types of crimes, on which demographics, and to what result. This kind of record keeping is the only way we as a society will learn about the scope of benefits and impact.

And crucially, agencies must be required to disclose to the accused if and how facial recognition technology was used as part of an investigation or enforcement action.

- **Standardized, evidence-backed best practices for evaluation and use**

[26] I believe I am at liberty to say that although there was wide disagreement at our FRT convenings on the propriety of law enforcement using FRT, there was remarkable consensus around the inadequacies of current procedures and policies to protect basic rights, racial justice, or ensure simple accuracy of the technology. Our checklist builds on this consensus.
[27] NAS Report at 92-93.
[28] Use policies should describe authorized uses and users; authorized uses and users, training requirements, privacy protections, internal oversight mechanisms, audit processes, and penalties for misuse. Policies also should identify which vendors and software programs are being used.

Current law enforcement use of facial recognition is utterly lacking in standards and best practices. The absence of standards pervades the entire pipeline – from the designers and developers of the core technology, to law enforcement agency policies to training for the officers and prosecutors who rely on the technology. This choose-your-own-adventure approach makes no sense. A policing agency using FRT in Wichita, Kansas has the same interest in system accuracy and data security protection as does the LAPD. Similarly, best practices for reducing cognitive biases from human review of FRT results should guide the use of the technology no matter the jurisdiction.

In short, there is a need for national and industry-wide standards that dictate the development, use, testing, and analysis of this technology. Our checklist provides a number of suggestions for areas that would benefit from standards development. We also support the National Academies' recommendation calling on federal agencies like DOJ and DHS to engage in a "multi-disciplinary and multi-stakeholder" process to develop best practices and guidelines for safe and equitable use of facial recognition.[29] NAS has developed a comprehensive list of areas that would benefit from federal guidelines development, including appropriate and inappropriate uses, guidance for how FRT results are reported to analysts, standards and requirements for training and certification of human reviewers, and reporting and auditing requirements.[30]

- **Promoting best practices at state and local levels**

Although much of the work of standards and best practice development for law enforcement use of facial recognition should happen at the federal level, the policies and procedures developed from this process can and should extend beyond federal agencies. Law enforcement remains largely a creature of the states, with over 18,000 law enforcement agencies at the state and local levels compared to just 83 at the federal.[31] And many of these state and local agencies have been using facial recognition for years without any meaningful guidance. Although Congress may not be able to directly regulate state and local agencies as it can with federal law enforcement, the federal government has the ability to influence local agencies by requiring recipients of federal grants and support to adhere to requirements and best practices established though any federal standards-setting process.[32] By extending governance standards to federal grant recipients, the federal government can ensure state and local implementation of these best practices.

VI. Conclusion

At the Policing Project, we believe there is real promise for new technologies to promote public safety. We also believe that decisions to use any policing technology must be democratically accountable and supported by actual proof of benefit and a commitment to minimize harms to civil rights, civil rights, and racial justice. Protecting public safety and protecting civil rights are not mutually exclusive aims – they are, in fact, necessarily intwined. Federal law enforcement would do well to treat them as such. And federal policymakers can make sure they do.

---

[29] NAS Report at 5-6.
[30] *Id.*
[31] Duren Banks et al., National Sources of Law Enforcement Employment Data, Office of Justice Programs, U.S. Dep't of Justice (Apr. 2016), https://bjs.ojp.gov/content/pub/pdf/nsleed.pdf; Connor Brooks, Federal Law Enforcement Officers, 2016 – Statistical Tables, Office of Justice Programs, U.S. Dep't of Justice (Oct. 2019), https://bjs.ojp.gov/content/pub/pdf/fleo16st.pdf.
[32] *See* NAS Report at 5-6.