Policing Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

January 17, 2024

Submitted via email to office.of.legal.policy@usdoj.gov

Re: Request for comment on law enforcement agencies' use of facial recognition technology, other technologies using biometric information, and predictive algorithms, as well as data storage and access regarding such technologies pursuant to Executive Order 14074, Comments of Policing Project at New York University School of Law.

The Policing Project is a nonpartisan center at New York University School of Law dedicated to promoting public safety through transparency, equity, and democratic engagement. We submit this comment in response to the Department of Justice (DOJ) and the Department of Homeland Security's (DHS) request for comment to help inform the development of a report to the President that assesses law enforcement agencies' use of facial recognition technology, other technologies using biometric information, and predictive algorithms, as well as data storage and access regarding such technologies ("the Request").

Our comment makes three key points:

(1) DOJ/DHS should expand the scope of the Request beyond biometrics and person-based predictive algorithms to include place-based predictive algorithms and other advanced surveillance technologies that present similar privacy, civil rights, civil liberties, and racial justice concerns.

(2) Law enforcement use of advanced technologies suffers from a lack of transparency and front-end regulation, which has caused harm.

(3) The recent Office of Management and Budget Guidance on federal agency use of artificial intelligence presents a model of best practices and sound governance for law enforcement use of advanced technologies.

I. Background on the Policing Project

The Policing Project is a nonpartisan, nonprofit center at NYU School of Law. 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 venders, to promote democratically-accountable and equitable policing. Our mission is to promote "front-end accountability," which means that before policing agencies utilize novel practices or emerging technologies, there are democratically-ratified policies or regulations in place governing how they do so.

One of our primary focus areas is the use of emerging technologies by policing agencies. Increasingly, this means AI-powered tools and systems such as biometric technologies and predictive algorithms. We have spent countless hours researching and addressing these policing technologies, including with racial justice and civil liberties advocates, technologists, and policing agencies themselves. We have developed numerous resources dedicated to promoting the sound governance of biometric and algorithmic public safety technologies, from a model statute regulating automated license plate readers (ALPRs) to regulatory frameworks for police use of facial recognition technology (FRT). 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 advanced policing technologies.

Our Comment draws on our deep study and past work on policing technology and our fundamental belief that adoption and use of these tools must be transparent, democratically-legitimate, and guided by a commitment to racial justice, and to minimizing harm.

In addition, we have attached as an appendix two letters we wrote at the invitation of Justice Department officials following the issuance of Executive Order 14074 that contains recommendations for what the federal government can and should be doing regarding police use of surveillance technologies.

I. DOJ/DHS should expand the scope of the Request to include additional advanced policing technologies.

Although we welcome this opportunity to inform the development of a report to the President on law enforcement use of biometrics and predictive algorithms, we have two concerns with the scope of the Request. First, the list of covered technologies is too narrow. To be sure, law enforcement use of biometric technologies and predictive algorithms raises serious civil liberties, civil rights, and racial justice concerns. But these concerns are not unique to these policing technologies. Rather, there are many other policing technologies that likewise rely on mass data collection, are powered by AI algorithms, and are capable of surveillance and thus present parallel concerns.

In your report to the President on law enforcement technologies, we recommend that DOJ/DHS apply the selection criteria established in recent draft guidance on artificial intelligence (AI) from the Office of Management and Budget ("the OMB Guidance"), which classifies AI based on whether the technology facilitates a decision or action that could have a legal or material impact on an individual's or community's rights or safety.[1] According to this framework, OMB classifies not only biometrics and predictive algorithms but also license plate readers, social media monitoring, and AI-powered surveillance tools more broadly as presumptively "rights-impacting" or "safety-impacting."[2] OMB's focus on capability and impact – rather than discrete products – provides a more logical and flexible taxonomy and one that is designed to ensure safeguards are applied according to a technology's likelihood of causing harm.

Second, we also join our peers at the Brennan Center and the Project on Government Oversight in recommending that the Request expand its scope to include place-based predictive algorithms rather than just person-based ones. As they note, law enforcement uses the former more frequently, and both types of predictive algorithms raise serious civil rights, civil liberties, and racial justice concerns.

Although our comment is responsive to the technologies listed in the Request, we also intend it to apply more broadly to police use of other AI-powered surveillance technologies such as ALPRs, drones, robots, and place-based predictive algorithms.

[1] 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 (Nov. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf [hereinafter "OMB Guidance"].

[2] *See id.* Sec. 5(b).

II. Law enforcement use of advanced technologies suffers from a lack of transparency and front-end accountability, which has caused harm.

Law enforcement agencies have rushed ahead to use emerging technologies with little transparency and even less in the way of regulation or authoritative guidance on responsible use. This unfettered, often non-transparent use in a context as high-risk as law enforcement already has led to real harms to the public's civil rights and liberties – from false arrests to excessive use of force.[3] Such unauthorized, unregulated use also harms democratic legitimacy and undermines public trust. As the American Law Institute's Policing Principles explain, transparency is both a "foundational value of democracy" and "essential to effective policing."[4]

The Request asks whether we have "ever heard" of law enforcement agencies using certain biometric and predictive technologies. The answer is a resounding yes – to all the technologies listed. Unfortunately, our awareness and knowledge of this use stems largely, sometimes exclusively, from investigative reporting, or from our own work with policing agencies – and not, as it should, from agency transparency or any democratically-enacted legislation or publicly available policies.[5] For example, the most comprehensive public record of local and state law enforcement agencies' use of facial recognition technology to date comes from a 2016 report from Georgetown Law. After a year of study, including over 100 public records requests, this report found that half of all American adults were part of law enforcement face recognition databases and that at least a quarter of all state or local policing agencies could run FRT searches.[6] Despite this rampant use, there was not a single city, state, or federal law regulating law enforcement use of this technology.[7] Eight years later, this research report remains our best public accounting of law enforcement use of facial recognition and the statutory landscape remains nearly as sparse.

Federal law enforcement agencies' own technology transparency track record is no better. Sticking with facial recognition, the FBI provides an instructive example. The Bureau started piloting FRT in 2011 and had a fully operational system by 2015.[8] In 2016, a U.S. Government Accountability Office (GAO) audit found that the FBI had only limited information of the accuracy of its system and needed to "improve

[3] *See, e.g.*, 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/business/facial-recognition-false-arrest.html; (reporting on false arrests from law enforcement use of facial recognition technology); Vanessa Romo, No Charges for Colorado Officers Who Held Black Children at Gunpoint, NPR (Jan. 8, 2021), https://www.npr.org/2021/01/08/955165485/no-charges-for-colorado-officers-who-held-black-children-at-gunpoint, (reporting on officers holding family at gunpoint following ALPR misidentification).

[4] 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.

[5] *See, e.g.,* Jessica Pishko, The Impenetrable Program Transforming How Courts Treat DNA Evidence, Wired (Nov. 29, 2017), https://www.wired.com/story/trueallele-software-transforming-how-courts-treat-dna-evidence/ (law enforcement use of probabilistic genotyping); Andrew Pollack, Building a Face, and a Case, on DNA, N.Y. Times (Feb. 23, 2015), https://www.nytimes.com/2015/02/24/science/building-face-and-a-case-on-dna.html (law enforcement use of predictive phenotyping); Melissa Del Bosque, Prying Eyes: Border Sheriffs to Use Iris Scanning Tech in Push for 'Virtual Wall,' Texas Observer (July 12, 2017), https://www.texasobserver.org/prying-eyes-border-sheriffs-use-iris-scanning-tech-push-virtual-wall/ (law enforcement use of iris recognition); Cailtin Rearden, Forensic genealogy helping to solve some of the toughest cold cases, WFMZ (Dec. 4, 2023), https://www.wfmz.com/news/area/berks/forensic-genealogy-helping-to-solve-some-of-the-toughest-cold-cases/article_d1480c06-92fb-11ee-889d-f3e0f62a5760.html.

[6] *See generally* Clare Garvie et al., The Perpetual Line-Up, Ctr. on Privacy & Tech., Georgetown Law (Oct. 18, 2016), https://www.perpetuallineup.org.

[7] *Id.* at 2.

[8] 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.

transparency and oversight to better safeguard privacy."[9] In a 2019 follow-up audit, the FBI still had not fully complied with these transparency and accuracy recommendations.[10] 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. [11] In other words, despite the fact that the FBI has conducted hundreds of thousands of searches of a facial recognition database containing over 30 million photos of American citizens, it has no policy in place to protect these citizens' civil rights and civil liberties and the vast majority of the staff conducting these searches are untrained.[12]

The lack of transparency over federal law enforcement use of facial recognition extends beyond the FBI violations identified by GAO. DOJ likewise has failed to disclose various federal law enforcement agencies' use of facial recognition as part of its federally-mandated AI use case inventory.[13] Its most recent disclosure lists six AI uses cases, but not one mention of facial recognition use by the FBI, DEA, ATF, or U.S. Marshals even though federal auditors have reported significant use of this technology by each of these agencies.[14]

Despite the veil of secrecy that has defined law enforcement use of advanced technologies, we know that this use has caused harm. Law enforcement use of facial recognition has led to multiple false arrests – all of them of Black individuals.[15] These false arrests have had a cascade of negative consequences for these individuals: Porcha Woodruff, who was falsely arrested while eight months pregnant, had to go to the emergency room when the stress of being held in jail for eleven hours caused her to have contractions.[16] Michael Oliver, another victim of a facial recognition misidentification, lost his job as a result of his false arrest.[17] Officers in Colorado held a Black family at gunpoint after an ALPR false identified their car as stolen.[18]

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

[10] *See generally* U.S. Gov't Accountability Off., *supra* note 8.

[11] 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

[12] Facial Recognition Technology: Ensuring Transparency in Government Use: Hearing Before the House Oversight and Reform Committee (2019) (Statement of Kimberley J. Del Greco), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use#:~:text=The%20FBI%20FACE%20Services%20Unit,completed%20on%20December%2017%2C%202018; *see* U.S. Gov't Accountability Off., *supra* note 11.

[13] EO 13960: Artificial Intelligence (AI) Use Case Inventories: Guidance for Creating Agency Inventories of AI Use Cases, U.S. Chief Information Officers Council (2023), https://www.cio.gov/assets/resources/2023-Guidance-for-AI-Use-Case-Inventories.pdf.

[14] AI Use Case Inventory Submission on Open Data, U.S. Dep't of Justice (2023), https://www.justice.gov/media/1305831/dl?inline; U.S. Gov't Accountability Off., *supra* note 11.

[15] 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.

[16] Amy Goodman, Meet Porcha Woodruff, Detroit Woman Jailed While 8 Months Pregnant After False AI Facial Recognition, Democracy Now! (Aug. 9, 2023), https://www.democracynow.org/2023/8/9/porcha_woodruff_false_facial_recognition_arrest.

[17] Khari Johnson, How Wrongful Arrests Based on AI Derailed 3 Men's Lives, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives.

[18] Romo, *supra* note 3.

In addition to these individual harms, the unauthorized, unregulated, non-transparent use of these technologies also further erodes community trust in law enforcement. People are distrustful when surveillance technologies are used without transparency and rules. This is only natural. And trust is the currency of effective law enforcement in a democracy.[19]

What is needed instead of the current secretive, rush-to-deploy model for law enforcement use of advanced technologies like biometrics and predictives is rigorous study, stepwise adoption, public accounting of these technologies' 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 equity. In other words, what is needed is a model of sound governance that ensures access to information and transparency over public agency uses and establishes rules, **on the front end**, for how police can and cannot use these tools.

III. The OMB Guidance presents a model of best practices and sound governance for law enforcement use of advanced technologies.

The bottom line is that advanced policing technologies like biometrics and predictive algorithms simply should not be used without regulatory frameworks in place – on the front-end – that impose strict controls around their use and ensures that they serve communities, particularly historically marginalized communities and specifically Black communities.

OMB's recent proposed guidance for federal agency use of AI-powered technologies provides a model of sound governance for law enforcement use of advanced technologies whether they rely on AI or not. In this section, we highlight some of the key OMB Guidance safeguards that would help ensure law enforcement use of these technologies promotes public safety while protecting people's civil rights and liberties.

- A commitment to benefit-cost analysis and proof of efficacy

At the Policing Project, our evaluation of any law enforcement technology starts with a basic question: will the public benefit from the use of this tool? It is a bedrock principle of cost-benefit analysis that before one even considers the costs of government action, the burden is on government to show there is some identifiable, concrete benefit that will be obtained. The OMB Guidance implements this analysis by requiring federal agencies to articulate the "expected benefit" of any rights- or -safety-impacting AI and to demonstrate this benefit through "quantifiable measures."[20]

Agencies are required to prove up the benefits of any covered technology by testing it in "real-world context[s]" and through independent evaluation.[21] As we have explained in a white paper on evaluating law enforcement use of facial recognition technology, testing technologies as they actually are used in the real world is essential to know if they work or not. Crucially, the OMB Guidance recognizes that technological performance is not static but needs to be measured and monitored repeatedly.[22] And the OMB Guidance does not just talk the talk of benefit-cost analysis; rather it follows its demands to its logical and necessary

[19] *See, e.g.*, Final Report, President's Task Force on 21st Century Policing 1 (2015), https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf ("Trust between law enforcement agencies and the people they protect and serve is essential in a democracy. It is key to the stability of our communities, the integrity of our criminal justice system, and the safe and effective delivery of policing services.").
[20] OMB Guidance, *supra* note 1, Sec. 5(c)(iv)(A)(1).
[21] *Id.* Sec. 5(c)(iv)(B)(C).
[22] *Id.* Sec. 5(c)(iv)(D).

conclusion by requiring agencies to stop use of any rights- or safety-impacting technology if its benefits and efficacy cannot be proven.[23]

These are exactly the sorts of requirements that law enforcement use of biometrics, predictive algorithms, and other advanced technologies should have to meet: proof of benefit and efficacy and a commitment to stop use in their absence. OMB has provided the map, DOJ and DHS just need to make sure their law enforcement agencies follow it.

- Meaningful transparency

As noted above, transparency is essential to both democratic legitimacy and effective policing. The OMB Guidance's commitment to transparency is apparent in various provisions. For example, prior to deploying any technology, agencies must document the intended uses, benefits, risks and any data used to design or operate these tools in an impact assessment.[24] Agencies also must document the test methods and results of all system evaluations.[25] Perhaps most importantly, agencies are required to disclose their use of technology to the public through a "use case inventory" which is intended to "serve[] as adequately detailed and generally accessible documentation of the system's functionality."[26] This kind of thorough documentation and public disclosure of use are essential to the sound governance of law enforcement agency use of advanced technologies.

In addition to the transparency safeguards found in the OMB Guidance, we recommend that DOJ/DHS consider one more requirement for law enforcement agencies. All agencies that use or access advanced technologies should be required to draft and publicly disclose use policies. Often the best way to maximize the benefits of a technology, while minimizing harms, is by setting clear rules on how the technology is used and disclosing the use policies to the public. Among other things, these policies should include provisions describing authorized uses and users, training requirements, privacy protections, internal oversight mechanisms, audit processes, and penalties for misuse. They should be attentive to the harms of the technology, especially privacy and racial harms. They also should identify which vendors and software programs are being used. And crucially, these policies should require agencies to disclose to the accused any time a surveillance technology was used as part of an enforcement action.

- A commitment to equity and empowering public voice

The OMB Guidance reflects two commitments that should be at the center of law enforcement adoption and use of advanced surveillance technologies: equity and public voice. The OMB Guidance instantiates these values by requiring agencies to report additional details in the use case inventory about any risks to equity and how they are managing those risks and by imposing additional safeguards on rights-impacting AI that are designed to "advance equity, dignity, and fairness."[27] One of these key additional requirements is that agencies must "[c]onsult and incorporate feedback from affected groups," including underserved communities, in decisions to acquire and use rights-impacting AI.[28] This heightened focus on risks to equity and a requirement to consult impacted communities represent best practices that should apply to any law enforcement decisions to acquire and use advanced surveillance technologies.

[23] *Id.* Sec. 5(c).
[24] *Id.* Sec. 5(c)(iv)(A).
[25] *Id.* Sec. 5(c)(iv)(B)(C).
[26] *Id.* Sec. 5(c)(iv)(H).
[27] *Id.* Sec. 5(c)(v).
[28] *Id.* Sec. 5(c)(v)(B).

Thank you for the opportunity to comment.

Respectfully submitted,

Barry Friedman
Founder and Faculty Director

Max Isaacs
Senior Staff Attorney

Katie Kinsey
Chief of Staff and Tech Policy Counsel

APPENDIX

Policing Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

June 29, 2022

Vanita Gupta, Associate Attorney General
U.S. Department of Justice
950 Pennsylvania Ave. NW
Washington, D.C. 20530

Dear Vanita,

This letter (belatedly) takes you up on your invitation to submit suggestions about what the federal government can and should be doing regarding police use of surveillance technologies. Thank you for allowing us this opportunity. We had it ready a while ago, but wanted to take in and incorporate President Biden's recent Executive Order on policing.

Although there has been important federal attention given to aspects of policing, such as use of force, officer misconduct, and data collection, that has not been the case regarding surveillance technologies. Yet, the fact is that recent years have seen unprecedented growth in the use of these technologies by federal, state, and local agencies. These technologies are slowly but steadily changing the way policing occurs, with detrimental impacts already being felt by many, particularly those in highly-policed communities.

Take automated license plate readers (or "ALPRs") as an example. This technology once was so costly that even major metropolitan police departments could afford only a few, and therefore directed those they had toward serious crimes involving vehicles. Now, any camera — every dash cam, body cam, and CCTV— can be used as an ALPR.[1] The technology has become so widespread that it allows police to issue citations en masse for expired registration or lapsed insurance.[2] Some agencies use ALPRs to track "gang-affiliated" license plates, enabling the use of pretextual traffic stops to target those drivers.[3] Smaller agencies and jurisdictions geo-fence their communities, creating an log of all incoming and outgoing traffic.[4] Much of this occurs without any express democratic authorization. And ALPRs are only the tip of the surveillance technology iceberg — an iceberg that includes facial recognition, cell site simulators, mobile forensic data terminals, and much, much more.

[1] For example, Rekor, a leading ALPR vendor, has developed a software program which "enables accurate automatic license plate and vehicle recognition on nearly any IP, traffic, or security camera." *See Rekor Scout*, Rekor, https://www.openalpr.com/software/scout (last visited June 17, 2022).

[2] Okla. Stat. §§ 47-4-606.1 (authorizing use of ALPRs to enforce state compulsory insurance law).

[3] *See Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Ctr. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.

[4] Flock Safety, another ALPR vendor, markets this capability to communities as a "virtual gate." *See Flock Safety Secures This South Carolina "Beautiful Peninsula with a Virtual Gate*, Flock Safety (Mar. 10, 2020), https://www.flocksafety.com/articles/tega-cay-virtual-gate.

The failure to regulate use of these technologies properly — or even to require minimal transparency about their use — has had a number of ill effects. There have been documented instances of inappropriate surveillance, including the targeting of Black and brown communities.[5] This has bred understandable mistrust in heavily-policed communities (and, frankly, well beyond them). And it has engendered backlash that in some instances has resulted in outright bans on certain technologies — denying police the use of tools that, if properly regulated, might prove beneficial to public safety.[6] In other cases, court proceedings have been jeopardized because of the lack of appropriate disclosure of surveillance by prosecutors.[7]

President Biden's recent Executive Order takes some of the most significant steps in recent memory regarding surveillance technology. Section 13 of the Order addresses body-worn cameras and certain advanced law enforcement technologies. The National Academy of Sciences study and the subsequent interagency process regarding facial recognition, biometric technologies, and predictive algorithms, strikes us as particularly important. But still there is much more to be done, and federal leadership is desperately needed.

What follows is a short list of steps we believe to be imperative for the federal government to take around surveillance technologies. We would be happy to discuss these with you or any other government officials. We cannot stress enough how overdue some of these measures are.

Inventory – A recent Government Accountability Office report made clear that many federal law enforcement agencies either were altogether unaware that their officers were using facial recognition or were unaware of what system was being used.[8] Any efforts in this area should begin with a directive to federal law enforcement agencies to inventory the surveillance tools and tactics they use.

Policy – No agency should be using a surveillance tool or tactic without a written policy governing its use. Policies should have some uniformity across agencies and ideally would be developed with input from outside stakeholders. There are many things that might go into such policies, but at a

[5] *See* Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html; Antonia Noori Farzan, *Memphis Police Used Fake Facebook Account to Monitor Black Lives Matter, Trial Reveals*, WASH. POST (Aug. 23, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals; Matt Apuzzo & Adam Goldman, *After Spying on Muslims, New York Police Agree to Greater Oversight*, N.Y. TIMES (Mar. 6, 2017), https://www.nytimes.com/2017/03/06/nyregion/nypd-spying-muslims-surveillance-lawsuit.html. *See generally* Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FDN. (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance.

[6] *See* Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 7, 2013), https://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program/.

[7] See Nicky Woolf, *2,000 Cases May Be Overturned Because Police Used Secret Stingray Surveillance*, GUARDIAN (Sept. 4, 2015), https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance.

[8] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, FACIAL RECOGNITION TECHNOLOGY, FEDERAL LAW ENFORCEMENT AGENCIES SHOULD BETTER ASSESS PRIVACY AND OTHER RISKS (2021), https://www.gao.gov/assets/gao-21-518.pdf.

minimum they should include: permissible and prohibited use cases, training on use, supervisor approval for some sensitive uses, relevant protections to guard against racial disparity or violations of civil liberties (such as prohibitions on using the technologies at lawful protests, on the basis of protected characteristics, or in a manner that leads to avoidable racial disparities), data retention and deletion practices, data security, procedures for disclosure to defense counsel, and more. We think the Knowledge Lab could play an important role here, and we at the Policing Project would be more than happy to assist.

Transparency – Once agencies have inventoried what tools they use and set policies to govern their use, they then should make at least some (if not all) of these terms public. We understand the need for secrecy in ongoing investigations but we are deeply skeptical that the government needs to or should keep the fact of using certain tools from the public. Even if we are wrong in this — and we would welcome engaging on the matter and learning where we err — a decision to keep a particular technology from public view only should be made at the very highest levels of government, and for the most compelling of reasons. The failure of police to disclose their use of cell-site simulator technology (i.e., "Stingrays") became a scandal in some jurisdictions.[9] There is room for debate about precisely what information agencies should disclose — but this is a debate worth having, and would be a monumental improvement over how most agencies (federal, state, and local) operate today. The federal government should set an example for law enforcement agencies nationwide.

Law Enforcement Databases – The federal government maintains a variety of law enforcement databases, including the National Crime Information Center (NCIC), Next Generation Identification (NGI), the Law Enforcement Enterprise Portal (LEEP), DHS's Automated Targeting System (ATS), and many others. Much of that information is collected in collaboration with state and local agencies, often without clear democratic authorization to do so. The information then is disseminated widely, often through the fusion center network, which itself operates with inadequate transparency. There is reason to believe that much of that information is stale or inaccurate.[10] The consequences of being in such a database can be devastating for individuals, leading to stops by law enforcement officials — stops which disproportionately affect minority populations. The federal government should invite an evaluation of these databases by the Inspector Generals of relevant departments. Such an evaluation should include the legal bases for authorization to maintain the databases and the particular information in them, as well as an audit of the accuracy of the records those databases contain.

Funding – The above measures apply directly to the federal government. But the fact of the matter is that federal agencies have through grants — both public and undisclosed — facilitated a troubling use of technologies by state and local agencies. DHS Homeland Security Grants, for example, have funded the acquisition of license plate readers for use by small departments in

[9] *See, e.g.*, Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[10] *See* U.S. SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS, CMTE. ON HOMELAND SEC. AND GOV'T AFFAIRS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 101 (2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

localities that are nowhere near likely terrorism targets.[11] The federal government should begin by (a) taking inventory of the funding it presently is providing for surveillance technologies, (b) making that information public, and (c) providing training and model policies on how these technologies can be used in ways that are respectful of civil rights and civil liberties. It would be appropriate to go further and ensure future grants do not undermine democratic accountability by requiring approval by a jurisdiction's elected representatives prior to accepting such grants (much as should occur around militarized equipment that agencies obtain through the Department of Defense's Law Enforcement Support Office (LESO) Program (aka the 1033 Program).

As we said, the recent Executive Order on biometric and predictive technologies is an important start, but we hope we have persuaded you more is needed.

Thank you for your willingness to entertain these suggestions. We would be available to discuss any of them, or participate in any stakeholder consultation about what proper federal policy and practice should be.

Sincerely,

Barry Friedman
Jacob D. Fuchsberg Professor of Law
Affiliated Professor of Politics
Faculty Director, Policing Project
New York University School of Law

Farhang Heydari
Executive Director, Policing Project
New York University School of Law

[11] *See, e.g.*, Rosemond Crown, *Bell County: Sheriff's Dept. Uses Grant to Purchase License Plate Reader*, KWTX (Mar. 18, 2021), https://www.kwtx.com/2021/03/18/bell-county-sheriffs-dept-uses-grant-to-purchase-license-plate-reader.

Policing
Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

December 5, 2022

Catherine Crump
Domestic Policy Council
Catherine.N.Crump@who.eop.gov

Dear Catherine,

This letter takes you up on your invitation to submit suggestions about what the federal government can and should be doing regarding policing. Thank you for allowing us this opportunity. As we discussed, the focus of this letter will primarily be on: (I) police traffic enforcement, and (II) police use of technology and data.

I. Police Traffic Enforcement

Our country faces a public health crisis on our roadways. Road deaths, always a persistent national problem, have spiked to rates not seen in decades. Pedestrian and bicyclist deaths have increased dramatically as well. The United States is an outlier among similarly wealthy nations. This year, more Americans will die in traffic crashes than by gun violence. More children have died on the roads in the past two years than in the school shootings of the past two decades. This toll falls disproportionately on Black, Hispanic, and Native American communities.

But the central pillar of our national response to this public health crisis is a tactic that is in many respects perverse. Rather than focusing on the interventions that been proven to increase traffic safety, notably road and vehicle design, the federal government too often has promoted a tactic drawn from criminal law enforcement: frequent traffic stops. This tactic is relatively unproven in the context of traffic safety. And it involves substantial social costs. These costs include vast resource expenditures, such as officer time, but also resultant social harms such as the impact of fines and fees, racial profiling, and the death or injury of officers and members of the public in the course of encounters stemming from traffic enforcement, among others.

There is much the federal government can (and should) do in this space. Below we outline a few suggestions focused on DOT and DOJ:

Near Term

1. **End DOT and DOJ Support for Pretextual Traffic Stops.** As outlined in Farhang Heydari's draft law review article, *The Invisible Driver of Pretextual Policing*, the DOT has for decades supported the use of traffic stops as a crime fighting tool, in the process both undermining the agency's traffic safety mission and imposing substantial social harms. The White House should compel DOT to end its various programs that support the use of traffic stops as crime fighting tool (e.g., DDACTS). The DOJ likewise should

reevaluate its practices. Not only are BJA and NIJ supporters of DDACTS, but agencies have used DOJ funding for DDACTS implementation.

2. **Data Transparency Regarding Traffic Stops.** Each year, NHTSA and DOT administer hundreds of millions of dollars in grants, a significant portion of which make their way to local policing agencies. But details are difficult to come by. The White House should require DOT to track and publish how much federal funding flows to which state and local policing agencies. Then, encourage, if not require, funding recipients to report far more extensive data (e.g., demographics of people stopped; enforcement data, forfeiture data).

3. **Equitable Sharing.** Financial incentives undergird police use of traffic stops, with asset forfeiture being a significant aspect of this problem. The White House should minimize the extent to which the federal government contributes to this program by revising the Equitable Sharing program, which allows assets seized by state and local law enforcement to become subject to federal civil forfeiture law—thereby circumventing state law limits. Basic revisions should include:
   - Prohibiting federal adoption of forfeitures from activities in which federal law enforcement is not involved;
   - Allowing forfeiture funds to supplant locally provided budgets to law enforcement agencies (not just in addition to) so that communities can take advantage of funds acquired from forfeitures to finance others public safety purposes beyond policing;
   - Prohibiting the use of forfeited funds for particular controversial policing tactics (e.g., "buy" money, payments to informants, electronic surveillance equipment, weapons); and
   - Prohibiting any agency from receiving a greater share of proceeds from asset forfeiture than they would be permitted to receive directly under state law (which in some cases is none).

Medium to Long Term

4. **New Metrics for DOT Funding.** Earlier this year, NHTSA and the DOT issued a notice of proposed rulemaking indicating it may reconsider reporting conditions attached to annual Highway Safety Funding (23 U.S.C. 402). At present, hundreds of millions of dollars flow annually to states and localities in ways that subsidize police patrol and require police to count and report stops and tickets. This approach fuels an over-enforcement of traffic violations without regard to whether the enforcement actually improves road safety or whether its impact falls disparately on certain populations. The outcome of this proposed rulemaking is therefore critical, and we recommend the White House keep in close contact with this process.

5. **Bipartisan Infrastructure Bill Funding.** As a result of the recent bipartisan infrastructure bill, over the next five years, the DOT will dole out billions of dollars to states and cities. Some of this funding will go to creating and implementing traffic safety plans. It is essential that this funding not be used primarily for police traffic enforcement, and especially that it not be used to support pretextual traffic stops. To date, we have seen no DOT guidance on these issues. DOT should be far more explicit in its guidance when making these grants, and in collecting data to assess the impact of its funding.

6. **The "Cost" of a Traffic Stop**. Other fields—most notably, environmental justice—have created processes to standardize the way that we compare the costs of seemingly disparate programs. The "cost of carbon" is one example. At present, no federal agency does much of anything to measure the social costs of traffic stops (by "costs" we include everything form officer time and injuries to racial disparities), let alone in a way that would allow comparisons across policing tactics. The White House should initiate an inter-agency process to begin to create just such a standard—one that can be incorporated into future guidance across the executive branch (from DOT to federal law enforcement agencies).

II. Police Technology and Data

Although there has been important federal attention given to aspects of policing—such as use of force, officer misconduct, and data collection—that has not been the case regarding surveillance technologies. Yet, the fact is that recent years have seen unprecedented growth in the use of these technologies by federal, state, and local agencies. These technologies are slowly but steadily changing the way policing occurs, with detrimental impacts already being felt by many, particularly those in highly-policed communities.

The failure to regulate use of these technologies properly—or even to require minimal transparency about their use—has had a number of ill effects. There have been documented instances of inappropriate surveillance, including the targeting of Black and brown communities. This has bred understandable mistrust in heavily-policed communities (and, frankly, well beyond them). And it has engendered backlash that in some instances has resulted in outright bans on certain technologies—denying police the use of tools that, if properly regulated, might prove beneficial to public safety. In other cases, court proceedings have been jeopardized because of the lack of appropriate disclosure of surveillance by prosecutors.

President Biden's recent Executive Order takes some of the most significant steps in recent memory regarding surveillance technology. Section 13 of the Order addresses body-worn cameras and certain advanced law enforcement technologies. The National Academy of Sciences study and the subsequent interagency process regarding facial recognition, biometric technologies, and predictive algorithms, strikes us as particularly important. But still there is much more to be done, and federal leadership is desperately needed.

What follows is a short list of steps we believe to be imperative for the federal government to take around police technology and data. We would be happy to discuss these with you or any other government officials.

7. **Basic Transparency Regarding Surveillance Tech.** By executive order or otherwise, require that all federal agencies inventory the surveillance technologies they use and make public most (if not all) that are used in connection with domestic law enforcement. Require agencies do the same for any policies they have governing use of these technologies.

8. **Standardize Use Policies.** By EO or otherwise, create a task force to develop a unified set of policies for any federal use of common surveillance technologies (e.g., license plate readers, facial recognition, stingrays). This task force should include a range of stakeholders, including law enforcement, advocates from civil liberties and racial justice organizations, and individuals from affected communities.

9. **Federal Impact on Local Surveillance.** Require all federal agencies to (a) take inventory of the funding the agency has or is providing for non-federal entities to acquire surveillance technologies, (b) make that information public, and (c) provide training and model policies on how these technologies can be used in ways that are respectful of civil rights, civil liberties, and racial justice.

10. **Rein in DEA Provision of ALPRS to Local Agencies.** The DEA's National License Plate Reader Program is a federation of federal, state, local, and tribal law enforcement license plate readers—many purchased with federal dollars—linked into a cooperative system. The purpose of the system is ostensibly to interdict drug traffickers. Although there is much we do not know about the program, we have grave concerns that the program is outside of the DEA's statutory authority. But short of ending or securing legislative authorization for this program, we urge an evaluation of mission creep—to what extent are the local ALPRs that DEA funds being used for low-level criminal enforcement, as opposed to drug interdiction that is part of the DEA's mission? Answering this question would go a long way toward knowing how concerned we should be about this program.

11. **Normalize and Facilitate Real World Accuracy and Bias Testing of Facial Recognition Technology**. Advanced surveillance technologies—especially biometrics like FRT—must be proven to work in the real world, as they actually are used by law enforcement. The federal government should be leading in developing standards, best practices, and evaluation models for real world use of these technologies. One way to achieve this would be to empower and fund NIST to expand its current biometric testing program to include more real-world scenarios and data that better matches law enforcement use (e.g., testing FRT systems on lower quality surveillance camera images).

12. **Develop National Standards Around Forensics.** Facial recognition is top of mind for many, but other forensics technologies also require significant training, expertise, and standards to ensure sound use. To build such standards around forensics, the White House should reinstate the National Commission on Forensic Science, which was working to develop evidence-backed national standards for forensics and oversight mechanisms.

13. **Federal Gang Information:** The federal government currently uses lax criteria to label a person as a gang member within NCIC. (And states and localities mirror these lax practices in their own databases.) We suggest narrowing the criteria for inclusion in the NCIC's Gang File by, at a minimum, eliminating the following criteria: "Frequents a gang's area, associates with known members, and/or affects gang dress, tattoos, or hand signals." We would also limit the extent to which "self-admission" qualifies, particular when such admissions occur by youth on social media.

14. **Federal Audit of Funding for Gang Databases and Fusion Centers.** 28 C.F.R. Chapter 1, Part 23 sets forth policy standards applicable to all criminal intelligence systems (e.g., gang databases, fusion center databases) that are supported by funding under the Crime Control Act. Among the standards are requirements that funding recipients (a) only collect such information if they have reasonable suspicion that a person is involved in criminal activity and the information is relevant to that activity, and (b) disseminate information only to law enforcement authorities that agree to follow security/dissemination procedures consistent with the principles of the regulation. 28 C.F.R. § 23.20. In the context of gang databases and fusion centers in particular, there are ample media reports pointing to repeated violations of these terms. The White House should initiate a process to evaluate enforcement of its policy standards when it comes to its funding decisions and maintenance (awards require compliance with the § 23.20 standards), regulatory audits (*see* 28 C.F.R. § 23.40(b)), and assessing statutory fines for violations of the § 23.20 standards pursuant to 34 U.S.C. § 10231(d)).

We are of course aware that some of these issues may be addressed through the Working Group on Criminal Justice Statistics, created by President Biden's Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety. We welcome any role on this or any other process you feel would benefit from our input.

Thank you again for your willingness to hear our suggestions.

Best regards,

Barry Friedman
Jacob D. Fuchsberg Professor of Law
Affiliated Professor of Politics
Faculty Director, Policing Project
New York University School of Law

Farhang Heydari
Legal Director, Policing Project
New York University School of Law