epic.org

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

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. Department of Justice and Department of Homeland Security

Request for Written Submissions on

Section 13(e) of EO 14074

January 19, 2024

The Electronic Privacy Information Center (EPIC) submits these comments in response to the 2023 Guidance for Written Comments released by the Department of Justice (DOJ) and the Department of Homeland Security (DHS) to inform 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, and that safeguards privacy, civil rights, and civil liberties, as required by EO 14074. EPIC firmly believes that certain technology—such as facial recognition technology—should not be used at all for surveillance. EPIC also firmly believes that any use of these other technologies—such as DNA biometric technologies—must be based on a robust framework of safeguards that are present prior to any use and that are effectively enforced. As DOJ and DHS continue to review law enforcement use of these technologies, EPIC renews our call to protect privacy, civil rights, and civil liberties.

I. Interest of EPIC

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[1] EPIC has a particular interest in accountability, fairness, privacy, civil rights, and civil liberties in the context of surveillance and algorithm-powered technologies and related law enforcement techniques.[2] EPIC also has a long history of advocating for increased privacy protections for non-citizens and opposing the expansion of surveillance at the border.[3]

II. There are overarching issues of transparency, accountability, and oversight across multiple technologies deployed by law enforcement agencies, necessitating a need for a set of principles to ensure the protection of people's privacy, civil liberties, and civil rights.

Due to the risk of DOJ and DHS inconsistently exercising adequate oversight of law enforcement agencies' use of surveillance technology, including the agencies' own grantees, DOJ

[1] EPIC, *About Us* (2023), https://epic.org/about/.

[2] *See* EPIC Comments to OSTP on Public and Private Sector Uses of Biometric Technologies (Jan. 15, 2022), https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-uses-of-biometric-technologies/; EPIC Comments to the U.S. Postal Investigative Service on Using U.S.P.S. Customer Data for Law Enforcement (Jan. 18, 2022), https://epic.org/documents/epic-comments-to-the-u-s-postal-investigative-service-on-using-u-s-p-s-customer-data-for-law-enforcement/; EPIC Letter to Attorney General Garland Re: ShotSpotter Title VI Compliance (Sept. 27, 2023), https://epic.org/documents/epic-letter-to-attorney-general-garland-re-shotspotter-title-vi-compliance/.

[3] Dana Khabbaz, DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information (Aug. 2022), https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/; EPIC Comments to DHS: Advance Collection of Photos at the Border (Nov. 29, 2021), https://epic.org/documents/epic-comments-to-dhs-advance-collection-of-photos-at-the-border/; EPIC Comments to DHS on Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States (Dec. 21, 2023), https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/.

and DHS must implement stronger mechanisms for ensuring safeguards to protect privacy, civil rights, and civil liberties, and for strengthening American trust in our public institutions. Law enforcement agencies do not have the best track record for waiting until a technology has been validated before using it.[4] More robust legal process is required as guardrails for surveillance and analysis technologies, to prevent government agencies from capitalizing on a generally non-tech-savvy judiciary and ineffective legislature at the expense of defendants. Greater transparency and accountability will also be necessary.

The lack of a comprehensive federal privacy law, the failure of criminal procedure caselaw to keep pace with technological developments, and the purposeful lack of transparency and denial of informed community buy-in means that new methods of surveillance often gain a foothold without adequate external oversight.[5] This is a problem both in terms of law enforcement agencies taking advantage of a legal vacuum to push new surveillance activities without proper safeguards, and in terms of legal processes failing to close the gaps created by technological advances—even where potential civil rights issues are clear. While DOJ, DHS, and other agencies have published some interim policies on the use of particular technologies, these policies—and agencies' implementation

[4] *See, e.g.*, Excerpt, John F. Kelly & Phillip K. Wearne, *Tainting Evidence: Inside the Scandals at the FBI Crime Lab* (1998), *available at* https://archive.nytimes.com/www.nytimes.com/books/first/k/kelly-evidence.html ("Only when scientists from other fields challenged the spectrograph research and a major scientific controversy erupted did the FBI ask the National Academy of Sciences (NAS) to review voiceprint technology. An NAS evaluation committee quickly concluded that the theory had not been validated. Yet, incredibly, many courts continued to allow the admissibility of voiceprints long after the NAS study had been published."); Joseph Goldstein, *Guilty Until Proven Innocent: The Failure of DNA Evidence*, 12 Drexel L. Rev. 597, 614–15 (2020) (internal citations omitted) (recounting examples of "other 'new' evidentiary techniques that have come and gone the way of fallibility" including ballistics, polygraph testing, blood splatter, and burn pattern analysis, "[a]ll [of which] have been revealed to be vulnerable to varying degrees to the human biases they were meant to inoculate against.").

[5] Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. Rev. 1491, 1545–46 (2015) ("…even if policymakers would be interested in regulating a particular surveillance method, they are often not notified of new techniques in advance, leaving the new methods to gain a foothold absent external oversight.").

of those policies—has proven to be manifestly inadequate to protect privacy, civil rights, and civil liberties.

Some technologies should never be deployed without adherence to these principles, if at all, which we discuss in greater detail below. Irrespective of the specific technology involved, the DOJ is tasked with protecting civil rights.[6] Additionally, EO 14074 requires DOJ and DHS to identify best practices specifically addressing safeguards for privacy, civil rights, civil liberties, regular assessments for accuracy and for disparate impact, and consistency with respect to the dignity and rights of all persons and with fair and impartial justice.[7] As such, DOJ and DHS must require that any organization collecting, handling, storing, and transmitting data from surveillance or analytics technologies including but not limited to facial recognition technology, predictive policing algorithms, social media surveillance, and DNA analysis adhere to a new set of principles to safeguard people's privacy, civil liberties, and civil rights, while strengthening public trust in its law enforcement agencies. Adherence to these principles should be required for any agency or sub-component within DOJ or DHS, for any agency using such technology at the request or permission of DOJ or DHS, or for any agency using DOJ or DHS funding to procure or expand the use of such technology.

In Sections III through VI, we describe the issues and risks of specific surveillance technologies. Section III discusses facial recognition technology; Section IV discusses predictive policing algorithms; Section V discusses social media surveillance; and Section VI discusses DNA analysis and forms of genetic surveillance. Within each section, we discuss the application of the set

[6] DOJ, Organization, Mission, and Functions Manual, https://www.justice.gov/doj/organization-mission-and-functions-manual (last visited Jan. 19, 2024).

[7] Exec. Order No. 14,074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety § 13, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/.

of principles that DOJ and DHS should compel, or where appropriate incentivize, adherence to. In brief, these include[8]:

- prohibiting mass surveillance;
- protecting privacy, civil rights, and civil liberties;
- protecting constitutional rights;
- proving that the technology and its implementation do not result in a disparate impact for protected classes;
- requiring adequate evaluation of the purpose, objectives, benefits, and risks of the technology;
- adopting stricter data minimization procedures;
- ensuring adequate security for retained data;
- regular independent auditing;
- strengthening accountability and oversight, and;
- advancing public trust, prioritizing transparency, and requiring substantiation for claims relating to the technology, especially related to its effectiveness.

Recommendation One: DOJ and DHS should prohibit mass surveillance by ensuring that use of these technologies is context dependent and for explicit and legitimate purposes.

One of the primary risks to civil rights posed by law enforcement use of emerging surveillance technologies is that these technologies—individually or layered on top of one another—will be used for mass surveillance. By enabling surveillance at scale and at minimum cost, these emerging surveillance tools allow law enforcement to quickly identify and track individuals to an extent previously impossible. Given this scalability and the current lack of safeguards, the risk of mission creep is significant. And as more tools are integrated into larger platforms and supplemented by artificial intelligence, the threats to civil rights only grow.

[8] *See* Caitriona Fitzgerald, Testimony to Mass. Joint Comm. on the Jud. On "An Act to Regulate Face Surveillance" (Nov. 23, 2021), https://epic.org/documents/an-act-to-regulate-face-surveillance-massachusetts/.

Therefore, DOJ and DHS should prohibit mass surveillance via these technologies by ensuring that any use be context dependent. At the same time DOJ and DHS must effectively delineate and enforce a list of prohibited purposes, including ensuring that law enforcement agencies do not use surveillance technology to target minority communities or chill free speech and other constitutional activities.

Recommendation Two: DOJ and DHS should protect civil rights by prohibiting arrests based solely on untested surveillance technology.

Law enforcement organizations cannot be permitted to rely solely on unproven technologies as a basis for arresting individuals. For example, despite Interim DOJ policy and similar investigative leads policies across state, local, tribal, and territorial law enforcement agencies, there have been multiple documented instances of wrongful arrests based solely on use of facial recognition tools.[9] There has been no public action by the DOJ to suggest that corrective measures have been taken. Similarly, for investigations involving genetic information, the DOJ requires law enforcement agencies to check potential evidence against CODIS before attempting any forensic genetic genealogy searches.[10] The extent to which the DOJ oversees compliance to this requirement is unclear.[11]

Recommendation Three: DOJ and DHS should protect criminal defendants' constitutional rights by requiring adequate notice of the use of these surveillance technologies and ensuring that the technology is subject to adversarial interrogation during criminal litigation.

It is vital to just outcomes and to public trust in lawful process that technology and implementation of technology be subject to adversarial interrogation during criminal litigation. This includes the defendant's constitutional right to disclosure per *Brady v. Maryland*, 373 U.S. 83

[9] *See infra* note 104.

[10] Nat'l Inst. of Just., *An Introduction to Forensic Genetic Genealogy Technology for Forensic Science Service Providers* 2 (Sept. 2022), https://forensiccoe.org/private/6320f16805925.

[11] Jennifer Lynch, *Forensic Genetic Genealogy Searches: What Defense Attorneys & Policy Makers Need to Know*, EFF (Jul. 26, 2023), https://www.eff.org/wp/forensic-genetic-genealogy-searches-what-defense-attorneys-need-know.

(1963), and the confrontation clause of the Sixth Amendment. *Brady* requires the disclosure of all evidence that may be of an exculpatory nature.[12] In the context of biometric databases, this should include how many results came back with what confidence levels, as well as information about the accuracy of the technology used to search the database and produce results.

DOJ and DHS should expressly prohibit parallel construction—a common law enforcement practice by which agents recreate an evidentiary trail to conceal the role of a particular surveillance technique.[13] Parallel construction thus precludes courts from assessing the legality of that surveillance and undermines requirements to produce relevant materials in discovery.[14] Without prohibiting parallel construction, law enforcement agencies can evade scrutiny by merely recreating the evidentiary trail.[15] If law enforcement agencies want their technologies and techniques to be trusted as reliable, they should win on their merits in the light of day, not use court procedure to hide from scrutiny that might expose their deficiencies.

Recommendation Four: DOJ and DHS should ensure that any surveillance technology it plans to use is provably non-discriminatory and prohibit the use of such technology unless this non-discrimination is verified.

Title VI prohibits recipients of federal financial assistance from discriminating based on race, color, and national origin.[16] Title VI's prohibition "applies to intentional discrimination as well as to procedures, criteria or methods of administration that appear neutral but have a discriminatory effect

[12] *See* DOJ, Justice Manual 9-5.001, https://www.justice.gov/jm/jm-9-5000-issues-related-trials-and-other-court-proceedings#9-5.001 (DOJ policy regarding disclosure of exculpatory information).
[13] *See* Hum. Rts. Watch, *Dark Side Secret Origins of Evidence in US Criminal Cases* (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/darkside/secret-origins-evidence-us-criminal-cases.
[14] *Id.*
[15] *See* EPIC Comments re: New Jersey Regulating Law Enforcement's Use of Facial Recognition Technology 8 (Mar. 11, 2022), https://epic.org/documents/epic-comments-re-new-jersey-regulating-law-enforcements-use-of-facial-recognition-technology/.
[16] 42 U.S.C. § 2000d.

on individuals because of their race, color, or national origin."[17] Title VI may be violated where "a predominantly minority community is provided lower benefits, fewer services, or is subject to harsher rules than a predominantly nonminority community."[18] It also may be violated when a recipient of federal financial assistance relies on biased assumptions about certain individuals and groups to determine how and when to apply particular procedures or methods.[19] We urge agencies to consider how usage of these technologies and techniques may have disproportionately severe impacts on some populations as compared to others.

DHS and DOJ contracts have provided law enforcement agencies across with country with millions of dollars for this tech, with state and local law enforcement pushing that number easily into the hundreds of millions.[20] EPIC recently filed a petition with the Department of Justice to do a Title VI rulemaking and review.[21] ShotSpotter is an acoustic gunshot detection tool, funded in part by the Department of Justice, that perpetuates patterns of racist policing practices due to being disproportionately deployed in majority-minority neighborhoods. EPIC also sent a letter regarding predictive policing tools at large due to the tens of millions of dollars in funding funneled into this technology, the lack of evidence that these systems are effective at preventing crime, and the fact that law enforcement agencies don't even have records of what tools are being funded.[22] The fact

[17] *Civil Rights Requirements- A. Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d et seq. ("Title VI")*, U.S. Dep't of Health & Hum. Servs., https://www.hhs.gov/civil-rights/for-individuals/special-topics/needy-families/civil-rights-requirements/index.html (last visited Jan. 19, 2024).

[18] *Id.*

[19] *Id.*

[20] *Funding & Awards*, Bureau of Just. Assistance (2022), https://bja.ojp.gov/funding.

[21] EPIC Letter to Attorney General Garland Re: ShotSpotter Title VI Compliance, *supra* note 2.

[22] EPIC Letter to Attorney General Garland Re: Title VI Compliance and Predictive Algorithms (Jul. 6, 2022), https://epic.org/documents/epic-letter-to-attorney-general-garland-re-title-vi-compliance-and-predictive-algorithms/; Dell Cameron, *Justice Department Admits: We Don't Even Know How Many Predictive Policing Tools We've Funded*, Gizmodo (Mar. 17, 2022), https://gizmodo.com/justice-department-kept-few-records-on-predictive-polic-1848660323; Letter from 8 Members of Congress to Att'y Gen. Merrick Garland (Apr. 15, 2021), *available at* https://drive.google.com/file/d/1l56rBOiDA7k-vQScVfTu6eEMck1VAiLb/view.

that no such records exist point to a lack of substantiation that belies the American people whose tax dollars were funneled into this technology. Both DOJ and DHS should create and improve policies of how Title VI can be meaningfully enforced when it comes to funds being used for carceral technologies.

Recommendation Five: New surveillance technology—and new uses for existing surveillance technologies—should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, and its risks.

Currently, the E-Government Act of 2002 requires federal to conduct, review, and publish Privacy Impact Assessments (PIAs) before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or before collecting new information.[23] While the E-Government Act sets forth minimum requirements for PIAs, it also grants agencies broad discretion to design their own PIAs, which may leave out key information.[24] Further, the Biden administration's Executive Order on AI and related OMB guidance call for an impact assessment prior to agency use of rights-impacting AI and during use.[25]

Therefore, DOJ and DHS should develop—and consistently carry out—more robust PIAs prior to deploying a particular surveillance tool. Impact assessments should, at a minimum, consider several key factors including the fit between mission and proposed use, the sensitivity of info collected, data minimization procedures, due diligence on vendor and data quality, oversight and accountability procedures.

DOJ and DHS must also ensure that these PIAs are conducted promptly and adequately. As EPIC has shown, agencies—including the Federal Bureau of Investigation, the Census Bureau, and

[23] 44 U.S.C. § 3501 note at 208(b)(1)(A)(ii).
[24] 44 U.S.C. § 3501 note at 208(b)(3).
[25] *See* Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-andtrustworthy-development-and-use-of-artificial-intelligence [hereinafter "Executive Order 14110"]; Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, 88 Fed. Reg. 75625 (Nov. 3, 2023).

the U.S. Postal Service—have routinely failed to adhere to the E-Government Act's PIA requirements.[26] Without meaningful enforcement of these new assessment requirements, any progress toward meaningful pre-deployment evaluation will be illusory.

Recommendation Six: DOJ and DHS should adopt stricter data minimization procedures, including a prohibition on retention of biometric data after identity is confirmed.

Data minimization should be a core principle of any law enforcement activity that involves the collection of personal information. Rather than accepting the status quo of "collect it all," law enforcement collection activities should obtain only the information they need, to avoid the compilation of facial recognition databases. Doing so minimizes downstream harms. It is well-documented that lax data minimization rules—especially in the law enforcement context—can lead to abuse, misuse, and other harms.[27]

Therefore, DOJ and DHS should adopt stricter data minimization procedures. EPIC recommends that these data minimization procedures include:

- justifications for what data is needed to accomplish the specific defined task that the tool was acquired for;
- a prohibition on retention of biometric data after identity is confirmed; and
- prompt deletion of all data acquired in violation of any of these rules or that is no longer permissibly retained.

[26] *See, e.g.*, *EPIC v. USPS*, No. 1:21-cv-02156, 2022 WL 888183 (D.D.C. 2022); *EPIC v. Commerce*, 928 F.3d 95 (D.C. Cir. 2019); *EPIC v. FBI*, 72 F. Supp. 3d 388 (D.D.C. 2014).

[27] *See* Alina Selyukh, *NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog*, Reuters (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-toolson-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927; Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, Associated Press (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43; Sam Stanton et al., *Hundreds of California Police Misuse Law Enforcement Computer Databases, Investigation Shows*, Sacramento Bee (Nov. 13, 2019), https://www.desertsun.com/story/news/2019/11/13/california-police-misuselaw-enforcement-databases-computers/2509747001/.

Recommendation Seven: DOJ and DHS should ensure adequate security for all retained data, with correspondingly greater protections for more sensitive data.

Even if every piece of data is collected with scrupulous attention to privacy, civil rights, and civil liberties, and is disclosed with appropriate transparency and community buy-in, public trust may still suffer if that data is not adequately secured and a breach occurs.[28] As government agencies and private companies continue to amass sweeping amounts of personal information, including biometric information, the risks posed by security breaches continue to grow. Indeed, law enforcement agencies and their vendors have routinely been the subject of data breaches, risking further downstream harms from the collection of sensitive information.[29] Therefore, DOJ and DHS must ensure adequate security for collected information, with greater controls for high-risk or particularly sensitive information like biometric data.

Recommendation Eight: DOJ and DHS should require regular independent auditing of all surveillance technologies both prior to deployment and periodically thereafter.

Independent audits must be required for use of technology, especially when algorithms are involved. This should occur at both the procurement and deployment/use stage of a new technology. While there is no single model audit, DOJ and DHS should require that audits of surveillance technology have—at a minimum—several key characteristics, including:

- The audits should be conducted by a qualified, independent body, such as NIST, to ensure real results.
- The audits should review both the inputs and outputs of these systems—the data used to train these programs and the decisions they produce. In doing so, audits should essentially replicate the circumstances under which the technology is actually used.

[28] *See, e.g.*, Joseph Cox, *Here Are Images of Drivers Hacked From a U.S. Border Protection Contractor*, Vice (June 13, 2019), https://www.vice.com/en/article/43j5wm/here-are-images-of-drivers-hacked-from-a-us-border-protection-contractor-on-the-dark-web-perceptics.

[29] *See* Nicole Perlroth & Julian E. Barnes, *D.C. Police Department Data Is Leaked in a Cyberattack*, N.Y. Times (Apr. 27, 2021), https://www.nytimes.com/2021/04/27/us/dc-police-hack.html; *Police Software Vendor Breach Exposes Personal Data, Raid Plans*, Gov't Tech. (Jan. 23, 2023), https://www.govtech.com/security/police-software-vendor-breach-exposes-personal-data-raid-plans; Andy Greenberg, *Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents*, Wired (June 22, 2020), https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack/.

- Audits should be performed regularly—at least annually—and if these audits reveal harm that cannot be adequately resolved, the use of that technology should be immediately paused, either temporarily or permanently.

Recommendation Nine: DOJ and DHS should strengthen accountability and oversight mechanisms, including by requiring robust training, incident reporting, and consequences for misuse or other harms.

DOJ and DHS should strengthen accountability and oversight mechanisms, including by requiring robust training, incident reporting, and consequences for misuse or other harms. To that end, DOJ and DHS should also require all components carry out specialized training on the use of specific surveillance technologies at regular intervals. This training should be robust, routine, and validated by external auditors. Training materials, guidance, and policies should be published to enhance transparency. And analysts with access to particularly sensitive or invasive technologies—such as facial recognition—should be held to a higher standard. All agents authorized to conduct or approve searches of surveillance technologies should be regularly evaluated for compliance with these rules.

Agencies should also be required to build all systems with the capacity to create audit logs of all use of surveillance tools in support of incident reporting, audit, and oversight responsibilities. With these systems in place, agencies should be required to track incident reports—generated through these internal audits or the required independent audits mentioned above—to identify any errors, biases, or other documented harms of that agency's use of that system, as well as any remedial measures that the agency plans to take to mitigate those harms.

Finally, DOJ and DHS should ensure that agencies are responsible for outcomes from the use of surveillance technology, including by delineating consequence for agencies that fail to abide by these principles. Further, DOJ and DHS should enact strong accountability procedures as part of their compliance framework, with escalating consequences for agents who misuse or abuse their access to these systems, including—but not limited to—revocation of that agent's access to the system, administrative sanction, or more serious penalties for willful misconduct.

Recommendation Ten: DOJ and DHS should advance public trust, prioritize transparency, and require substantiation of claims relating to surveillance technology.

EPIC is encouraged by the Departments' emphasis on public trust in law enforcement agencies and urges the agencies to consider advancing public trust by limiting the scope of how surveillance technologies may be used, by prioritizing transparency surrounding use of technologies, and by requiring substantiation for any claims made about what a given technology is likely to achieve or historically has achieved.

While law enforcement agencies (and their tech vendors) tout the benefits of a given surveillance technology for solving the most heinous crimes, the reality is often that once a technology is deployed, it gets used for all manner of investigations, including minor crimes. As noted above, it may even be used in ways that chill participation in the democratic process, which includes participating in protests or attending places of worship. Ignoring or otherwise circumventing warrant requirements, internal policies, or local restrictions on the use of surveillance technology further erodes public trust.[30] Imposing, and more importantly enforcing, limitations on government use of surveillance technology to prevent violations of privacy, civil rights, and civil liberties is vital to cultivating public trust in the use of these technologies by law enforcement.

Prioritizing transparency about what data and technologies agencies are using, ideally through a process that allows for community input, would also go a long way towards strengthening public trust in law enforcement agencies. Historical deficiencies here include leadership being kept

[30] *See, e.g.*, Zack Whittaker, *Secret Service and ICE conducted warrantless stingray surveillance, says watchdog*, TechCrunch (Mar. 2, 2023), https://techcrunch.com/2023/03/02/secret-service-ice-warrantless-stingray/.

in the dark about what their staff is using,[31] law enforcement agencies deliberately equivocating about not being customers of a surveillance product when they were in fact using it on a free trial basis,[32] and—as mentioned above—law enforcement agencies using non-disclosure agreements to pre-emptively obstruct transparency about the technologies being used.[33]

The DOJ should require substantiation for any claims made about the accuracy and effectiveness of a given surveillance technology, both by law enforcement agencies and by tech vendors. For example, this includes equivocations such as claiming a product "reduces crime" when in reality it merely produces additional investigative leads.[34] It hurts public trust to claim these technologies achieve more than they actually do. While we believe the Federal Trade Commission (FTC) has adequate authority to pursue the tech vendors when deceptive claims about their products come from the mouths of government agencies acting as endorsers or influencers for those vendors,[35]

[31] *See, e.g.*, Drew Harwell, *Clearview AI to stop selling facial recognition tool to private firms*, Wash. Post (May 9, 2022), https://www.washingtonpost.com/technology/2022/05/09/clearview-illinois-court-settlement/ (noting that Clearview AI—as part of a settlement—agreed to stop offering free trials to police officers without their supervisors' approval).

[32] Ryan Mac et al., *Surveillance Nation*, BuzzFeed News (Apr. 6, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

[33] *See, e.g.*, Dell Cameron, *Docs Show FBI Pressures Cops to Keep Phone Surveillance Secrets*, Wired (June 22, 2023), https://www.wired.com/story/fbi-cell-site-simulator-stingray-secrecy/.

[34] *See* Eileen Guo, *How Amazon Ring uses domestic violence to market doorbell cameras*, MIT Tech. Rev. (Sept. 20, 2021), https://www.technologyreview.com/2021/09/20/1035945/amazon-ring-domestic-violence/ (noting that while Amazon Ring's central premise is reducing crime, independent analysis has failed to corroborate these claims). This can also result in a transparency issue when it comes to reporting. *Compare Morning Cybersecurity*, Politico Pro (Aug. 8, 2023) (claiming DHS "used Clearview's software to crack hundreds of backlogged child abuse cases") *with* Thomas Brewster, *Exclusive: DHS Used Clearview AI Facial Recognition in Thousands of Child Exploitation Cold Cases*, Forbes (Aug. 7, 2023), https://www.forbes.com/sites/thomasbrewster/2023/08/07/dhs-ai-facial-recognition-solving-child-exploitation-cold-cases/ (stating that "[the *operation*]…led to hundreds of identifications of children and abusers" and "no single *effort* like this has resulted in that amount of identifications in such a short period of time", with only one facial recognition-linked arrest cited in the story) (emphasis added).

[35] *See* EPIC Comment to FTC on Proposed Rule on Consumer Reviews and Endorsements 3–4 (Sept. 29, 2023), https://epic.org/documents/epic-comment-ftc-proposed-rule-on-consumer-reviews-and-endorsements/.

it seems likely that only the DOJ can take direct action against law enforcement agencies themselves. Moreover, especially in light of the recent joint statement from the DOJ, FTC, CFPB, and EEOC on AI,[36] there is no reason the DOJ could not stand side-by-side with the FTC in policing these vendors as well. Consumers should be able to trust that when their local police department promotes use of a specific product or service that their police department is doing so in the best interests of public safety.[37]

III. Facial Recognition Technology

a. Law Enforcement Should Not Use Facial Recognition Technology.

Facial recognition is a dangerous and privacy-invasive surveillance technology that law enforcement should not use. As a law enforcement investigative tool, facial recognition has not been proven to be reliable and the typical steps involved in law enforcement's use of facial recognition—from the selection of probe photos to the human review of the search results—can all contribute to its unreliability. Furthermore, facial recognition has been shown to be biased and will likely continue to be disproportionately focused on marginalized communities and will only exacerbate the historical inequalities in the criminal justice system. On a broader scale, the widespread use of facial recognition technology by law enforcement will undermine democratic values and Constitutional

This is even more problematic when there are marketing arrangements in place between the vendor and the law enforcement agency or a given public servant. One international industry association for surveillance equipment noted that a lack of transparency can harm the industry as a whole and diminish public trust: "We are troubled by recent reports of agreements [between the selling company and law enforcement organizations] that are said to drive product-specific promotion, without alerting consumers about these marketing relationships. This lack of transparency goes against our standards as an industry, diminishes public trust, and takes advantage of these public servants." Alfred Ng, *Amazon Ring's Police Partnership 'Troubled' Security Industry Group*, CNET (Aug. 8, 2019), https://www.cnet.com/news/amazon-rings-police-partnerships-troubled-security-industry-group/.

[36] Press Release, DOJ, Justice Department's Civil Rights Division Joins Officials from CFPB, EEOC and FTC Pledging to Confront Bias and Discrimination in Artificial Intelligence (Apr. 25, 2023), https://www.justice.gov/opa/pr/justice-department-s-civil-rights-division-joins-officials-cfpb-eeoc-and-ftc-pledging.

[37] *See* EPIC Comment to FTC, *supra* note 35.

rights. It is a perfect tool of oppression and poses far too great a risk to our democracy to become a ubiquitous tool of police surveillance. This is true even with regulations in place but particularly true given the current lack of federal regulations to protect against the potentially worst outcomes.

i. Facial recognition is inaccurate and biased and has not been established as a reliable investigative tool.

Several studies have shown that many facial recognition algorithms have accuracy issues. Furthermore, these accuracy issues tend to be most prominent among people of color, creating a racial bias issue in the accuracy of facial recognition algorithms. The accuracy and bias issues are exacerbated by the steps police often take in the process of using facial recognition for identification. These steps introduce other points of potential error instead of compensating for the accuracy and bias issues of facial recognition technology.

1. Facial recognition is inaccurate and often biased.

A landmark 2018 study by Joy Buolamwini and Timnit Gebru found alarming racial and gender disparities in a range of facial recognition and detection products marketed by some of the most prominent technology companies in the world.[38] While the systems were relatively accurate when analyzing the faces of white men, Buolamwini and Gebru found they failed up to one in three times when classifying the faces of Black women.[39] Subsequent studies have supported these results. In 2019, National Institute of Standards and Technology (NIST) evaluated several facial recognition algorithms and found "empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms."[40] NIST's 2019 study on demographic effects

[38] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[39] *Id*. at 1.

[40] Patrick Grother, Mei Ngan, & Kayee Hanaoka, *Face Recognition Vender Test Part 3: Demographic Effects*, NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [hereinafter "NIST FRT Demographic Effects Test"].

found that across algorithms, women were 2-5x more likely to be misidentified (a false positive) than men.[41] The same study found that Black people were typically 100x more likely to be misidentified than white people, though results varied somewhat across algorithms.[42]

The latest NIST reports use a variety of datasets to assess the accuracy of facial recognition algorithms, including both high quality images like passport photos, and lower quality images drawn from immigration lane cameras.[43] The NIST testing reveals a broad variance in accuracy of the facial recognition algorithms that are available to law enforcement—finding false negative rates ranging from 0.12 to 50 percent of searches against a mugshot database.[44] A 50 percent false negative error rate will return all wrong results in a disturbing half of its searches. While the best algorithms performed very well on controlled mugshot images, the same algorithms had error rates above 20 percent "for side-view images, poorer quality webcam images, and, particularly, for newly introduced ATM-style kiosk photos that were not originally intended for automated face recognition."[45]

NIST's testing reveals that even the best algorithms are only as good as the reference image. And even though more recent NIST tests contain a broader range of image variability, the NIST tests still do not regularly test algorithms against the types of photos that police are likely to encounter in investigations, such as surveillance cameras images where the subject is blurry, looking away, obscured in some way, or in poor light. While setting high thresholds for accuracy may prevent some misidentifications, the low-quality target images used by police continue to pose a substantial threat of wrongful identification, arrest, and in the worst cases, wrongful conviction—particularly for

[41] *Id*. at 7.
[42] *Id*.
[43] Patrick Grother, Mei Ngan, & Kayee Hanaoka, *Face Recognition Technology Evaluation (FRTE) Part 2: Identification*, NIST 5 (Feb. 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf [hereinafter "NIST FRT Identification Evaluation"].
[44] *Id.*
[45] *Id.*

people of color. It unfortunately should come as no surprise that, for the publicly reported cases, every single person wrongfully arrested due to the use of facial recognition has been Black.[46]

2. Police facial recognition identification procedures can compound the accuracy and bias issues of facial recognition instead of counteracting them.

Facial recognition has not been established as a reliable investigative tool, indeed, there is plenty of evidence that suggests law enforcement procedures compound the potential for misidentifications and biased outcomes. As one facial recognition expert has explained:

> No study has comprehensively examined the reliability of face recognition as actually used by a representative sample of U.S. law enforcement officers, taking into account the full range of possible variabilities generated by unconstrained probe photo qualities, probe photo manipulation, variably trained human analysis, and the contextual and other biases that may be present in many searches conducted in police departments across the country today.[47]

Despite the lack of comprehensive review of facial recognition as deployed by law enforcement, there is plenty of evidence that speaks to its unreliability. The unreliability of facial recognition as a law enforcement investigative tool does not merely stem from potential misidentifications by the facial recognition algorithm itself, but also stem from the various steps police typically take in the use of facial recognition for identification, including: 1) the selection of a probe photo, 2) the choice

[46] Katie Hawkinson, *In every reported case where police mistakenly arrested someone using facial recognition, that person has been Black*, Bus. Insider (Aug. 6, 2023), https://www.businessinsider.com/in-every-reported-false-arrests-based-on-facial-recognition-that-person-has-been-black-2023-8.

[47] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. on Priv. & Tech. 16 (2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

of database to use for the search, 3) the preprocessing of the probe photo, 4) the algorithm used for the search, and 5) the human review conducted of the results of the search.[48]

The probe photo is the photograph chosen of the unknown subject used to run the facial recognition search. The quality of the photo affects the accuracy of the search results.[49] The photos of an unknown subject police have to work with vary in quality. The angle of the photo, the lighting, and the sharpness of the photo, among other things, can all have an impact on the accuracy of the search results, so much so that oversight and scientific bodies have issued standards for photos and vendors have made minimum photo quality recommendations.[50]

Despite the role that probe photos play in the reliability of the search results, "available information suggests that few agencies engage in a robust analysis of probe photo quality or prescribe a minimum photo quality standards…."[51] There are numerous examples of police using unsuitable probe photos. In 2019, the Las Vegas Metropolitan Police Department used "unsuitable" photos for its facial recognition searches nearly half the time.[52] The NYPD used a photo that was not even of the subject but a celebrity that apparently looked like the subject.[53] Sometimes photos are not even used. Several police departments have used the forensic sketch of a suspect as the probe photo for a facial recognition search.[54] These practices of using low-quality photos, photos that are not actually of the subject, and sketches all contribute to increase the unreliability of facial recognition searches.

[48] *Id.* at 9.
[49] *Id*. at 9–10.
[50] *Id*. at 10.
[51] *Id*.
[52] Todd Feathers, *Las Vegas Cops Used 'Unsuitable' Facial Recognition Photos To Make Arrests*, Motherboard (Aug. 7, 2020), https://www.vice.com/en/article/pkyxwv/las-vegas-cops-used-unsuitable-facial-recognition-photos-to-make-arrests.
[53] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (2019), https://www.flawedfacedata.com.
[54] *Id*.

The database a probe image is run against affects the reliability of the results. If a subject is not in the database against which a facial recognition search is run, all the results returned will necessarily be false positives. The quality of the images in the chosen database will affect reliability. Databases with older and/or lower quality images will increase the potential for errors. Additionally, the size of the database has an impact on reliability. Larger databases are more likely to contain people who look similar, which can lead to misidentification.[55]

Preprocessing of a probe photo involves some type of editing of the photo itself, which can impact the reliability of the facial recognition search. Law enforcement have used software to edit probe photos in several different ways, including "using the blur tool to add pixels into a low-quality image; cutting and pasting new features into the subject photograph; combining photographs of two different people to generate a single image; and using 3D modeling to recreate an approximation of facial features not visible in the original image."[56] These changes to the probe photos may make it more likely that the facial recognition search returns results, but it also is likely to increase the unreliability of the returned results.

The algorithm used in a facial recognition search can also impact the reliability of the results. The accuracy of algorithms can vary widely and is impacted by, among other things, the data used to train the algorithm. For example, algorithms trained on images of predominately white males will likely be relatively accurate with facial recognition searches of white males but tend to be less accurate when performing a search of a person of color.[57] Additionally, older algorithms tend to be less accurate than newer algorithms.

[55] Garvie, *supra* note 47, at 10.
[56] *Id*. at 11.
[57] NIST FRT Demographic Effects Test, *supra* note 40, at 2.

The issues created by photo selection, choice of database, preprocessing of photos, and the algorithms used are not necessarily mitigated by the human review of the search results. On the contrary, the human review can create its own reliability issues due to variance in people's ability to identify unfamiliar faces, training issues, and various bias issues.

Facial recognition searches generally return a candidate list of possible matches with each candidate associated with a confidence score. A human is then responsible for sorting through the list of possible matches to identify the correct one. The general assumption is that with a human in the loop, they can mitigate the potential misidentifications. Of course, this assumes that humans are good at face comparisons.

Research shows that people are generally not great at identifying unfamiliar faces.[58] This is true even when dealing with high-quality photos, which is rarely the case with law enforcement probe photos. The unfamiliarity of the subject, low-quality images, the different angles of photos, the obfuscation of facial features, among other things, all contribute to the difficulty of identifying whether a probe photo and one of the photos from the candidate list are indeed a match.

The issues with trying to confirm the identification of a probe photo are compounded by various cognitive biases that are so often a part of subjective analysis. For example, people are susceptible to confirmation bias where they focus on or interpret new information in a manner consistent with existing expectations or beliefs. Consequently, a human reviewing the results of a facial recognition search will be biased towards agreeing with an algorithm's conclusion rather than independently reviewing the biometric similarities and differences between the faces.[59] A 2020 study of facial recognition systems sponsored by the Department of Homeland Security Science &

[58] Garvie, *supra* note 47, at 22.
[59] *Id.* at 30–31.

Technology Directorate demonstrated this bias and cautioned that the human in the loop may be biased towards agreeing with an algorithm's false positive determination.[60]

ii. Law enforcement's use of facial recognition is disproportionately directed at communities of color and exacerbates the historical racial inequalities in the criminal justice system.

There is plenty of evidence that police surveillance is disproportionately directed at communities of color, particularly Black communities. There are no shortage of examples including the lantern laws during colonial times, the FBI's COINTELPRO program, the war on drugs, and the surveillance of Black Lives Matter activist just to name a few—police surveillance has a long history of targeting Black people.[61] The targeting of Black people for police surveillance has contributed to the historic inequalities in the criminal justice system. Unfortunately, this trend of disproportionately directing surveillance technologies towards communities of color has already started with facial recognition and will only increase if law enforcement continues to expand its use.

1. Law enforcement's use of facial recognition is and will continue to be disproportionately directed at communities of color if police continue to use facial recognition technology.

Facial recognition technology is not only problematic because it has not been established as a reliable investigative tool, but also because of how it is deployed. Law enforcement's use of facial recognition technology is disproportionately directed towards communities of color and other marginalized communities.

Despite the research showing that facial recognition algorithms often have the highest error rate on people of color, the technology is most often directed towards communities of color. In New Orleans, the city council voted to lift a ban on police's use of facial recognition after a violent crime

[60] *See* John J. Howard et al., *Human-algorithm Teaming in Face Recognition: How Algorithm Outcomes Cognitively Bias Human Decision-making*, 15 PLoS ONE 1, 15 (2020).
[61] *See generally* Simone Browne, *Dark Matters: On the Surveillance of Blackness* (2015).

rose in the city.[62] The technology was touted as "effective, fair tool for identifying criminals quickly."[63] Roughly a year after New Orleans police began using facial recognition again, the reality was the technology "had low effectiveness, was rarely associated with arrests and was disproportionately used on Black people."[64]

In Detroit, the Project Green Light surveillance program has connected high definition cameras at over 700 locations that send a live feed to Detroit Police's real time crime center (RTCC).[65] These live video feeds can be used to pull images for facial recognition searches against a database that contains "mug shots, sex offender registry photographs, driver's license photos and state ID photos[.]"[66] Almost every Michigan resident is in the database, but the Project Green Light cameras are concentrated in majority-Black areas.[67] A 2019 critical analysis of Project Green Light reported that "surveillance and data collection was deeply connected to diversion of public benefits, insecure housing, loss of employment opportunities, and the policing and subsequent criminalization of the community members that come into contact with these surveillance systems."[68] Despite claims that Project Green Light reduces crime, there is little evidence so far that it actually does.[69]

[62] 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.

[63] *Id*.

[64] *Id*.

[65] City of Detroit, Crime Intel. Unit, *Project Green Light Detroit Presentation* (Aug. 6, 2020), https://detroitmi.gov/sites/detroitmi.localhost/files/2020-08/Facial%20Recog%20and%20Project%20Green%20Light%20%281%29.pdf.

[66] Detroit Cmty. Tech. Proj., *A Critical Summary of Detroit's Project Green Light and its Greater Context* 5 (June 9, 2019), https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=.

[67] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harv. GSAS Sci. Pol'y Grp. Blog (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[68] Detroit Cmty. Tech. Proj., *supra* note 66, at 5.

[69] Laura Herberg, *Tracked and Traced: Does Project Green Light in Detroit Reduce Crime?*, WDET.org (Feb. 3, 2022), https://wdet.org/2022/02/03/tracked-and-traced-does-project-green-light-in-detroit-reduce-crime/.

In New York City, the Decode Surveillance NYC Project found that there are more surveillance cameras compatible with facial recognition in non-white communities.[70] Just as minority communities in New York City have been disproportionately impacted by "stop-and-frisk" policies, the report finds that Black and Brown communities are facing disproportionately higher rates of potential facial recognition surveillance.[71] The end result of increased use of facial recognition by law enforcement is predictable, the technology will be disproportionately directed at marginalized communities, particularly communities of color, and the current inequalities in the criminal justice system will be exacerbated by its use. Facial recognition will follow in the footsteps of other surveillance technology and programs and be disproportionately directed at marginalized communities and this will spell disaster for communities of color.

2. The racial bias in policing combined with the use of facial recognition by law enforcement will only exacerbate the historical racial inequalities in the criminal justice system.

There is no shortage of evidence that demonstrates the racial bias in the criminal justice system.[72] Many if not all aspects of the criminal justice system produce racially disparate outcomes, including traffic stops, searches, drug arrests, pretrial detention, and sentencing outcomes. A 2020 study analyzing nearly 100 million traffic stops from all over the country found racial bias in stop decisions and a lower bar for searching Black and Hispanic drivers compared to their white

[70] Amnesty Int'l, *Inside the NYPD's Surveillance Machine*, https://banthescan.amnesty.org/decode/ (last visited Jan. 21, 2024).

[71] *Id*.

[72] Radley Balko, *There's Overwhelming Evidence That the Criminal Justice System Is Racist. Here's the Proof*, Wash. Post (June 10, 2020), https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/.

counterparts.[73] A 2013 Justice Department study found that Black drivers were more likely to get pulled over and more likely to be searched than white drivers.[74]

These broad studies are further supported by numerous analyses of traffic stops in states and cities across the United States. A 2023 statewide analysis of traffic stops in Connecticut found that Black motorists were more likely to be searched yet less likely to be found with contraband from those searches.[75] A study of stops by police in Springfield, Missouri found "substantial disparities in the rate at which African-Americans were stopped, and that the disparities increased, from 2012 to 2016 in Springfield."[76] A study of traffic stops in Kansas City found that Blacks were 2.7 times more likely to be pulled over for an investigatory traffic stop and five times more likely to be searched.[77] Black drivers in Vermont were found to be four times more likely to be searched than a white driver.[78] Similarly, a study of hundreds of thousands of traffic stops in San Diego found that police were more likely to search Black and Latino drivers compared to white drivers—despite the fact that white drivers were more likely to be found with contraband.[79]

[73] Emma Pierson et al., *A Large-scale Analysis of Racial Disparities in Police Stops Across the United States*, 4 Nature Hum. Behav. 736, 736 (2020), https://www.nature.com/articles/s41562-020-0858-1.pdf.

[74] Lynn Langton & Matthew Durose, *Police Behavior During Traffic and Street Stops*, DOJ (Sept. 2013), https://bjs.ojp.gov/content/pub/pdf/pbtss11.pdf (revised Oct. 27, 2016).

[75] Ken Barone et al., *Connecticut Racial Profiling Prohibition Project, Traffic Stop Data Analysis and Findings 2021*, Univ. Conn. Inst. for Mun. & Reg'l Pol'y 45–58 (Oct. 2023), https://assets-global.website-files.com/6076e3f57e39855392637f16/6525a6b30968fb82c5a80237_2021%20CTRP3%20Traffic%20Stop%20Analysis%20and%20Findings%20Report.pdf.

[76] Mike Stout, *Racial and Ethnic Disparities in Traffic Stops and Stop Outcomes in Springfield, Missouri: 2012-2016* 2 (Aug. 8, 2017), https://www.springfieldmo.gov/DocumentCenter/View/45970/Racial-and-Ethnic-Disparity-in-Traffic-Stops-Report-2012-2016-.

[77] Lisa Rodriguez, *Study of KC Metro Traffic Stops Shows Race Deeply Embedded In Police Practice*, NPR (Mar. 12, 2015) https://www.kcur.org/show/up-to-date/2015-03-12/study-of-kc-metro-traffic-stops-shows-race-deeply-embedded-in-police-practice#stream/0.

[78] Stephanie Seguino & Nancy Brooks, *A Deeper Dive into Racial Disparities in Policing in Vermont* 28 (Mar. 26, 2018), http://mediad.publicbroadcasting.net/p/vpr/files/201803/a_deeper_dive_into_racial_disparities_in_policing_in_vermont_3.26_final.pdf.

[79] Joshua Chanin et al., *Traffic Enforcement in San Diego, California: An Analysis of SDPD Vehicle Stops in 2014 and 2015* ii (Nov. 2016), https://www.sandiego.gov/sites/default/files/sdpdvehiclestopsfinal.pdf.

There are similar disparities when looking at police-shootings. The National Academy of Sciences published an August 2019 study that analyzed police-shooting from 2013-2018. The study found the Black men were 2.5 times more likely than white men to be killed by police and Black women were 1.4 times more likely than white women to be killed by police.[80] Another study looked at police shootings at the county level from 2011–2014 and found "evidence of a significant bias in the killing of unarmed [B]lack Americans relative to unarmed white Americans, in that the probability of being {Black, unarmed, and shot by police} is about 3.49 times the probability of being {white, unarmed, and shot by police} on average."[81] Furthermore, the study found "no relationship between county-level racial bias in police shootings and crime rates (even race-specific crime rates), meaning that the racial bias observed in police shootings in this data set is not explainable as a response to local-level crime rates."[82] Law enforcement use of facial recognition creates the inevitable event where an innocent person will be killed by police because they were misidentified by an algorithm.

Despite Black and white people using and selling drugs at roughly the same rate, Black people are arrested, charged, and convicted of drug crimes at a much higher rate. In New York City, "[B]lack people were arrested on low-level marijuana charges at eight times the rate of white, non-[H]ispanic people."[83] For Hispanic people it was five times the rate of white people.[84] Despite the legalization and decriminalization on marijuana in several states, "[B]lack people are 3.64 times

[80] Frank Edwards, Hedwig Lee, & Michael Esposito, *Risk of Being Killed by Police Use-of-force in the U.S. by age, race/ethnicity, and sex* 3 (Aug. 2, 2019), https://www.prisonpolicy.org/scans/police_mort_open.pdf.
[81] Cody T. Ross, *A Multi-Level Bayesian Analysis of Racial Bias in Police Shootings at the County-Level in the United States, 2011–2014* 1 (Nov. 5, 2015), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0141854&type=printable.
[82] *Id.*
[83] Benjamin Mueller, Robert Gebeloff, & Sahil Chinoy, *Surest Way to Face Marijuana Charges in New York: Be Black or Hispanic*, N.Y. Times (May 13, 2018), https://www.nytimes.com/2018/05/13/nyregion/marijuana-arrests-nyc-race.html.
[84] *Id.*

more likely than white people to be arrested for marijuana possession."[85] Additionally, "African Americans are about five times as likely to go to prison for drug possession as whites—and judging from exonerations, innocent [B]lack people are about 12 times more likely to be convicted of drug crimes than innocent white people."[86]

Once arrested, the disparities for Black people do not improve. Looking at the research on plea bargaining, the Bureau of Justice Assistance found that "the majority of research on race and sentencing outcomes shows that [B]lacks are less likely than whites to receive reduced pleas."[87] Similarly, Black men receive longer sentences than their white counterparts for the same crime.[88] A review of the academic literature on racial disparities in pretrial detention found that "in large urban areas, Black felony defendants are over 25% more likely than white defendants to be held pretrial."[89]

The racial inequalities in policing and the criminal justice system are well documented and there is no reason to believe that facial recognition technology will not be applied in a racially bias manner, indeed, as shown in the previous section, facial recognition is already directed in a racially bias manner. Furthermore, a study that analyzed facial recognition deployment by police and arrests in over a 1,000 U.S. cities found that it "contributes to greater racial disparity in arrests."[90] It's clear

[85] ACLU, *A Tale of Two Countries: Racially Targeted Arrests in the Era of Marijuana Reform* 5 (Apr. 16, 2020), https://www.aclu.org/publications/tale-two-countries-racially-targeted-arrests-era-marijuana-reform?eType=EmailBlastContent&eId=f3aa6ff4-fdc5-4596-b96a-2c0fe443df39.

[86] Samuel R. Gross, Maurice Possley, & Klara Stephens, *Race and Wrongful Convictions in the United States*, Nat'l Registry of Exonerations iii (Mar. 7, 2017), https://www.law.umich.edu/special/exoneration/Documents/Race_and_Wrongful_Convictions.pdf.

[87] Bureau of Just. Assistance, DOJ, *Research Summary: Plea and Charge Bargaining* 3 (Jan. 24, 2011), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/PleaBargainingResearchSummary.pdf.

[88] U.S. Sentencing Comm'n, *Demographic Differences in Sentencing: An Update to the 2012 Booker Report* (Nov. 2017), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2017/20171114_Demographics.pdf.

[89] Wendy Sawyer, *How Race Impacts Who is Detained Pretrial* (Oct. 9, 2019), https://www.prisonpolicy.org/blog/2019/10/09/pretrial_race/.

[90] Thaddeus L. Johnson et al., *Facial Recognition Systems in Policing and Racial Disparities in Arrests* 1, 9 (Oct. 2022), https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892.

that the continued use and adoption of facial recognition technology by law enforcement will magnify the historic inequalities of the criminal justice system.

iii. Facial recognition is a dangerous tool of oppression and poses too great a risk to our democracy that is amplified by the lack of strict federal regulation.

The dangers of facial recognition do not begin and end with racial bias. Even if facial recognition was perfectly accurate for and equally applied to all types of people, the dangers of facial recognition would not disappear. In some sense, the danger would be even greater. Facial recognition is a powerful surveillance tool that can destroy any sense of privacy we may have as we go about our daily lives. The technology itself enables comprehensive surveillance which poses a threat to privacy and civil liberties. Face surveillance can be used for real-time tracking and for identification of individuals in crowds. These abilities are nearly unique to facial recognition. Comprehensive real time surveillance will substantially chill freedom of speech and protest as individuals rightfully fear identification and retaliation for engaging in lawful protests. Facial recognition has already been used numerous times by law enforcement agencies to conduct surveillance on people engaged in First Amendment-protected activities.[91] Simply put, facial recognition technology places too much power in the hands of the police.

These dangers are heightened by the fact that the U.S. lacks strict regulation of the use of facial recognition technology. Strict regulation would not completely eliminate the dangers of facial recognition but would at least decrease it. Currently, law enforcement can generally implement facial recognition with little to no oversight and take advantage of the vast number of images of

[91] *See, e.g.*, U.S. Gov't Accountability Office, GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks 17 (June 3, 2021), https://www.gao.gov/assets/gao-21-518.pdf (finding that at least six agencies used facial recognition to surveil Black Lives Matter protestors); Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, Rolling Stone (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/ (reporting that the Baltimore Police Department used facial recognition and social media surveillance to surveil protestors following the death of Freddie Gray).

people that are available online through social media and other websites, in government databases like DMV or Passport photo databases, or that are caught on the millions of CCTV cameras across the country. The ease of implementation of facial recognition makes the technology too tempting to resist and all the more dangerous. The dangers and risk of facial recognition technology to individuals and our democracy are far too great to allow its use by law enforcement.

b. <u>If Using Facial Recognition Technology, DOJ and DHS Must Adequately Mitigate Harm.</u>

While EPIC firmly believes that law enforcement should not use facial recognition, any existing use of this technology must be bounded by robust safeguards to mitigate and eliminate related harms.[92]

Recommendation One: DOJ and DHS should prohibit mass surveillance.

DOJ and DHS should prohibit mass surveillance via facial recognition technologies by ensuring that any use be context dependent. Facial recognition enables law enforcement to covertly identify and track anyone at any time. Moreover, facial recognition technology is often deployed as part of a broader ecosystem of surveillance tools, allowing law enforcement to quickly connect persons identified through facial recognition to a vast amount of information in government or commercially available databases.[93] Facial recognition technology can also be deployed at scale, allowing law enforcement agencies to conduct mass surveillance of large crowds. DHS and DOJ can partially mitigate the risks of facial recognition technology by:

- Only performing facial recognition searches authorized by a warrant supported by probable cause;
- Imposing a "serious violent felony" requirement for facial recognition searches;

[92] *See supra* note 8 and accompanying text.

[93] *See* Zac Larkham, *The Quiet Rise of Real-Time Crime Centers*, Wired (Jul. 18, 2023), https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/; Dhruv Mehrotra, *Cops Used DNA to Predict a Suspect's Face—and Tried to Run Facial Recognition on It*, Wired (Jan. 22, 2024), https://www.wired.com/story/parabon-nanolabs-dna-face-models-police-facial-recognition/.

- Prohibiting use of probe images obtained from First Amendment protected activities or images obtained in violation of the Fourth Amendment; and

- Prohibiting use of facial recognition systems that search databases derived from social media like Clearview AI or PimEyes.

Because of the relative scalability of facial recognition and availability of off-the-shelf technology, the risks of mission creep are significant. While facial recognition is often touted for specific purposes, it is often repurposed for other, secondary purposes that stray far afield from its original justification. And as this mission creep continues, the risks that agencies will use these systems to target minority communities and constitutionally protected activities only increases. For example:

- The U.S. Government Accountability Office found that at least six agencies reported using facial recognition to surveil Black Lives Matter protesters in the summer of 2020.[94]

- The U.S. Postal Investigation Service also used facial recognition to monitor racial justice protesters during that same period of 2020.[95]

- The New York Police Department used facial recognition technology to identify a prominent activist accused of assault for yelling loudly at a police officer.[96]

- The Baltimore Police Department used facial recognition technology—in combination with location-based social media tracking—to surveil protesters following the death of Freddie Gray.[97]

Together, these factors make law enforcement use of facial recognition particularly dangerous to civil rights. As we've already seen, without necessary safeguards in place, facial recognition

[94] U.S. Gov't Accountability Office, GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks 17 (June 3, 2021), https://www.gao.gov/assets/gao-21-518.pdf.

[95] Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program*, Yahoo News (May 18, 2021), https://news.yahoo.com/facial-recognition-fakeidentities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program214234762.html.

[96] George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, Gothamist (Aug. 14, 2020), https://gothamist.com/news/nypd-used-facialrecognition-unit-in-siege-of-black-lives-matter-activists-apartment.

[97] Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, Rolling Stone (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/.

technology will only serve to exacerbate protest policing and political repression, over-policing of minority communities, and risk of wrongful identification and wrongful arrest.

Therefore, DOJ and DHS should require that biometric data be processed fairly and lawfully, collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with these specified purposes.

DOJ and DHS should, as a matter of policy, require that law enforcement agents obtain a search warrant supported by probable cause before using facial recognition technology. This probable cause requirement can also be implemented with limited exceptions for certain emergency circumstances, so long as agencies follow up with the court as soon as practically possible. Individualized court approval for facial recognition searches will ensure that such use is narrowly tailored and context-specific, prevent dragnet surveillance, and further public trust of law enforcement activities.

In doing so, DOJ and DHS should delineate permissible purposes for the use of facial recognition. In a facial recognition policy template for state, local, tribal, and territorial law enforcement, DOJ and DHS recommend delineating authorized uses of these systems and suggest a non-exhaustive list of uses, including:[98]

- "A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity[;]"
- "An active or ongoing criminal or homeland security investigation[;]" and
- "To investigate and/or corroborate tips and leads."

[98] DHS & DOJ Bureau of Just. Assistance, *Face Recognition Policy Development Template for Use in Criminal Intelligence and Investigative Activities* 14 (Dec. 2017), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf [hereinafter "DHS/DOJ Facial Recognition Policy Template"].

The sheer breadth of these authorized uses gives law enforcement agents incredible discretion in deploying this technology. And with that incredible discretion comes increased risk that it will be deployed inappropriately. Therefore, EPIC recommends that DOJ and DHS follow proposed legislative approaches, such as requiring probable cause that the individual sought through facial recognition has committed or is committing a "serious violent felony", as defined in 18. U.S.C. 3559(c)(2)(F).[99]

Similarly, DOJ and DHS should also include explicit impermissible purposes. DOJ's NGI-IPS Policy Implementation Guide prohibits submitting probe photos obtained in violation of the First or Fourth Amendments.[100] Other DOJ and DHS materials similarly recommend as a best practice that state, local, tribal, and territorial law enforcement agencies include prohibited uses, including where use violates the First, Fourth, and Fourteenth Amendments or where it is based solely on "religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race[], ethnicit[y], citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law."[101] However, oversight and implementation remain unclear, especially concerning the use of off-the-shelf facial recognition technology like Clearview AI.[102] Surveillance systems should not be

[99] *See, e.g.*, Facial Recognition Act of 2023, H.R. 6092, 118th Cong. § 101(b)(3)(F) (2023).

[100] Kimberly J. Del Greco, Deputy Assistant Dir., Criminal Justice Info. Srvs. Div., FBI, Statement Before the House Comm. on Oversight & Gov't Reform on "Law Enforcement's Use of Facial Recognition Technology" (Mar. 22, 2017), https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology.

[101] *See* DHS/DOJ Facial Recognition Policy Template, *supra* note 98, at 19–20.

[102] While Clearview AI's Terms of Service contains prohibited uses—including a vague prohibition on using its software to "engage in activity that would discriminate against any person or violate any person's civil rights[,]" it is unclear to what extent—if at all—these provisions are enforced. *See* Clearview AI, Terms of Service, https://www.clearview.ai/terms-of-service (last visited Jan. 19, 2024).

used to monitor the exercise of democratic rights, such as voting, privacy, peaceful assembly, speech, or association, in a way that limits the exercise of civil rights or civil liberties.[103]

Recommendation Two: DOJ and DHS should protect civil rights by prohibiting arrests based solely on information derived from facial recognition matches.

As with other untested technologies, law enforcement agencies have erroneously relied solely on facial recognition as the basis for arrests. And there have been multiple documented instances of wrongful arrests based solely on use of facial recognition tools and no public indication that DOJ has taken corrective measures, despite its own interim policy prohibiting such reliance.[104] Most law enforcement agencies today claim that facial recognition is used only as a "investigative lead", but this misnomer has not prevented misidentifications. In some cases, law enforcement agencies have attempted to comply with the investigative lead requirement using a flawed photo lineup derived from the initial facial recognition identification.[105] A subsequent witness identification is not enough; DHS and the DOJ should require independent corroborating evidence before requesting any warrant stemming from a facial recognition identification.

[103] *See, e.g.*, Sidney Fussell, *Did a University Use Facial Recognition to ID Student Protesters?*, Wired (Nov. 18, 2020, https://www.wired.com/story/did-university-use-facial-recognition-id-student-protesters/; Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program*, Yahoo News (May 18, 2021), https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html?guccounter=1; Mike Holden, *Pittsburgh police used facial recognition technology during Black Lives Matter protests*, WXPI News (May 21, 2021), https://www.wpxi.com/news/top-stories/pittsburgh-police-used-facial-recognition-technology-during-black-lives-matter-protests/VT52MGWM3VCDJINJSZPOO5NHKU/ (revealing that Pittsburg Police used Clearview AI to identify protesters in violation of a city ban on Clearview).

[104] *See, e.g.*, ACLU, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart* (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart; *see also* Thomas Germain, *Cops Say They Only Use Facial Recognition for Leads, But It's Often the Sole Basis for Arrests*, Gizmodo (Dec. 6, 2022), https://gizmodo.com/facial-recognition-cops-police-sole-basis-arrests-study-1849859483.

[105] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (Jun. 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *New Jersey v. Arteaga*, Brief of EPIC et al. as Amicus Curiae at 22-23, https://epic.org/documents/new-jersey-v-arteaga/ [hereinafter "Arteaga Amicus Brief"].

Therefore, DOJ should strengthen the prohibition on arrests based solely on facial recognition matches, ensure that these policies are followed in practice, and publish information on accountability measures for violations of these policies. Agencies should not be permitted to rely solely or mainly on unproven technologies as a basis for arresting individuals.

Recommendation Three: DOJ and DHS should protect criminal defendants' constitutional rights by requiring adequate notice of the use of facial recognition technology and ensuring that the technology is subject to adversarial interrogation during criminal litigation.

DOJ and DHS should prohibit related abusive surveillance practices that work to undermine constitutional rights and obfuscate the use of technologies like facial recognition. Around the country, agencies have concealed the use of facial recognition, and they are either not required to give notice of the use of facial recognition to criminal defendants or construe any requirements narrowly. This obfuscation undermines due process rights and prevents defendants from challenging unconstitutional surveillance.[106] In one recent case, the defendant was not identified by the local police's technology and techniques, so the local law enforcement agency outsourced the photo to another jurisdiction for processing. The local police refused to provide discovery on the facial recognition system, the original photo and whether edits were performed to the photo before the search was run by the other jurisdiction, as well as information about the analyst who performed the search.[107] There are numerous points at which errors could have been made and a criminal defendant is entitled to understand the evidence presented against them through discovery. Because of this, some states have begun to enact rules requiring adequate notice.[108]

DOJ and DHS should also ensure that criminal defendants are provided adequate notice where evidence is derived from the use of facial recognition technology. EPIC recommends that

[106] *See* 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/.
[107] *See* Arteaga Amicus Brief, *supra* note 105.
[108] *See, e.g.*, S.B. 218, 2020 Gen. Session (Utah 2020), https://le.utah.gov/~2020/bills/sbillint/SB0218.pdf.

DOJ and DHS adopt a notice rule that clarifies that criminal defendants must receive notice of any information or evidence derived from the use of facial recognition technology, such as when the agency "would not have possessed the information or evidence ***but for*** the use of facial recognition, regardless of any claim that the information or evidence is attenuated from such recognition, and would inevitably have been discovered or obtained the information or evidence through other means."[109] In doing so, DOJ and DHS should also expressly prohibit parallel construction, which enables agencies to evade obligations to criminal defendants.[110]

Recommendation Four: DOJ and DHS should ensure technology is provably non-discriminatory prior to deployment.

DOJ and DHS should ensure that any and all facial recognition technology sought to be deployed is provably non-discriminatory and prohibit the use of such technology unless this non-discrimination is certified.

As noted above, there is a huge corpus of information indicating disparate impacts and results of facial recognition technology.[111] Law enforcement reliance on biased facial recognition technology has severe consequences for the rights of minority communities which are already over-policed.[112] Indeed, all six individuals to publicly sue for their wrongful arrest due to facial recognition are Black.[113]

[109] *See* Facial Recognition Act of 2023, *supra* note 99, § 3(3) (emphasis added).
[110] *See supra* notes 13–15 and accompanying text.
[111] *See supra* Sec. 3(a)(i)(1).
[112] *See* Nicol Turner Lee & Caitlin Chin-Rothmann, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, Brookings (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.
[113] Katie Hawkinson, *In every reported case where police mistakenly arrested someone using facial recognition, that person has been Black*, Bus. Insider (Aug. 6, 2023), https://www.businessinsider.com/in-

Therefore, law enforcement agencies—and any private company supplying off-the-shelf facial recognition tools—should bear the burden of proving the technology and its use are non-discriminatory prior to deploying that technology. To effectively and holistically assess the use of facial recognition, both the system itself and the database searched against should be demonstrably unbiased.[114] This evaluation must also include testing under circumstances that materially replicate conditions in which the system is deployed, including with respect to image quality.

Recommendation Five: DOJ and DHS must carry out an adequate evaluation of technology prior to deployment.

Facial recognition technology should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, and its risks. As noted above, EPIC urges DOJ and DHS to ensure that impact assessments consider, at a minimum, several key factors related to the collection, use, dissemination, and retention of biometric data. These factors include:[115]

a. *Mission analysis and fit between mission and proposed use:* The stated purpose of the system, a detailed description of its capabilities, the permissible and impermissible uses of the system, and the justification for adopting the system.[116]

b. *Needless over-collection of data:* Information about the data collected for or by a system, including but not limited to the purpose for collection and the source(s) of the data.

every-reported-false-arrests-based-on-facial-recognition-that-person-has-been-black-2023-8; *see also* Letter from 18 Members of Congress to Merrick Garland, Att'y Gen. (Jan. 18, 2024), https://subscriber.politicopro.com/f/?id=0000018d-1ee1-d7e3-a9dd-1ff117dc0000&source=email (requesting "information about the U.S. Department of Justice's (DOJ) funding and oversight of facial recognition tools and other biometric technologies under the Civil Rights Act of 1964 and other applicable federal statutes and regulations").

[114] As NACDL has called for, review must ensure that these technologies "do not produce demographically-based disparate impacts or results, including in the confidence intervals, scores associated with possible matches, and in broader policing practices." *See* NACDL, Resolution on Facial Recognition Technology (Oct. 23, 2023), https://www.nacdl.org/Content/NACDL-Facial-Recognition-Resolution,-4AC-Draft.

[115] *See* EPIC Comments to OSTP, *supra* note 2, at 6; EPIC Comments to OMB re: Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum 18 (Dec. 5, 2023), https://epic.org/wp-content/uploads/2023/12/EPIC-OMB-AI-Guidance-Comments-120523-1.pdf.

[116] Systems designed for mass surveillance, like combined facial recognition and social media search systems, are presumptively overbroad and should not pass the initial evaluation stage.

c. *Lack of consent:* Information about data collection methods, including the scope of consent obtained (if any) and limitations on scraping.

d. *Failure to minimize:* Information about the management, retention, deletion, and transfer of data.

e. *Lack of transparency:* Information about the logic and development of a system.

f. *Lack of due diligence:* Initial tests regarding the accuracy and propriety of a system and information about ongoing tailored testing of a system. In addition to accuracy and propriety, audits and impact assessments must center civil rights, specifically testing for disproportionate impact based on race or other protected classes.

g. *Lack of accountability:* Any appeal procedures or harm mitigation strategies employed and information about key players, including the developer of a system, the user of a system, and the evaluators of the system.

Recommendation Six: DOJ and DHS must adopt a strict data minimization framework.

As noted above, there is a well-documented risk of lax data minimization rules leading to abuse, misuse, other harms.[117] We emphasize here that data minimization and preservation of an evidentiary record are not in tension. Data minimization should be a primary objective for 1:1 identity verification systems and for database design in 1:many identification systems. But once an investigation has begun, those data minimization procedures must also account for the need to retain robust records for audits and criminal litigation obligations.

Therefore, DOJ and DHS should adopt stricter data minimization procedures. EPIC recommends that these data minimization procedures include:

For identity verification systems:

- A prohibition on retention of faceprints and derived information after identity is confirmed.

For Search and Identification systems:

- Data minimization through access limitation so that the evidence resulting from a facial recognition search should only be accessible for the purposes of the investigation which prompted the search;

[117] *See supra* note 27.

- Robust forensic recordkeeping and disclosure to criminal defendants to satisfy Brady requirements; and
- Database design such that probe photos are not incorporated into the database or used to train the system.

For both types of system:

- Prompt deletion of all data acquired in violation of any of these rules or that is no longer permissibly retained; and
- Rigorous auditing of data retention and minimization practices.

Recommendation Seven: DOJ and DHS should ensure data is adequately secure.

As discussed above, adequate security is of paramount importance as the government and its vendors continue to sweep in more and more sensitive information.[118] It is all the more important with faceprints and information derived from facial recognition technology. Therefore, DOJ and DHS should strengthen security for all retained biometric data, including by requiring that:

- Faceprints and derived information should be encrypted and stored separately from other data;
- Access to this data should be limited to those who need it; and
- Data-handlers should assure the security of this data during transmission to third parties.

Recommendation Eight: DOJ and DHS should require independent auditing of technology.

As EPIC has argued more generally, "[r]obust, transparent, and independent audits of AI systems and their outputs are the gold standard for safely using any sort of automated system that impacts individuals."[119] And as the government has taken steps to improve AI governance, it too has recommended audits of rights-impacting AI systems like facial recognition to ensure that these

[118] *See supra* notes 28–29 and accompanying text.
[119] *See* EPIC, *Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making* 51 (Sept. 2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf.

systems are fair and accurate.[120] Therefore, DOJ and DHS should ensure that independent audits are a cornerstone of any law enforcement use of facial recognition technology.

While there is no single model audit, DOJ and DHS should require that audits of facial recognition technology have—at a minimum—several key characteristics. First, these audits should be conducted by a qualified, independent body, such as NIST, to ensure real results. Second, these audits should review both the inputs and outputs of these systems—the data used to train these programs and the decisions they produce. In doing so, audits should essentially replicate the circumstances under which facial recognition technology is actually used, including by using the types and quality of images in an operational setting, and it should measure accuracy across different criteria and demographics. Audits should be performed regularly—at least annually—and if these audits reveal harmful biases or inaccuracies, the use of that facial recognition technology should be immediately paused until that harm has been resolved adequately, if it can be.

Recommendation Nine: DOJ and DHS should strengthen accountability and oversight measures.

Across the government, agencies have failed to track the use of facial recognition and monitor against misuse. The GAO found that twenty law enforcement elements—of 42 surveyed—used facial recognition, and that the majority of these elements did not track use of these systems.[121] Another GAO report found that all seven reviewed agencies in DOJ and DHS initially used facial recognition services without requiring any training, and that the six agencies with available data had

[120] The White House recommends audits as part of its Blueprint for an AI Bill of Rights, and NIST includes audits, testing, and evaluation as core features of its AI Risk Management Framework.

[121] *See* U.S. Gov't Accountability Off., GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks 20 (2021), https://www.gao.gov/assets/gao-21-518.pdf,

cumulatively conducted roughly 60,000 searches without training requirements in place.[122] And as of April 2023, only two of these agencies had begun to require training.[123]

DOJ and DHS should also require all components carry out specialized training on facial recognition at regular intervals. This training should be robust, routine, and validated by external auditors. Training materials, guidance, and policies should be published to enhance transparency. And analysts conducting facial recognition searches should be regularly evaluated for compliance with these rules.

Relatedly, agencies should be required to build their systems to create audit logs of all use of facial recognition tools in support of incident reporting, audit, and oversight responsibilities. With these systems in place, agencies should be required to track incident reports—generated through these internal audits or the required independent audits mentioned above—to identify any errors, biases, or other documented harms of that agency's use of facial recognition, as well as any remedial measures that the agency plans to take to mitigate those harms.

Finally, DOJ and DHS should ensure that agencies are responsible for outcomes from the use of facial recognition technology, including by delineating consequence for agencies that fail to abide by these principles. Further, DOJ and DHS should enact strong accountability procedures as part of their compliance framework, with escalating consequences for agents who misuse or abuse of their access to these systems, including—but not limited to—revocation of that agent's access to the system, administrative sanction, or more serious penalties for willful misconduct.

[122] *See* U.S. Gov't Accountability Off., GAO-23-105607, Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties 19 (2023), https://www.gao.gov/assets/gao-23-105607.pdf.
[123] *Id.* at 20.

Recommendation Ten: DOJ and DHS should emphasize transparency and public trust.

Law enforcement agencies across the country have regularly adopted facial recognition technology in secret, evading the public scrutiny that is crucial to ensuring agencies stay within appropriate bounds. More than 1,800 agencies—at the federal, state, local, tribal, and territorial levels—have implemented and used facial recognition technologies with no meaningful oversight or even public notice.[124] Law enforcement agencies have routinely demonstrated this same hostility to transparency, in the context of facial recognition technology and other emerging surveillance practices.[125] DOJ and DHS should reverse course and adopt stronger transparency requirements for the use of facial recognition technology.

To start, DOJ and DHS should publish revised procedures governing procurement and use of facial recognition technology, including by detailing the circumstances in which private companies can sell or otherwise share biometric systems, biometric datasets, or data from those systems with DOJ or DHS components.[126] As noted recently in the Office of the Director of National Intelligence (ODNI) Senior Advisory Group Panel on Commercially Available Information, the intelligence community—including DOJ and DHS components—should develop more specific guidance on how agencies may procure and handle commercially-available biometric data, including what heightened

[124] Ryan Mac, Caroline Haskins, Brianna Sacks & Logan McDonald, *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, BuzzFeed News (Apr. 9, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

[125] *See Docs Show FBI Pressures Cops to Keep Phone Surveillance Secrets*, *supra* note 33; Dell Cameron, & Dhruv Mehrotra, *Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records*, Wired (Nov. 20, 2023), https://www.wired.com/story/hemisphere-das-white-house-surveillance-trillions-us-call-records/; Dell Cameron, *The FBI Just Admitted It Bought US Location Data*, Wired (Mar. 8, 2023), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/.

[126] *See* EPIC Comments to the UK ICO's Office for the Consultation on the Draft Biometric Data Guidance 6 (Oct. 20, 2023), https://epic.org/documents/epic-comments-to-the-uk-icos-office-for-the-consultation-on-the-draft-biometric-data-guidance/.

safeguards apply in this context.[127] These procedures should ensure that any procurement of facial recognition systems or information is consistent with EPIC's recommended principles.

DOJ and DHS should also publish transparency reports about the use of facial recognition technology. As other experts have previously recommended, this reporting could be modeled after the current disclosures in the Wiretap Act, including the number of searches run, the crimes for those searches were run to investigate, and the arrests and convictions resulting from those cases in which searches were run.[128] This reporting should also contain the number of noncompliant searches and a description of the remedial measures taken.

IV. Predictive Policing Algorithms

Person-based predictive policing tools (PBPPT) are technology that "[try] to measure the risk that a given individual will commit crimes."[129] These tools are used to take a targeted individual and assess the risk that a crime will occur or identify an individual who will commit a crime, often based on previous contact with the criminal justice system. However, PBPPT also encompasses other technologies such as emotion recognition and facial analysis technology that purport to detect aggression in the faces of students in schools to prevent school shootings.[130]

[127] *See* ODNI Senior Advisory Grp., Panel on Commercially Available Information, Report to the Dir. of Nat'l Intel. 35 (Jan. 27, 2022), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [hereinafter ODNI SAG Report] (calling for special rules around biometrics).

[128] Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Priv. & Tech. 64–65, https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[129] Ben Winters, *Layered Opacity: Criminal Legal Technology Exacerbates Disparate Impact Cycles and Prevents Trust*, 12 J. Nat'l Sec. L. & Pol'y 327, 330 (2021) (hereinafter "*Layered Opacity*").

[130] *See* Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 35, 2019),

Some of these tools are merely analog checklists, but more and more of these tools are being digitized and automated, to the detriment of civil liberties. Predictive analysis techniques are being added to other law enforcement tools. Some include school record risk assessment tools, face-based emotional recognition, auditory emotional recognition systems, and heat lists. The products are often little more than snake oil, based on faulty psychological studies bordering on phrenology. Regardless of the underlying statistical support or scientific methods, the tools are deployed in a biased manner against extremely vulnerable populations like poor people, Black people, students, and immigrants.[131] Even minor contacts with law enforcement, like being added to a database from a field interview, is potentially and statistically likely to be life ruining.[132]

a. DOJ and DHS Should Not Employ Predictive Policing Technologies Because They Are Untested, Riddled with Bias, and Rife with Systemic Issues.

https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/; Dave Gershgorn, '*Aggression Detection' Is Coming to Facial Recognition Cameras Around the World,* Medium (Sep. 25, 2020), https://onezero.medium.com/aggression-detection-is-coming-to-facial-recognition-cameras-around-the-world-90f73ff65c7f ; DHS, *Targeted Violence and Terrorism Prevention Grant Program*, https://www.dhs.gov/tvtpgrants (last visited Jan. 19, 2024); *Diverting Hate*, https://www.divertinghate.org/ (example of a DHS TVTP funded technology that purports to detect violent radicalization on social media).

[131] *See* EPIC Letter to Attorney General Garland Re: ShotSpotter Title VI Compliance, *supra* note 2 (petitioning DOJ to review the disproportionate deployment of ShotSpotter against minority populations); Stop LAPD Spying Coalition, *Automating Banishment: The Surveillance and Policing of Looted Land*, (Nov. 2021), https://automatingbanishment.org/assets/AUTOMATING-BANISHMENT.pdf (hereinafter "Automating Banishment") (discussing the use of PBPPT to over-police minority neighborhoods in Los Angeles); Dan Sullivan & Matt Cohen, *Pasco Sheriff discontinues controversial intelligence program, court documents say*, Tampa Bay Times (Mar. 23, 2023), https://www.tampabay.com/news/pasco/2023/03/23/pasco-sheriff-discontinues-controversial-intelligence-program-court-documents-say/ (Discussing Pasco County, Florida's overbroad deployment of PBPPT against students); Kathleen McGrory et al., *Targeted*, Tampa Bay Times, https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/ [hereinafter "*Targeted"*] (discussing the way Pasco County law enforcement officers targeted students using school records).

[132] Jon Swaine et al., *Young black men killed by US police at highest rate in year of 1,134 deaths*, Guardian (Dec. 31, 2015), https://www.theguardian.com/us-news/2015/dec/31/the-counted-police-killings-2015-young-black-men; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10228454/#CR24 ; Barry Holman & Jason Ziedenberg, *The Dangers of Detention: The Impact of Incarcerating Youth in Detention and Other Secure Facilities*, Justice Policy Institute, (Nov. 28, 2006), https://justicepolicy.org/wp-content/uploads/justicepolicy/documents/dangers_of_detention.pdf (Hereinafter "*Dangers of Detention*");

i. *Predictive Policing Tools Lack A Basis in Evidence Based Science, leading to tangible harms which force law enforcement to abandon costly and resource intensive projects.*

1. Criminal Intent Identifying Algorithms.

One category of PBPPT is software that analyzes faces and other biometric data for criminal intent. Adding behavioral and sociological analysis to an already flawed facial recognition technology adds a layer of discrimination to a deeply flawed product. The facial recognition technology underlying the emotional recognition systems, as stated in depth above, is rife with race and gender bias. However, analysis that attempts to identify criminal intent comes with its own problems. The technology itself is not based in sound science, the concept of malintent or criminal intent is a vague and internal process that is not measurable externally, and the technology could discriminate against the disabled community based on common cues associated with criminal intent.

First, these facial recognition algorithms are trained on images of faces, which are not capable of indicating a change in criminality or possible future criminality.[133] Second, eye movement tracking algorithms are suspect, and can be discriminatory against the disabled community. Several of the algorithms that attempt to identify criminal intent, when not using facial recognition, focus on eye movement, gait, and other soft biometrics.[134] Eye movement tracking to ascertain cognitive processing is based on unsubstantiated claims due to the fact that there is no evidence that outward

[133] One study found that when the facial images were controlled for race, gender, nationality, and age, there was no "subjectively meaningful typical face of criminals." Xioalin Wu & Xi Zhang, *Automated Inference on Criminality using Face Images*, arXiv (Nov. 13, 2016), https://arxiv.org/pdf/1611.04135v1.pdf. There is no meaningful, visual change in a person's facial appearance after conceiving, committing, or being convicted of a crime. *See* Kevin W. Bowyer et al., *The "Criminality From Face" Illusion*, 1 IEEE Transactions on Tech. & Society 175, 183(Dec. 2020), https://ieeexplore.ieee.org/document/9233349.

[134] *See, e.g.*, DHS Sci. & Tech. Directorate, Future Attribute Screening Technology, https://www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST.pdf (last visited Jan. 21, 2024.)

features like eye movement reliably indicate inward processes like intent.[135] Finally, eye movement tracking technology can be used to diagnose Autism, Parkinson's, Alzheimer's, and psychiatric conditions like depression.[136] Individuals with Autism Spectrum Disorder typically look at people's mouths rather than making eye contact.[137] Under the so-called criminal intent identifying algorithms, these individuals would be read as having criminal intent when no such intent actually exists, making the technology less reliable and more high risk.

Finally, some schools and hospitals in the United States are deploying auditory aggression detectors trying to identify school shooters or other violent individuals before an incident can occur despite the lack of evidence that the product works.[138] The microphones pick up the auditory landscape and capture "sound patterns deemed aggressive."[139] Some experts contest the fact that verbal aggression "precedes school violence" and argue that increased surveillance could "increase[] student distrust and alienation."[140] A popular product offering these services in the United States, Sound Intelligence, developed its aggression detector by placing microphones in a Dutch pub district

[135] Studies have debunked the idea that eye movement is a reliable indicator of lying, *see* Richard Wiseman et al., *The eyes don't have it: lie detection and Neuro-Linguistic Programming*, 7 PLoS ONE (Jul. 12, 2012); and that the start position of the eyes, a marker that can "indicate [a] location is optimal for information extraction," is the result of "a complex combination of visuo-motor effects and simple sampling strategies as well as cognitive factors" that are "very difficult to tease apart". Joseph Arizpe et al., *Start Position Strongly Influences Fixation Patterns during Face Processing: Difficulties with Eye Movements as a Measure of Information Use*, 7 PLoS ONE (Feb. 2, 2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3271097/. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0040259; and that the start position of the eyes, a marker that can "indicate [a] location is optimal for information extraction," is the result of "a complex combination of visuo-motor effects and simple sampling strategies as well as cognitive factors" that are "very difficult to tease apart". Joseph Arizpe et al., *Start Position Strongly Influences Fixation Patterns during Face Processing: Difficulties with Eye Movements as a Measure of Information Use*, 7 PLoS ONE (Feb. 2, 2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3271097/.

[136] Ian Taylor Logan, *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 Penn. St. L. Rev. 779, 783–85 (2019).

[137] Corinne Green & Kun Guo, *Factors contributing to individual differences in facial expression Categorization* 5 (2018), https://core.ac.uk/download/pdf/76999954.pdf.

[138] Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students,* ProPublica (June 35, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.

[139] *Id.*

[140] *Id.*

and cross-referencing police reports of aggressive behavior.[141] This product has since been primarily deployed in U.S. schools, which is dangerous due to the stark differences in setting and population between the training subjects and the final target population.[142]

These algorithms are not transparent and do not always explain what factors determine the different outputs deemed to be aggressive or criminal.[143] In fact, government watchdogs have already flagged the lack of evidence behind this type of tool. In 2017, the GAO found that TSA's behavioral detection and analysis techniques, a list of behaviors TSA agents watch out for to recommend travelers for increased scrutiny during the airport security process, were based on a list of behavioral indicators that was supported by little to no empirical evidence.[144] This is the second report GAO published on the matter, with no changes in recommendations from the original report since TSA was still unable to provide sufficient evidence that the behavioral indicators it deemed as suspicious activity were scientifically proven to be linked to risky or criminal behavior, even four years later.[145] As recommended by the GAO, this type of technology should not be funded or used due to the lack of sufficient scientific evidence proving the efficacy of the methods being used to assess human behavior.[146]

[141] *Id*.

[142] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37 Revision 2, 59 (Dec. 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[143] *See, e.g.*, GAO, GAO-20-72, Aviation Security: TSA Coordinates with Stakeholders on Changes to Screening Rules but Could Clarify Its Review Processes and Better Measure Effectiveness, 11–14 (2019), https://www.gao.gov/assets/gao-20-72.pdf.

[144] Letter from Nancy R. Kingsbury, Managing Dir., Applied Rsch. & Methods, GAO, & Jennifer A. Grover, Dir., Homeland Sec. & Just. Issues, GAO, to Rep. Bennie G. Thompson, Ranking Member, Comm. on Homeland Sec., & Rep. Bonnie Watson Coleman, Ranking Member, Subcomm. on Transp. & Protective Sec. (July 20, 2017), https://www.gao.gov/assets/gao-17-608r.pdf.

[145] GAO, GAO 14-159, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, 47 (2013), https://www.gao.gov/assets/gao-14-159.pdf [hereinafter "GAO TSA Behavior Detection Report"].

[146] *Id.*

2. Heat Lists.

The Chicago Police Department's heat lists, the Strategic Subject List (SSL) and Crime and Victimization Risk Model (CVRM), are the most direct examples of person based predictive policing tools, with the primary goals of "rank[ing] individuals with a criminal record according to their probability of being involved in a shooting or murder, either as a victim or an alleged offender."[147] The SSL and CVRM achieve this by estimating "an individual's risk of becoming a victim or a possible offender in a shooting or homicide in the next 18 months based on risk factors in a person's recent criminal or victimization history."[148] These algorithms used some of the following factors in its analysis: the number of times an individual was a victim of a shooting and/or aggravated battery or assault; an individual's age during their most recent arrest; an individual's recent criminal activity; and an individual's gang affiliations.[149] Neither of these models were evaluated, nor were there adequate controls on the data or adequate training for officers.[150] The Chicago Police Department began to phase out the use of these risk models in 2019.[151]

The Los Angeles Police Department (LAPD) had a similar program called the Chronic Offender Bulletin as a part of Operation LASER, or the Los Angeles Strategic Extraction and Restoration program.[152] LAPD gathered information from routine, non-adversarial police activity

[147] Chi. Police Dep't Special Order S09-11, *Strategic Subject List (SSL) Dashboard* (2016), https://perma.cc/YJ72-YJEG; *see also Layered Opacity*, *supra* note 129 at 332.
[148] Brianna Posadas, *How Strategic is Chicago's "Strategic Subjects List"? Upturn Investigates*., Equal Future (June 22, 2017), https://medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c.
[149] *Id.*; *see also* Layered Opacity, *supra* note 129, at 332.
[150] Chi. Inspector Gen.'s Off., *Advisory Concerning the Chicago Police Department's Predictive Risk Models* 4 (2020), https://perma.cc/6449-KSY4.
[151] *See Layered Opacity*, *supra* note 129, at 334.
[152] Craig D. Uchida et al., *The Los Angeles Smart Policing Initiative: Reducing Gun-Related Violence Through Operation LASER, Smart Policing: Research Snapshot*, Bureau of Just. Assistance, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/losangelesspi.pdf.

data which was then analyzed.[153] which was then analyzed. From that information, a list of "chronic offenders" was created and input into Palantir, an infamous data analytics software company,[154] to create thorough, but "information only" documents called Chronic Offender Bulletins.[155] These documents did not reflect individuals with outstanding warrants or someone who was wanted in relation to a particular crime, and did not grant police officers probable cause to stop individuals, instead, intended to improve "situational awareness."[156] The chronic offenders were then assigned a point value and ranked accordingly.[157] Those with the highest scores were collated into a spreadsheet with basic PII and were assigned field officers.[158] However, a report by the Office of the Inspector General found that 112 of the 637 people on the database had zero points under the LAPD's criteria.[159] The Stop LAPD Spying Coalition found that nearly half of the targeted individuals were Black, despite the city's population only being 9% Black.[160] Individuals on the list were the target of specialized Operation LASER units that would proactively monitor, serve warrants, conduct parole and probation checks (despite not being parole or probation officers), and stopping individuals.[161]

[153] Such activities include daily patrols, the Parole Compliance Unit, field interview cards, traffic citations, release from custody forms, crime and arrest reports, and criminal histories. *See* Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* 62 (2021) [hereinafter "*Predict and Surveil*"].

[154] Palantir, *About*, https://www.palantir.com/about/ (last visited Jan. 19, 2024); *see, e.g.,* Mara Hvistendahl , *How the LAPD and Palantir use Data to Justify Racist Policing*, Intercept (Jan. 30, 2021), https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing/. Palantir is also suspect in civil contexts. *See, e.g.*, Sam Levin, *Palantir to pay $1.7m over accusation it discriminates against Asian Applicants*, Guardian (Apr. 26, 2017), https://www.theguardian.com/technology/2017/apr/26/palantir-racial-discrimination-lawsuit-asians-peter-thiel.

[155] The bulletins included several pieces of personal information such as name, California Information and Identification numbers, physical descriptions, police history, and CalGang designation. *See Predict and Surveil*, *supra* note 153, at 62.

[156] *Id.*

[157] Examples of point values include five points for having a known gang affiliation, five points for a violent crime on the individual's rap sheet, and a point for every contact with law enforcement (including non-custodial stops). *Id.*

[158] *Id.*

[159] L.A. Police Comm'n, Off. of the Inspector Gen., *Review of Selected Los Angeles Police Department Data-Driven Policing Strategies* 15 (Mar. 12, 2019), http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.

[160] *See Automating Banishment*, *supra* note 131, at 15.

[161] *See Automating Banishment*, *supra* note 131, at 18.

Some individuals were stopped as many as four times a day by police officers.[162] After the release of the damning OIG report, the LAPD announced that it would end Operation LASER, including its broad location based predictive policing arm, admitting that the program was "an experiment."[163] However, just a year later, LAPD announced a new data-driven policing framework with a "community policing" perspective focused on police accountability that proved to be eerily similar to Operation LASER.[164] Despite the shift in language to one of police reform, several of Operation LASER's components were merely renamed and reinstated wholesale.[165]

3. DHS' Automated Targeting System (ATS).

DHS' Automated Targeting System (ATS) is a tool that collates several sources of information such as federal law enforcement data; classified intelligence; and commercially available data, to assess risk in imports, exports, and travel in and out of the United States.[166] CBP created a set of rules based on historical data and "patterns of suspicious activity" that indicate whether a target is at a higher risk of committing a crime, such as overstaying a visa or engaging in terrorism.[167] While there are several privacy impact assessments published,[168] little is known about ATS, the rules CBP created, how the predictive modeling works, how DHS agents engage with the system, or how the tool is operationalized. In fact, there are multiple reports from the GAO urging

[162] *See Predict and Surveil*, *supra* note 153, at 69. Some individuals even received home visits where officers would tell them the police were watching them. *See Automating Banishment*, *supra* note 131, at 16. This tactic of targeted and frequent police interactions resulted in the deterioration of neighborhoods by incarcerating mass quantities of individuals and applying the "self-deportation approach," which forces individuals to leave a neighborhood due to intolerable conditions. *Id.*; *see also* Sue Park, *Self-Deportation Nation*, 132 Harv. L. Rev. 7, 1880–84 (May 10, 2019), https://harvardlawreview.org/2019/05/self-deportation-nation/.

[163] L.A. Police Comm'n, *Regular Meeting* (April 9, 2019), https://www.youtube.com/watch?v=pr7ZY_3vNQo.

[164] *See Automating Banishment*, *supra* note 131, at 69.

[165] *Id.*

[166] DHS, DHS/CBP/PIA-006 Automated Targeting System – January 2017 – Appendix Update 1–3 (Jul. 2022), https://www.dhs.gov/publication/automated-targeting-system-ats-update.

[167] *Id.* at 4.

[168] DHS, DHS/CBP/PIA-006 Automated Targeting System (May 2022), https://www.dhs.gov/publication/automated-targeting-system-ats-update.

the department to conduct reviews of the system to ensure that the system is based on high quality data and is actually achieving its intended purpose.[169] For example, ATS is comprised of systems that are riddled with issues, such as federal terrorist watch lists that are filled with factual errors,[170] are based on unreachable goals,[171] and are composed of a vastly disproportionate number of Muslim individuals.[172] ATS also draws from commercially available data, such as spending $2 million on a contract with Google Maps as well as acquiring mobile application data from companies like Venntel.[173] Rather than scale back its usage of ATS or reviewing ATS' capabilities, though, DHS has expanded use of ATS to continually monitor certain categories of immigrants and individuals traveling in and out of the United States, according to a recently released DHS report on data mining.[174]

[169] *See* GAO, GAO-11-742, Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism 32-33(2011), https://www.gao.gov/assets/gao-11-742.pdf; GAO, GAO-14-531, Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness 37 (2014), https://www.gao.gov/assets/gao-14-531.pdf; GAO, GAO-20-72, Aviation Security: TSA Coordinates With Stakeholders on Changes to Screening Rules but Could Clarify Its Review Processes and Better Measure Effectiveness 18 (2019), https://www.gao.gov/assets/gao-20-72.pdf.

[170] Rachel Levinson-Waldman & José Guillermo Gutiérrez, *Overdue Scrutiny for Watch Listing and Risk Prediction*, Brennan Ctr. for Just., 3 (Oct. 19, 2023), https://www.brennancenter.org/our-work/policy-solutions/overdue-scrutiny-watch-listing-and-risk-prediction.

[171] GAO, GAO-20-72, Aviation Security: TSA Coordinates With Stakeholders on Changes to Screening Rules but Could Clarify Its Review Processes and Better Measure Effectiveness (2019), https://www.gao.gov/assets/gao-20-72.pdf.; Timme Bisgaard Munk, *100,000 false positives for every real terrorist: Why anti-terror algorithms don't work*, First Monday (Sep. 4, 2017), https://firstmonday.org/ojs/index.php/fm/article/view/7126/6522.

[172] *See* Council on Am.-Islamic Rels., *Twenty Years Too Many: A Call to Stop the FBI's Secret Watchlist* , 1 (2023), https://www.cair.com/wp-content/uploads/2023/06/watchlistreport-1.pdf; Levinson-Waldman & Guillermo Gutiérrez, *supra* note 170, at 3.

[173] Thomas Brewster, *Border Patrol Spent $2 Million on Google Maps for a Massive Surveillance Tool*, Forbes (Oct. 13, 2020), https://www.forbes.com/sites/thomasbrewster/2020/10/13/cbp-spent-2-million-on-google-maps-for-a-massive-surveillance-tool/.

[174] DHS, *2020 and 2021 Data Mining Report,* 16-33 (Aug. 2022), https://www.dhs.gov/sites/default/files/2023-08/23_0831_priv_dhs-data-mining-report.pdf.

ii. *Systemic Issues render the use of predictive policing technology inappropriate for the context in which law enforcement officials want to deploy them.*

1. ***Predictive policing technology is based on discriminatory policing patterns.***

Even if these algorithms were assessed appropriately for empirical accuracy based on the set parameters, PBPPT, particularly heat lists, work by analyzing a flawed set of training data. The developers of these algorithms purport to revolutionize policing, but strictly look back at policing's biased past and extend and entrench the ugly practices far into the future. Predictive technology trained on historical policing data reinforces the over policing of majority minority neighborhoods and communities, while dehumanizing those communities and adding a veneer of legitimacy and objectivity through "hard data."

Law enforcement historically and presently target Black and Latinx communities at disproportionate rates,[175] leading to lopsided arrest records which train the new, now lopsided, algorithms. Several agencies, including the DOJ, have noted that if the datasets "incorporate historical bias," the automated systems based on those datasets may contribute to unlawful

[175] *See* Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to be Dismantled.*, MITTech. Rev. (July 17, 2020), https://perma.cc/DS5L-JQRD (citing Office of Juvenile Justice and Delinquency Prevention Statistical Briefing Book for 2020, noting that black people were twice as likely to get arrested than white people and that black people were five times as likely to be "stopped without just cause" as white people); *Layered Opacity*, *supra* note 129, at 334 ("Any tool that predicts future crime based on past and current arrest data will be necessarily flawed and biased. Nationwide, police have been shown to arrest black people at a higher rate than white people, stop more black and Hispanic men than white men, and use force on black men at a significantly higher rate than other demographics"); Dhruv Mehrotra et al., *How We Determined Crime Prediction Software Disproportionately Targeted Low-Income, Black, and Latino Neighborhoods*, Markup (Dec. 2, 2021), https://themarkup.org/show-your-work/2021/12/02/how-we-determined-crime-prediction-software-disproportionately-targeted-low-income-black-and-latino-neighborhoods ("We found that in nearly 66 percent of the 131 stable block groups, predictions clustered on the blocks with the most Black or Latino residents inside of those block groups. Zooming in on blocks showed that predictions that appeared to target majority-White block groups had in fact targeted the blocks nestled inside of them where more Black and Latino people lived. This was true for 78 percent of the 46 stable, majority-White block groups in our sample."); Susannah N. Tapp & Elizabeth J. Davis, *Contacts Between Police and the Public, 2020, Bureau of Justice Statistics*, DOJ, 1 (Nov. 2022), https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/cbpp20.pdf ("Black (6%) and Hispanic (3%) persons were more likely to experience the threat of force or use of nonfatal force during their most recent police contact in 2020 than white persons (2%).").

discrimination.[176] Running the data through a series of math formulas and code does not substantively change the biased nature of the original data that determines the rules in the new algorithm. However, the sterile nature of an algorithm provides a veneer of legitimacy and objectivity that ignores the biased outputs and biased misuses of the technology. Even if the algorithm developers attempt to control for biased results by using data not facially tied to protected classes like race or gender, this problem persists. Certain types of data can function as pretext for protected classes, like zip codes as an almost direct analogue to race.[177]

Past arrest records and policing data also aren't synonymous with actual perpetration of crime. Arrest records do not guarantee that a suspect will be convicted, or even indicted.[178] Operation LASER recommended that police officers fill out field interview cards for every interaction while patrolling, gathering data on individuals who were not officially stopped, wanted for questioning, brought into custody, or otherwise involved in criminal matters.[179] This makes even the most innocuous police contact an entrance point to the mass surveillance network and further law enforcement scrutiny.

2. *Children are a vulnerable population and law enforcement contact, particularly automated contact, should be minimized.*

a. Children are legally distinct from adults, particularly with regards to the imposition of punishment.

Children enjoy several types of legally recognized protections in the criminal justice system. It is theorized that juveniles lack the brain development, particularly in the pre-frontal cortex which

[176] CFPB, DOJ, U.S. Equal Employment Opportunity Comm'n, FTC, Joint Statement on enforcement Efforts Against Discrimination and Bias in Automated Systems (Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[177] Michael Carl Tschantz, *What is Proxy Discrimination?*, 2022 ACM Conf. on Fairness, Accountability, & Transparency 1993, 2002 (June 2022), https://dl.acm.org/doi/pdf/10.1145/3531146.3533242.

[178] Nat'l Inst. of Just., *Arrests Without Conviction: How Often They Occur and Why,* 19–33 (1983), https://www.ojp.gov/pdffiles1/Digitization/90815NCJRS.pdf.

[179] *See Predict and Surveil*, *supra* note 153, at 63.

acts as the center for executive function decision-making, compared to adults.[180] This lack of development leads to a "period of heightened vulnerability to risk taking" in early adolescence.[181] The Supreme Court recognizes this difference, and over the years has struck down punishments that go too far, such as the death penalty, life without parole for a nonhomicide offense, and finally life without parole for a homicide offense.[182] Juveniles are more likely to desist from involvement in criminal activity as they mature, thus they are less likely than their adult counterparts to be "'incorrigible criminals."[183] The point of heightened protection is not to excuse culpability or bad behavior, but to develop strategies to address the root issues such as mental health, access to housing, and other sociological factors that better determine criminality.[184] Introducing children to the criminal justice system, even through minor police contact, can begin a campaign of police targeting and a path of no return.[185] Despite this vulnerable status, law enforcement have begun to take an "intelligence led" perspective to policing, going as far as predicting which children will lead a life of crime based on school discipline records and taking corrective action.[186]

[180] *See, e.g.,* Mariam Arain et al., *Maturation of the Adolescent Brain*, 9 Neuropsychiatric Disease & Treatment 449, 453–55 (2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3621648/pdf/ndt-9-449.pdf.

[181] Nadia Rossbach, *Innocent Until Predicted Guilty: How Premature Predictive Policing Can Lead to a Self-Fulfilling Prophecy of Juvenile Delinquency*, 75 Fla. L. Rev. 167, 184 (2023).

[182] *See Roper v. Simmons*, 543 U.S. 551, 574–75, 578 (2005); *Graham v. Florida*, 560 U.S. 48, 74–75, 82 (2010); *Miller v. Alabama*, 567 U.S. 460, 479, 489 (2012).

[183] Elizabeth S. Scott, *"Children are Different": Constitutional Values and Justice Policy*, 11 Ohio St. J. Crim. L. 71, 85 (2013) (quoting *Miller*, 567 U.S. at 471–72); William R. Kelly, *The Future of Crime and Punishment: Smart Policies for Reducing Crime and Saving Money* 203 (2016) [hereinafter *The Future of Crime and Punishment*].

[184] *See The Future of Crime and Punishment*, *supra* note 183, at 203.

[185] *See infra* notes 191–93.

[186] *See Targeted, supra* note 131 (case study of a Pasco County, Florida's use of school records to visit students at home before any crime was committed or suspected); *see also,* Pasco Sheriff's Off., ILP Manual, 3–4 (2016), https://www.flsheriffs.org/uploads/docs/ILP_manual_final_edit_010716.pdf (discussing Pasco County's policy on integrating "intelligence led policing" techniques to advance law enforcement goals.)

b. Increasing law enforcement engagement with students does not reduce criminal conduct.

The idea of increasing the presence of school resource officers and law enforcement risk assessments of children based on school records is based on the faulty premise that this intervention will set kids straight, but this could not be farther from the truth. The more a child engages with law enforcement, the more likely they are to enter the revolving door of the criminal justice system. Detention of minors seriously increases the risk of serious mental health issues and increases the chances of reoffending.[187] There is no evidence that school resource officer presence in schools reduces criminal conduct, but there is evidence that students feel more unsafe in their presence and that Black and Latinx students are faced with disproportionate uses of force more often than their white peers due to student resource officer presence.[188] The feeling of unease and anxiety could trigger abnormal behavior and set off other criminal intent identifying algorithms on accident, general feelings of alienation between peers and towards the school administration, and create adversarial relationships between students and school officials.[189] Furthermore, bringing law enforcement into the school setting only exacerbates the school to prison pipeline which disproportionately drives Black students into youth and adult punishment systems.[190]

[187] *See* Barry Holman & Jason Ziedenberg, *The Dangers of Detention: The Impact of Incarcerating Youth in Detention and Other Secure Facilities*, Just. Pol'y Inst. 7 (2013), https://justicepolicy.org/wp-content/uploads/justicepolicy/documents/dangers_of_detention.pdf [hereinafter "*Dangers of Detention*"].
[188] *See, e.g.*, Advancement Proj., *#AssaultAtSpring Valley: An Analysis of Police Violence* 5 (Dec. 12, 2022), https://policefreeschools.org/resources/assaultat-spring-valley-an-analysis-of-police-violence/; *School Resource Officers and the School-to-Prison Pipeline: Evaluating Responses to School Safety Concerns in an Age of School Shootings and Renewed Calls for Racial Justice*, Just. Pol'y Inst. (2022), https://justicepolicy.org/wp-content/uploads/2023/03/IOPxJPI-Final-Brief20.pdf; Jason P. Nance, *Students, Police, and the School-to-Prison Pipeline*, 93 Wash. U. L. Rev. 919, 924–26 (2015), https://journals.library.wustl.edu/lawreview/article/4451/galley/21284/view/.
[189] Nance, *supra* note 188, at 948–49.
[190] *Id.* at 952–54; Emily K. Weisburst, *Patrolling Public Schools: The Impact of Funding for School Police on Student Discipline and Long-term Education Outcomes*, 38 J. of Pol'y Analysis & Mgmt. 338, 340 (2019); Daniel J. Losen & Paul Martinez, Is *California Doing Enough to Close the School Discipline Gap? The Center for Civil Rights Remedies*, UCLA Civil Rights Project (Jun. 21, 2020), https://www.civilrightsproject.ucla.edu/research/k-12-education/school-discipline/is-california-doing-enough-to-close-the-school-discipline-gap.

c. Under FERPA, school records shouldn't be shared with law enforcement under FERPA without parental consent.

Law enforcement have extended their presence in school settings from mere school resource officers to combing general school records to increase law enforcement interventions. Up to 95% of out-of-school suspension, one of the most severe consequences available to punish students, are related to nonviolent misbehavior, such as "being disruptive, acting disrespectfully, tardiness, profanity, and dress-code violations."[191] When even the most severe consequences are barely related to violent misbehavior, it is a disproportionate response to share school records, even beyond disciplinary records, with law enforcement. The presence of student resource officers often leads to the disproportionate use of force, like bodily restraints that turn into assault, and escalated consequences like expulsion on students for minor infractions.[192] If law enforcement presence were extended to students outside of the school campus like it was in Pasco County, then minors who are supposed to dedicate their lives to learning and growing up peacefully instead have to deal with court fees, legal challenges, and extended police harassment campaigns.[193] For those reasons, law enforcement shouldn't be given access to student records.

The transfer of such data from schools to law enforcement is suspect and may interfere with the Family Educational Rights and Privacy Act (FERPA). FERPA gives parents rights over the data schools collect about their children until the age of 18, whereupon the rights transfer to the

[191] U.S. Comm'n on Civ. Rts., *Beyond Suspensions: Examining School Discipline Policies and Connections to the School-to-Prison Pipeline for Students of Color with Disabilities*, 32–33 (Jul. 2019), https://www.usccr.gov/files/pubs/2019/07-23-Beyond-Suspensions.pdf.

[192] Tim Stelloh & Tracy Connor, *Video Shows Cop Body-Slamming High School Girl in S.C. Classroom*, NBC News (Oct. 26, 2015), https://www.nbcnews.com/news/us-news/video-appears-show-cop-body-slamming-student-s-c-classroom-n451896.

[193] Dan Sullivan & Matt Cohen, *Pasco Sheriff discontinues controversial intelligence program, court documents say*, Tampa Bay Times, (Mar. 23, 2023), https://www.tampabay.com/news/pasco/2023/03/23/pasco-sheriff-discontinues-controversial-intelligence-program-court-documents-say/; *Automating Banishment*, *supra* note 131, at 16.

student.[194] Among the rights, parents have the rights to request the data schools have collected, as well as correcting any incorrect information.[195] Generally, schools need permission to share data, but under 34 CFR 99.31, schools can share information to "state and local authorities, within a juvenile justice system, pursuant to specific State law" and/or to comply with a "judicial order or lawfully issued subpoena."[196] However, in Pasco County, these records were sent wholesale to allow law enforcement to assess the risk of criminality in each child, not targeted to a specific child under a court order or subpoena.[197] Depending on the state, law enforcement may be entitled to this data, but largely FERPA would bar the transfer of data without parental consent.

b. DOJ and DOJ Must Adhere to Strong Safeguards to Mitigate Risk When Using Predictive Policing Tools.

EPIC strongly urges DOJ and DHS to reconsider their funding and use of predictive policing technology due to the severe and systemic risks associated with the tools. Developing more accurate tools will not erase the fact that these technologies accelerate and entrench existing discriminatory policing practices. Because of efficacy issues and systemic risks that infringe on core civil rights, DOJ and DHS should proactively engage with its privacy officers, oversight boards, and employees at every level to ensure that the following guidelines are met.

Recommendation One: DOJ and DHS should prohibit mass surveillance.

DOJ and DHS must stop using predictive policing technologies to enhance and accelerate the mass surveillance ecosystem. Many of these technologies involve innocent individuals in massive data sets that lack transparency and oversight. This creates opportunities for law enforcement to

[194] 34 C.F.R. § 99.5(a)(1).
[195] 34 C.F.R. § 99.10.
[196] 34 C.F.R. § 99.31(9)(i).
[197] *Targeted*, *supra* note 131.

monitor and harass[198] individuals (mostly from vulnerable populations) who would otherwise have no reason to interact with the criminal justice system at a higher rate than other individuals.[199]

Specifically, DOJ and DHS should create standards to discern a threshold for law enforcement intervention. These algorithms do not predict the commission of a crime, nor do they indicate conclusive evidence that a person has committed a crime.[200] Law enforcement intervention, such as performing a home visit, should be limited to situations where further investigation has occurred and information has been collected that indicates an actual crime has been committed. These algorithms should not constitute probable cause, and a search warrant should not be approved if the only evidence contained therein is from a predictive technology.

Furthermore, DOJ and DHS should limit the use of these technologies to situations where there is an ongoing investigation with individuals who have already been identified. Predictive technologies create an unprecedented opportunity for fishing expeditions,[201] and should only be used to create more in-depth profiles on existing targets, rather than attempting to identify new targets for investigation.

Recommendation Two: DOJ and DHS should protect civil rights by prohibiting arrests and adverse immigration decisions based solely on predictive policing tools.

Predictive policing technology does not indicate commission of a crime, it is merely a tool that increases situational awareness and alerts law enforcement to potential threats, so it should not be sole basis of an arrest. Aggression sensors and emotional recognition in general are technologies

[198] Under Operation LASER, some individuals received home visits where officers would tell them the police were watching them. *See Automating Banishment*, *supra* note 131, at 15. This tactic of targeted and frequent police interactions resulted in the deterioration of neighborhoods by incarcerating mass quantities of individuals and applying the "self-deportation approach," which forces individuals to leave a neighborhood due to intolerable conditions. *Id.*.

[199] Council on Am.-Islamic Rels., *supra* note 172, at 8; *Targeted*, *supra* note 131; *Automating Banishment*, *supra* note 131, at 15.

[200] *See supra* notes 158–99 and accompanying text.

[201] *See, e.g.*, *Predict and Surveil*, *supra* note 153, at 17–36.

based on faulty science and should not be deployed until adequate evidence-based research can demonstrate objective connections between inputs and actual crime commission.[202] Furthermore, the increased monitoring of individuals on heat lists is a self-fulfilling prophecy, because the more monitoring and scrutiny an individual receives, the more likely law enforcement are to find something incriminating regardless of prior history.[203] DOJ and DHS must draft guidelines as to when intervention following an alert from the technology is prudent, and when further investigation is necessary to ensure the technologies are not accelerating disparate impact.[204] Predictive policing technologies should not constitute probable cause, and search warrants based solely on outputs from these technologies should not be approved.

Recommendation Three: DOJ and DHS should protect criminal defendants' Constitutional rights by requiring adequate notice of the use of predictive policing tools and ensuring that the technology is subject to adversarial interrogation during criminal litigation.

In the predictive policing context, access to exculpatory evidence should include the disclosure of the tools law enforcement used in their investigation, including any predictive technologies that identified the defendant as a suspect. The accuracy and reliability results from audits and Privacy Impact Assessments (PIAs) resulting from the acquisition of these technologies are also relevant information to the defendant, particularly if law enforcement have little evidence beyond the outputs of these technologies.

Recommendation Four: DOJ and DHS should ensure technology is provably non-discriminatory prior to deployment.

Several of these technologies are biased based on the datasets they were created on, leading to outputs that skew towards marking vulnerable populations as criminal. When drafting PIAs for these technologies, DOJ and DHS should consider how these technologies affect vulnerable

[202] *See supra* notes 133–74.
[203] *See Automating Banishment*, *supra* note 131, at 58–62.
[204] *See supra* notes 179–97.

populations and incorporate recommendations to mitigate the risk of those harms. Furthermore, during the evaluation of the technology done during procurement and periodically after deployment, disparate impact based on protected class status should be an explicit component of the testing. If the technology cannot be verified to be non-discriminatory, it should not be deployed. Finally, under Title VI, the federal government is barred from funding discriminatory technology, and DOJ and DHS should cease further funding of new technologies until non-discrimination can be empirically proven.[205]

Recommendation Five: DOJ and DHS must carry out an adequate evaluation of technology prior to deployment.

Before acquisition and deployment, DOJ and DHS should develop and consistently carry out evaluations of technology beyond mere accuracy and efficacy. The problem that a technology will solve within a department's mission should be explicitly defined, and objective measures to assess whether the technology is meeting that goal should be set.[206] When drafting PIAs, DOJ and DHS should interrogate why the technology is being acquired to ensure that the advertised goal of the technology, such as evaluating an individual's criminality, is a valid, actionable goal with objective measures that the algorithm's efficacy can be tested against.[207] Furthermore, DOJ and DHS should ensure that the acquisition of the technology will measurably advance the department's mission and provide value to the officers using it.

Recommendation Six: DOJ and DHS Should Adopt a Strict Data Minimization Framework

Data minimization is important for privacy, minimizing downstream harms, and ensuring appropriate cybersecurity.[208] DOJ and DHS should only gather information that is legitimately

[205] *See also* GAO TSA Behavior Detection Report, *supra* note 145, at 47–48.
[206] *See infra* notes 254–68.
[207] *See supra* notes 166–74 and accompanying text.
[208] *See supra* note 28–29 and accompanying text.

gathered under state and federal law and that is narrowly tailored to specific, existing investigations to inform these datasets and algorithms. School records, even in-school disciplinary records, should not be transferred to law enforcement without the express consent of parents or the eligible student.[209] School records are sufficiently sensitive that they should be deleted from all law enforcement systems once the relevant investigation have been completed. DOJ and DHS should create standards to discern when data collected from routine, daily police activity should be included in predictive algorithms, minimizing the data submitted to these systems to that which is narrowly tailored to a specific investigation and align with the goals of the technology.[210]

Recommendation Seven: DOJ and DHS should ensure data is adequately secure.

Predictive technology, particularly heat lists and those based on biometric information, rely on highly sensitive data. This data is often stored in large, interconnected databases that interact with third party software, like Palantir, for analysis.[211] DOJ and DHS must identify and fund adequate security protocols and infrastructure to protect these databases. When working with third parties to analyze existing data or acquire new data (such as through commercial data broker contracts), DOJ and DHS should create strict protocols to ensure the risk of data breaches are minimized and ensure that the vendors are upholding strict data security protocols within their own systems. Finally, DHS and DOJ should limit the transfer of sensitive data to third party vendors and limit third party vendor access to databases that include PII to that which is necessary for the vendor to do its contracted work.

[209] *See supra* notes 191–97 and accompanying text.
[210] *See Predict and Surveil*, *supra* note 153, at 62–64.
[211] *See supra* notes 166–74 and accompanying text.

Recommendation Eight: DOJ and DHS should require independent auditing of technology.

First and foremost, DOJ and DHS should halt any current grants, funding opportunities, and/or other procurement processes until DOJ and DHS publish the studies ordered by the 2022 executive order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety and implement any recommendations found therein.[212]

Secondly, during the procurement process and periodically after deployment, DOJ and DHS must engage in several rounds of testing to ensure that the technology is provably non-discriminatory. In response to the recent sweeping AI Executive Order, the Office of Management and Budget (OMB) published a draft memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence. With the digitization of predictive policing technologies, DOJ and DHS should follow OMB's recommendations with regards to non-discrimination measures to ensure adequate protections.[213] Some of the most salient recommendations include:

- Pre-deployment AI impact assessments that identify uses, risks, limitations, and data misuse or overuse;[214]
- Ongoing and independent AI testing to ensure the systems continue to be accurate, reliable, and unbiased as the machine learning algorithms learn from new data;[215] and

[212] Exec. Order No. 14,074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety § 13, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/ (requesting reports including an investigation on ensuring timely and thorough investigations related to deadly force or death in custody, consistent discipline relating to use of deadly force or death in custody, best practices relating to law enforcement officer wellness, information on no-knock entries, among several other reports).

[213] Request for Comments on Advancing Governance, Innovation, and Risk Management for agency Use of Artificial Intelligence Draft Memorandum, OMB, 86 Fed. Reg. 75625 (Nov. 3, 2023) [hereinafter "OMB Request"]; EPIC Comments to OMB on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum 4 (Dec. 5, 2023) https://epic.org/wp-content/uploads/2023/12/EPIC-OMB-AI-Guidance-Comments-120523-1.pdf [hereinafter "EPIC OMB Comment"].

[214] OMB Request, *supra* note 213, at 17.

[215] *Id.*

- Instituting human training and assessment provisions to ensure agency employees have skills and resources to adequately oversee development, procurement, and use.[216]

Recommendation Nine: ***DOJ and DHS should strengthen accountability and oversight measures.***

DOJ and DHS must ensure robust compliance and oversight mechanisms are in place to adequately safeguard civil rights. Beyond EPIC's own investigations, several government agencies, including GAO and the DHS OIG have published reports over and over again stating that DHS and DOJ don't comply with their own existing privacy procedures, such as failing to update PIAs or test technology before fully deploying a tool.[217] In particular, filling out public PIAs in a thorough and timely manner is of the utmost importance to ensure proper transparency and accountability. The PIAs should focus on the disparate impact of these technologies on vulnerable populations and assess the vast amounts of personally identifiable information and biometric information in these systems. DHS and DOJ must also introduce robust oversight to deter misuse of these technologies, ensuring that the outputs remain information only rather than illusions of probable cause.[218] The creation of audit logs to monitor who uses the technology and routine supervision of those audit logs is paramount to understand how law enforcement uses these technologies and can help oversight bodies.[219] Finally, DOJ and DHS must strengthen accountability measures to ensure that meaningful oversight actually changes department policy and activity.

[216] *Id.* at 17–18.

[217] *See infra* note 241.

[218] *See Predict and Surveil*, *supra* note 153, at 63.

[219] *See* DHS Off. of the Inspector Gen., *CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data (REDACTED),* 13(Sep. 28, 2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf [hereinafter "DHS OIG Commercial Telemetry Report"] (In this report, DHS OIG found that DHS did not track the use of commercial telemetry data searches, leading to systemic misuse of the system as well as instances of officers using the commercial telemetry data to investigate personal matters. Even when a certain technology was able to track searches and individual use, DHS never requested audit logs despite multiple internal investigations of technology misuse. The OIG recommended the use of audit logs that are regularly reviewed by supervisors to "deter and detect" misuse of the technology.") .

Recommendation Ten: DOJ and DHS should emphasize transparency and public trust.

To advance DOJ and DHS' goal of strengthening public trust, the departments should disclose what technologies they are using, how they are using the technology, to what ends the technologies are useful, and the results of independent audits of the technology. PIAs fill some of this role, and DHS and DOJ must fill them out in a timely and thorough manner. Predictive policing technologies are new to the tech landscape and the heavy reliance on untested technology without disclosure erodes public trust, so focusing the department's efforts on public efficacy testing and routine audits is a major step in the right direction.

V. Social Media Surveillance

a. Social Media Surveillance is Overbroad and Should Not be Used.

i. How is social media surveillance carried out?

Law enforcement officials gather intelligence from social media in four primary ways: searching publicly available social media accounts and posts; creating an undercover account to monitor and/or interact with a targeted user; purchasing analytical software to track individuals, groups, and/or hashtags at a higher level; and obtaining a court order to get information about a specific user, including private messages.[220] Law enforcement engages in social media surveillance to gather intelligence for existing investigations, monitor social media for new and evolving threats, keep an ear to the ground by creating "situational awareness" of major events, to screen immigrants and individuals traveling in and out of the United States, among other reasons.[221]

[220] Rachel Levinson-Waldman, *Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media*, 71 Okla. L. Rev 997, 999–1000 (2019), https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1367&context=olr.

[221] Rachel Levinson-Waldman, Harsha Panduranga, & Faiza Patel, *Social Media Surveillance by the U.S. Governmen*t, Brennan Ctr. for Just. (Jan. 7, 2022) https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

The data gathered through social media are far and away more information than law enforcement could ever sift through, and the captured data neatly collates several sensitive categories of data that might otherwise be inaccessible to law enforcement through traditional means. A person's social media profile is more than just a picture and short biography; the profile itself can include demographic information, pictures of an individual's face, the individual's social network, the individual's interests, the individuals daily schedule, location, and more. Law enforcement typically gathers this information through commercial data sources such as Babel Street,[222] Geofeedia,[223] Digital Stakeout,[224] LifeRaft,[225] and SocialNet.[226] These companies gather information from social media accounts, among various other sources and some even come equipped with predictive technology to help assist law enforcement objectives.[227] While X (formerly Twitter), Facebook, and Instagram banned developers from using their Application Programming Interfaces for surveillance purposes, this ban did not extend to other techniques to scrape data.[228] This information is typically used to create dossiers to keep track of individuals and larger movements, particularly social movements and protests.[229] These dossiers are then integrated into law

[222] Babel Street, *About Us*, https://www.babelstreet.com/about-us (last visited Jan. 21, 2024).
[223] Ventura Cnty. Sheriff's Off., *What is Geofeedia?* (Feb. 11, 2015), https://www.aclunc.org/docs/20160921-pra_what_is_geofeedia.pdf.
[224] Digital Stakeout, *About Us*, https://www.digitalstakeout.com/about (last visited Jan. 21, 2024).
[225] Life Raft, *About LifeRaft*, https://www.liferaftinc.com/about (last visited Jan. 21, 2024).
[226] ShadowDragon, *SocialNet*, https://shadowdragon.io/socialnet/ (last visited Jan. 21, 2024).
[227] *See* Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat "Score*," Wash. Post (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.
[228] *See* Elizabeth Dwoskin, *Facebook Says Police Can't Use Its Data for "Surveillance*," Wash. Post (Mar. 13, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/13/facebook-says-police-cant-use-its-data-for-surveillance/; David Gilmour & Dell Cameron, *Twitter Cuts Off Third Surveillance Firm for Encouraging Police to Spy on Activists*, Daily Dot (Feb. 24, 2017), https://www.dailydot. com/layer8/media-sonar-twitter-social-media-monitoring/; April Glaser & Kurt Wagner, *Twitter Reminds Everyone It Won't Cooperate with Government or Police Surveillance*, Recode (Nov. 22, 2016), https://www.recode.net/2016/11/22/13719876/twitter-surveillance-policy-dataminr-fbi.
[229] *See supra* note 221.

enforcement's greater intelligence databases and fed into predictive policing tools, further compounding the data collected.[230]

The addition of the resulting data from social media surveillance to law enforcement's massive surveillance dragnet compounds the dangers to civil rights and civil liberties. DOJ and DHS do not monitor social media in isolation. This data is collected then collated into databases, which feed into several types of programs such as DHS' ATS.[231] DHS, for example, collects (among many, many other types of data) biometric data from immigrants; DMV data such as license plates and driver's license photos; data from utility companies;[232] and mobile phone location data.[233] Individually, this data is damaging and highly sensitive, but combined with the hoard of data the federal government keeps. it is a ticking time bomb. Government databases are regularly breached, such as in 2018 when the Postal Service exposed 60 million people to potential identity theft.[234] The Privacy Act of 1974 is supposed to protect this information, advocating for minimizing data collection to that which is "relevant and necessary," and reducing records related to First Amendment protected activity.[235]

This overbroad harvesting of data erodes the individual's ability to enjoy their privacy in public by creating a "virtual stakeout" of the entire world.[236] Privacy in public, and its related

[230] *See Predict and Surveil*, *supra* note 153, at 62.
[231] *See supra* notes 166–74 and accompanying text.
[232] *American Dragnet,* Geo. L. Ctr. on Priv. & Tech. 3 (May 18, 2022), https://americandragnet.org/sites/default/files/American_Dragnet_report_English_final.pdf.
[233] *See DHS OIG* Commercial *Telemetry Report, supra* note 219.
[234] *See, e.g.*, *USPS Site Exposed Data on 60 Million Users*, KrebsonSecurity (Nov. 21, 2018), https://krebsonsecurity.com/2018/11/usps-site-exposed-data-on-60-million-users/; Jim Sciutto, *OPM government data breach impacted 21.5 million*, CNN (Jul. 10, 2015), https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html.
[235] 5 U.S.C. § 552a.
[236] Jeramie Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. Bus. & Tech. L. 2, 153 (2017) https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1272&context=jbtl.

concept intellectual privacy, protects an individual's ability to generate ideas;[237] form beliefs;[238] and self-realize, supports freedom of thought, association rights, and prevents conformity of thought, thereby protecting the "free market of ideas that is vital for proper democratic discourse."[239] The advent of the internet, and social media in particular, have caused obscurity to fall by the wayside.[240] For example, there are several social media accounts dedicated to unmasking strangers in the background of social media content with facial recognition technology.[241] By analyzing and weaponizing this exorbitant amount of data, law enforcement is eroding public trust and actively chilling free speech.[242]

ii. Technical issues make social media surveillance impractical, if not impossible.

The sheer volume of content posted to user generated content websites makes manual review impractical to impossible. YouTube boasts that 500 hours of content is uploaded every minute to the platform, and that YouTube Shorts garners 70 billion views daily.[243] In April 2020, TikTok surpassed 2 billion downloads.[244] Even the companies who run the platforms have a hard time keeping up with content moderation despite employing thousands of content moderation staff.[245]

[237] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* 95 (2015).
[238] *Id.*
[239] *See Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, *supra* note 236, at 154.
[240] *Id.*
[241] *See, e.g.,* Joseph Cox, *The End of Privacy is a Taylor Swift Fan TikTok Account Armed with Facial Recognition Tech*, 404Media (Sep. 25, 2023), https://www.404media.co/the-end-of-privacy-is-a-taylor-swift-fan-tiktok-account-armed-with-facial-recognition-tech/.
[242] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, Pew Rsch. Ctr. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden.
[243] YouTube, *YouTube for Press*, https://blog.youtube/press/ (last visited Jan. 21, 2024).
[244] Ashley Carman, *TikTok reaches 2 billion downloads,* Verge (Apr. 29, 2020), https://www.theverge.com/2020/4/29/21241788/tiktok-app-download-numbers-update-2-billion-users.
[245] *See, e.g.,* Tom Simonite, *Facebook is Everywhere; Its Moderation is Nowhere Close*, Wired (Oct. 25, 2021), https://www.wired.com/story/facebooks-global-reach-exceeds-linguistic-grasp/; Meta, *Regulation (EU) 2022/2065 Digital Services Act: Transparency Report for Facebook,* 19 (Oct. 27, 2023), https://transparency.fb.com/sr/dsa-transparency-report-oct2023-facebook/ [hereinafter "Meta DSA Regulation Report (Facebook)"].

Social media also often contains low quality content that creates noise for algorithms trying to analyze data, which could make identifying text-based threats more difficult.[246] Examples of noisy content include incorrect grammar, misspelled words, slang, and text in multiple languages.[247] This is not only done unintentionally, but also on purpose to proactively avoid content moderation. One way users skirt content moderation algorithms is by changing language to avoid filters is by using euphemistic language like "unalive" in place of dying, suicide, and other death related topics, or deliberately misspelling words in captions (i.e. "seggs" instead of sex or "le$bian" instead of lesbian).[248]

Social media can often be adversarial to the point of hyperbole, causing problems in courts assessing whether a threat was genuine or whether it was a joke.[249] This confusion is exacerbated by machine learning algorithms, which have been repeatedly found to have trouble with context, such as jokes, sarcasm, and hyperbole due to the lack of annotated data sets and lack of formal evaluation methods to train the algorithms.[250]

iii. Dragnet social media surveillance is not a useful tool for investigation purposes and should be discontinued.

DHS, in particular, has spent the last several years implementing social media analysis into its screening of immigrants and individuals traveling in and out of the United States with a limited

[246] Swati Agarwal, *Applying Social Media Intelligence for Predicting and Identifying On-line Radicalization and Civil Unrest Oriented Threats*, arXiv, 2–3 (2015), https://arxiv.org/pdf/1511.06858.pdf

[247] Liang Zhao et al., *Unsupervised Spatial Event Detection in Targeted Domains with Applications to Civil Unrest Modeling,* 9 PLoS ONE 1 (Oct. 28, 2014), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0110206.

[248] Christianna Silva, *Content moderation is changing how we speak — and dictating who gets heard*, Mashable (Sep. 26, 2022), https://mashable.com/article/content-moderation-changing-language-fast; Jake Cline, *Internet Slang is More Sophisticated than it Seems*, Atlantic (Aug. 10, 2019), https://www.theatlantic.com/entertainment/archive/2019/08/how-internet-slang-makes-people-better-writers/595858/.

[249] *Missouri v. Metzin*ger, 456 S.W.3d 84, 101–02 (Mo. Ct. App. 2015).

[250] Thomas Winters, *Computers Learning Humor is No Joke*, MIT Press (Apr. 30, 2021), https://hdsr.mitpress.mit.edu/pub/wi9yky5c/release/3.

understanding of the analysis' efficacy. In 2016, DHS began a pilot program for screening visa applicants' social media for possible terrorist activity.[251] The DHS Office of the Inspector General found that this pilot program, "on which DHS plan[ned] to base future department-wide use of social media screening[,]" lacked criteria for measuring performance to ensure the program was meeting its objectives.[252] The OIG found that "absent [such] measurement criteria, the pilots may provide limited information" for expanding effective social media screening programs.[253] The pilot did not define what a successful outcome would be after screening an individual.[254] The tool could screen for the existence of a social media account linked to an individual, but USCIS found that automated screening was less effective than manual review.[255] USCIS did not define whether the existence of an account or lack of social media presence was a success, nor did USCIS define a certainty level for a successful screening.[256] In 2021, the Biden administration rejected a proposal to collect social media identifiers on travel and immigration forms because DHS did not "adequately [demonstrate] the practical utility of collecting" such information, noting that the executive order that ordered the screening proposal, the infamous Muslim Ban, had since been repealed.[257] In fact, the Biden administration went as far as calling for a review of whether collection of social media identifiers "meaningfully improved screening and vetting."[258] Biden administration intelligence officials have

[251] DHS Off. of Inspector Gen., *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted),* 1-2 (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.
[252] *Id.*
[253] *Id.*
[254] *Id.*
[255] *Id.* at 2–3.
[256] *Id.* at 3.
[257] Harsha Panduranga, *White House Office Rejects DHS Proposal to Collect Social Media Data on Travel and Immigration Forms*, Brennan Ctr. for Just. (Apr. 27, 2021), https://www.brennancenter.org/our-work/analysis-opinion/white-house-office-rejects-dhs-proposal-collect-social-media-data-travel.
[258] Exec. Order No. 10,141, 85 Fed. Reg. 7005 (Jan. 20, 2021), https://www.federalregister.gov/documents/2021/01/25/2021-01749/ending-discriminatory-bans-on-entry-to-the-united-states.

stated that social media identifiers "add no value" when collected in relation to the screening and vetting process, going as far as saying that it may not be collected going forward.[259]

Similarly, in 2021, the DHS Office of General Counsel released an internal review that echoed the 2016 OIG report's concerns about social media surveillance efficacy, noting that the DHS Intelligence and Analysis' use of social media surveillance to search for true threats of violence before they happen is a difficult task.[260] The review focused on I&A's monitoring of Portland, Oregon during the civil unrest and protests in the summer of 2020 following the murder of George Floyd. The former acting chief of DHS I&A likewise testified to Congress following the January 6th insurrection that "actual intent to carry out violence can be difficult to discern from the angry, hyperbolic — and constitutionally protected — speech and information commonly found on social media."[261] Beyond the failures of the surveillance goal itself, the internal review also highlighted undertrained, overworked teams that "crippled its workforce and engendered poor performance[,]" leading to the leakage of unclassified documents to two journalists in Portland, created a "poor understanding of the collection process," (which the review disapproves of for already being "so broad that the boundaries of the search are not well defined"), created confusion as to what "constituted a true threat" despite existing internal memos distinguishing between hyperbole and reportable threats, inability to identify sources, misunderstanding of when the duty to warn outside units comes into force, and many other failures.[262] These failures led to "mixed operational results,"

[259] Charlie Savage, *Visa Applicants' Social Media Data Doesn't Help Screen for Terrorism, Documents Show*, N.Y. Times (Oct. 5, 2023), https://www.nytimes.com/2023/10/05/us/social-media-screening-visa-terrorism.html.

[260] DHS, *Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest: Portland, Oregon, June through July 2020*, 16-20 (Jan 6. 2021), http://cdn.cnn.com/cnn/2021/images/10/01/internal.review.report.20210930.pdf.

[261] Melissa Smislova, Acting Under Secretary, DHS Office of Intel. & Analysis, Testimony to the Sen. Comm. on Homeland Sec. & Governmental Affs. on "Examining the January 6 Attack on the U.S. Capitol", https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Smislova-2021-03-03.pdf.

[262] *See supra* note 260.

which engendered complaints from law enforcement officials who found the threat warnings to be "crap" and full of noise.[263] I&A's deployment of officials to Portland was also "poorly planned" and "impaired from the outset," leading to intelligence gathering issues and threats to the safety of the officials as well as Portland residents due to the lack of military training and/or equipment.[264] The officials attempting to anticipate future threats as they popped up collected information on a "broad range of general threats that did not meet the threshold of intelligence collection" and provided "information of limited value," including "memes, hyperbole, statements on political organizations and other protected First Amendment speech."[265]

iv. Social media surveillance undermines First Amendment rights and chills free speech and assembly.

Not only does this data collection go far beyond the limits of privacy norms, it also produces a strong chilling effect against an individual's First Amendment speech and assembly rights. In the aftermath of the January 6th insurrection at the Capitol, DHS alleges that it has changed how it reacts to protected speech on social media, becoming more proactive.[266] I&A can only refer things they believe includes "true threats or incitements to violence" that aren't hyperbole, provides information that "enhances understanding on known threat actors[,]" or "includes information that demonstrates a risk of violence during a heightened threat environment."[267] However, peaceful protests, which are

[263] *Id.*

[264] *Id.*

[265] *Id.*; *see also* Rachel Levinson-Waldman et al., *Social Media Surveillance by the U.S. Government*, Brennan Ctr. for Just. (Jan 7. 2022), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

[266] Devlin Barrett, *Homeland Security official: Jan. 6 changed how we handle online intelligence*, Wash. Post (Nov. 3, 2021), https://www.washingtonpost.com/national-security/homeland-security-official-jan-6-changed-how-we-handle-online-intelligence/2021/11/03/108484f0-3cb7-11ec-bfad-8283439871ec_story.html; *Before, During, After, The Attack: The Jan. 6 siege of the U.S. Capitol was neither a spontaneous act nor an isolated event.*, Wash. Post (Oct. 31, 2021), https://www.washingtonpost.com/politics/interactive/2021/jan-6-insurrection-capitol/?itid=hp-top-table-main#key-findings&itid=lk_inline_manual_6&itid=lk_inline_manual_5.

[267] *Id.*

protected First Amendment activities, have been closely monitored by law enforcement, particularly those in support of racial minorities.[268] These harms are not abstract. Several guides on how to attend protests safely recommend face coverings, nondescript clothing, and something to cover any identifying marks such as tattoos to actively avoid surveillance, both when physically at the event and through pictures and videos posted on social media afterwards.[269] Some guides even go so far as to recommend turning off or setting phones to airplane mode to disable mobile data collection.[270]

Beyond protest monitoring, social media surveillance chills First Amendment expression, and courts are failing to push back against the invasive technology. The Brennan Center for Justice and the Knight First Amendment Institute filed a lawsuit in 2019 against collecting social media identifiers on visa forms due to the violation against the First Amendment rights.[271] The lawsuit alleges that the registration of social media accounts along with related retention and dissemination policies "deprive visa applicants of the rights to anonymous speech and private association," chill constitutionally protected speech and association, all while being poorly tailored to the government's stated interests.[272] The plaintiffs allege that visa applicants consider their social media presence and adjust their usage in preparation for surrendering social media identifiers to the U.S. government because they are worried that their speech, or others' speech imputed onto them, might subject them to additional scrutiny or delayed processing of their immigration application.[273] The U.S. District

[268] *See supra* note 260; Cam Wolf, *How the FBI is Using T-Shirts, Online Shopping Accounts, and Tattoos to Track Down Protesters,* GQ (June 23, 2020) https://www.gq.com/story/fbi-track-down-protester-etsy-t-shirt.
[269] *See, e.g.*, Nat. Res. Def. Council, *How to Protest Safely* (Oct. 26, 2022), https://www.nrdc.org/stories/how-protest-safely; Louryne Strampe & Lauren Goode, *How to Protest Safely: What to Bring, What to Do, and What to Avoid*, Wired (Jun. 24, 2022), https://www.wired.com/story/how-to-protest-safely-gear-tips/.
[270] N.Y.U. L. Ctr. on Race Inequality & L., *Protest Tips and Resources, NYU Law: The Center on Race Inequality & The Law,* https://www.law.nyu.edu/centers/race-inequality-law/protest-tips (last visited Jan. 21, 2024).
[271] Compl., *Doc Society et al. v. Blinken et al.*, No. 1:19-cv-03632 (D.D.C. Dec. 5, 2019); *Doc Society v. Blinken*, Brennan Ctr. for Just. (Nov. 30, 2023), https://www.brennancenter.org/our-work/court-cases/doc-society-v-blinken [hereinafter "*Doc Society* Case Page"].
[272] *Doc Society* Case Page, *supra* note 271.
[273] *Id.*

Court for the District of Columbia dismissed the suit based on significant deference to the executive branch on immigration enforcement and national security grounds, but noted that the challenged policies *do* run the risk of chilling constitutionally protected speech and association.[274] Plaintiffs filed for appeal in October 2023.

b. DOJ and DHS Must Adhere to Robust Safeguards to Mitigate Risks.

EPIC strongly recommends that DOJ and DHS shutter their social media surveillance programs and do not fund further projects. Social media surveillance is a clear example of a bloated, overbroad project that invades the privacy of most, if not all Americans. If these programs are to continue, DOJ and DHS must strip these programs to brass tacks and build them up with vigorous, proactive protections.

Recommendation One: DOJ and DHS should prohibit mass surveillance.

Situational awareness is a vague and subjective term, and broad social media surveillance often clogs up resources by providing officers useless or even misleading information.[275] DOJ and DHS should limit their use of social media surveillance to investigations where target individuals have already been identified through other means, and where the information in the social media content cannot be found by other, less invasive means. Furthermore, indiscriminate social media monitoring should constitute a search under the Fourth Amendment and a violation of First Amendment freedoms which would require law enforcement to seek a warrant or other court order and would provide individuals the ability to challenge authorities who improperly monitor them.

Recommendation Two: DOJ and DHS should protect civil rights and prohibit arrests and/or adverse immigration decisions based solely on social media surveillance.

DHS and DOJ should strengthen guidelines relating to intervention based on I&A threat warnings to ensure that law enforcement officials are not arresting people based on First Amendment

[274] *Id.*
[275] *See supra* note 263.

protected speech or assembly.[276] I&A members, and other law enforcement officials who employ social media surveillance, must be adequately trained when they are hired, and then periodically receive training thereafter to ensure the continued quality of monitoring and threat assessment.[277] Oversight mechanisms should periodically review the threats that have been flagged and sent beyond the monitoring teams to ensure that the threats being flagged match the appropriate standards for true threats. DOJ and DHS should also create clear guidelines as to when law enforcement should intervene based on the content of a flagged threat and train all law enforcement officials on those guidelines. Furthermore, DHS should prohibit the infliction of adverse immigration application decisions based solely on social media surveillance.

Recommendation Three: DOJ and DHS should protect criminal defendants' constitutional rights by requiring adequate notice of the use of social media surveillance technology and ensure that the technology is subject to adversarial interrogation during criminal litigation.

Criminal defendants are legally entitled to exculpatory evidence, and this must include any use of social media surveillance to gather information on the defendant. Substantively, the information provided to defendants should include the use of any technology to engage in social media monitoring, any accounts or content monitored pursuant to the investigation that were not directly linked back to the defendant, the exact content and/or accounts that were flagged that led to further police intervention, and audit logs from the law enforcement officials use of technology during the social media surveillance process. In addition, the defendant should be provided with the results of independent audits performed on the technology to assess the error rates and likelihood that the technology mischaracterized the social media content.

[276] *Id.*
[277] *Id.*

Recommendation Four: DOJ and DHs should ensure that technology is provably non-discriminatory prior to deployment.

When algorithms and other technologies are used to engage in social media surveillance, the technology must be provably non-discriminatory. DOJ and DHS must engage in thorough testing during the procurement phase and periodically after deployment to ensure there is no disparate impact on vulnerable communities. One factor particular to social media surveillance is language. The technologies need to be trained on languages other than English. In reports to EU regulatory bodies pursuant to the Digital Services Act (DSA), every single social media platform and search engine that submitted reports reported significantly higher error rates in content moderation technology when the language was not English.[278] America does not have an official language, and the targets of law enforcement investigations (particularly those focused on combatting terrorism) often speak languages other than English.[279] Social media surveillance teams should include individuals who speak and write in other languages to ensure that threats are being adequately evaluated. If a threat is flagged, it must be reviewed by a human individual who is fluent in the language before being escalated beyond the monitoring team.

Recommendation Five: DOJ and DHS must carry out an adequate evaluation of technology prior to deployment.

When employing algorithms or other technologies, the technology should have a clear goal, such as finding information about specific events rather than identifying examples of nebulous concepts like "radicalization" or "terrorism." The algorithms need to have objective, actionable end goals, such as matching an individual appropriately to their social media accounts or finding specific kinds of language that may indicate true threats or incitements of violence.

[278] *See, e.g.,* Twitter, *Digital Services Act: Transparency Report*, https://transparency.twitter.com/dsa-transparency-report.html [hereinafter "*Twitter DSA Transparency Report*"].

[279] *See supra* note 172.

Beyond the technology that enhances the monitoring, the monitoring teams themselves must have a clear understanding of what constitutes a true threat and where First Amendment protections apply. There must be a clear understanding of when escalation beyond monitoring is needed and when a threat is deemed non-actionable. DOJ and DHS should create clear guidelines and adequately train the monitoring teams when they are first hired as well as periodically thereafter to ensure the continued quality of threat assessments.

Recommendation Six: DOJ and DHS must adopt a strict data minimization framework.

Social media monitoring should only occur pursuant to specific investigations of individuals who are already targeted. Broad, untargeted social media surveillance should be considered a Fourth Amendment search and require a warrant or similar court order. Information collected pursuant to an investigation should be deleted once the investigation is closed. Data pulled from social media investigations should not be included into databases that are not directly linked to the investigation. DOJ and DHS should strengthen guidelines on data retention to ensure prompt deletion of sensitive data from the vast databases housed on federal government servers.

Recommendation Seven: DOJ and DHS should ensure data is adequately secure.

DOJ and DHS should focus on strong data minimization procedures to help ensure proper cybersecurity hygiene. In particular, the identification of individuals and confirmed social media accounts they own is highly sensitive data and can be used to doxx people.[280] This information must be stored for as little time as is necessary to complete an investigation, then promptly deleted to minimize the likelihood that such data would be exposed in a data breach.

[280] Sen Nguyen, *What is doxing and what can you do if you are doxed?*, CNN (Feb. 7, 2023) https://www.cnn.com/2023/02/07/world/what-is-doxxing-explainer-as-equals-intl-cmd/index.html; Andrew Quodling, *Doxxing, swatting and the new trends in online harassment*, Conversation (Apr. 21, 2015), https://theconversation.com/doxxing-swatting-and-the-new-trends-in-online-harassment-40234; Anemona Hartocollis, *After Writing an Anti-Israel Letter, Harvard Students Are Doxxed,* N.Y. Times (Oct. 18, 2023), https://www.nytimes.com/2023/10/18/us/harvard-students-israel-hamas-doxxing.html.

Recommendation Eight: DOJ and DHS should require independent auditing of technology.

When employing algorithms or other technology to monitor social media or enhance human review of social media, the technology should be evaluated during the procurement process and periodically after deployment to ensure accuracy. In addition to other general requirements all AI should be evaluated on,[281] social media surveillance technology must be trained appropriately on languages beyond just English. The algorithms should learn how to assess context, humor, satire, and hyperbole to be able to accurately assess true threats and distinguish them from benign, "lawful but awful" speech.[282] The algorithms must be provably non-discriminatory before deployment and further funding.

Recommendation Nine: DOJ and DHS should strengthen accountability and oversight measures.

Not only should the algorithms themselves be audited, but the law enforcement officials using the technology should also regularly be audited to ensure the technology is being used properly to attain the most accurate results and that the technology is being deployed in a non-biased manner. DHS and DOJ should require social media surveillance teams to retain audit logs of all inquiries made with the social media surveillance tools, and there should be regular supervision of these audit logs.[283] DHS and DOJ should strengthen accountability measures to ensure that oversight reports end in meaningful department policy change and actual reform.[284]

Recommendation Ten: DOJ and DHS should emphasize transparency and public trust.

DHS and DOJ must publish what social media surveillance tools they use, including contracts with commercial data brokers. PIAs are the traditional vehicle for this, and DOJ and DHS should ensure that PIAs are promptly and thoroughly filled out to ensure the public can understand

[281] *See supra* notes 212–16 and accompanying text.
[282] *See, e.g., Twitter DSA Transparency Report*, *supra* note 278.
[283] *See* DHS OIG Commercial Telemetry Report, *supra* note 219, at 13.
[284] *Id.* at 14*; see supra* note 219.

exactly how social media surveillance is being carried out, including what information the federal government is collating. DHS and DOJ should publish public guidelines on when information gathered from social media surveillance may be added to federal government databases, the retention schedule of that information, and any other information on the data infrastructure that affects the sensitive data collected from social media.

VI. DNA and Genetic Surveillance

a. Genetic Databases and DNA Information Raise Issues with Data Mining, Scope Creep, Disparate Impact, Reliability, Transparency, Accountability, and Public Trust.

i. Current DOJ Policy and Areas of Concern

There are multiple types of DNA databases with different submission, access, and analysis protocols for law enforcement agencies. Criminal databases, which can include information on exonerated defendants as well as non-convicted arrestees, include the Federal Bureau of Investigation's (FBI's) Combined DNA Index System (CODIS)[285]—to which the Department of Homeland Security (DHS) also submits samples taken from arrestees or immigrant detainees age 14 or older[286]—as well as state and local government databases.[287] Non-criminal databases from which

[285] One part of which is the National DNA Index System (NDIS). FBI, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/how-we-can-help-you/dna-fingerprint-act-of-2005-expungement-policy/codis-and-ndis-fact-sheet (last visited Jan. 19, 2024).

[286] DHS, Privacy Impact Assessment for CBP and ICE DNA Collection, No. DHS/ALL/PIA-080 (July 23, 2020, updated Oct. 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs080-detaineedna-october2020.pdf. Customs and Border Protection further claims it "has the discretion" to collect DNA samples from minors under the age of 14 "in potentially criminal situations." *See id.* at 15.

[287] Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. Ann. Surv. Am. L. 639, 673 (2014), https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2942&context=faculty_pub.

law enforcement agents may attempt to access information could include government health databases,[288] private health databases,[289] as well as direct-to-consumer DNA testing databases.[290]

Law enforcement agents may attempt to use these databases to identify exact or partial matches to individuals, or to investigate familial relationships, through methods such as familial DNA searching and forensic genetic genealogical DNA analysis and searching (FGG/FGGS). Significantly, FGG analyzes different DNA markers than search and analysis centered on individual matches,[291] and is less reliable than exact match DNA testing.[292] The U.S. Department of Justice has an interim policy for FGGS that applies to the Department's own components but has not issued any standards.[293]

[288] *DNA of every baby born in California is stored. Who has access to it?*, CBS News (May 12, 2018), https://www.cbsnews.com/news/california-biobank-dna-babies-who-has-access/.

[289] Joseph Goldstein, *Hospital and Drugmaker Move to Build Vast Database of New Yorkers' DNA*, N.Y. Times (Aug. 12, 2022), https://www.nytimes.com/2022/08/12/nyregion/database-new-yorkers-dna.html.

[290] Jordan Smith, *Police Are Getting DNA Data From People Who Think They Opted Out*, Intercept (Aug. 18, 2023), https://theintercept.com/2023/08/18/gedmatch-dna-police-forensic-genetic-genealogy/.

[291] Nat'l Inst. of Just., *In-Brief: An Introduction to Forensic Genetic Genealogy Technology for Forensic Science Service Providers* 3 (Sept. 2022), https://forensiccoe.org/private/6320f16805925; DOJ, Interim Policy Forensic Genetic Genealogical DNA Analysis and Searching 2–3 (Sept. 2, 2019), https://www.justice.gov/olp/page/file/1204386/download [hereinafter DOJ Interim Policy]; Claire L. Glynn, *Bridging Disciplines to Form a New One: The Emergence of Forensic Genetic Genealogy*, 13 Genes 1381, at PDF p. 1–3 (2022), https://doi.org/10.3390/genes13081381.

[292] *See, e.g.*, Joseph Zabel, *The Killer Inside Us: Law, Ethics, and the Forensic Use of Family Genetics*, 24 Berkeley J. Crim. L. 47, 71 (2019); Kerry Abrams & Brandon L. Garrett, *DNA and Distrust*, 91 Notre Dame L. Rev. 757, 782 (2015).

[293] DOJ's interim policy on FGG includes regulations and requirements such as a prohibition on arresting individuals based solely on genetic association, a requirement that exact match DNA typing be subsequently performed, the limitation that FGG only be conducted to solve violent crimes or attempts to commit violent crimes or where there is "a substantial and ongoing threat to public safety or national security," as well as requirements for prompt destruction of reference samples, derivative profiles, and other account information. *See* DOJ Interim Policy, *supra* note 291 at 4–5. *But see* Christi J. Guerrini et. al., *Four Misconceptions About Investigative Genetic Genealogy*, 8 J.L. & Biosciences 1, 15 (2021); Alexandra Zaretsky, *DNA Collection in Immigration Custody and the Threat of Genetic Surveillance*, 109 Cal. L. Rev. 317, 323 (2021). The National Institute of Justice published a brief on FGG for Forensic Science Service Providers (FSSPs), which places the burden of compliance with this interim policy on FSSPs and their multidisciplinary teams rather than on FGG vendors. *See* Nat'l Inst. of Just., *In-Brief: An Introduction to Forensic Genetic Genealogy Technology for Forensic Science Service Providers* (Sept. 2022), https://nij.ojp.gov/library/publications/introduction-forensic-genetic-genealogy-technology-forensic-science-service.

While there have been DOJ audits of specific crime labs since 2001[294] (although none published within the last five and a half years),[295] and Quality Assurance Standards (QAS) published as recently as 2020,[296] the FBI has not published a similarly comprehensive audit report since 2001 (although there was a follow-up report in 2006).[297] These audits are important as they measure compliance with the QAS; QAS includes mandatory developmental validation prior to use of a novel methodology,[298] qualified auditing,[299] and record retention regarding proficiency tests.[300]

DHS's role in DNA analysis is more circumscribed than DOJ's. In terms of DHS policy, its 2020 Privacy Impact Assessment (PIA) notes that it is unlikely "that CBP or ICE would be able to use a DNA profile match for public safety or investigative purposes prior to either an individual's removal to his or her home country, release into the interior of the United States, or transfer to another federal agency."[301]

DNA has earned a reputation for unparalleled reliability, but it is important to avoid equivocation, especially in the interest of building public trust through transparency—not all forms of DNA analysis are identically reliable. In terms of reliability, exact matching of a single sample collected in a controlled setting is the gold standard of DNA analysis. But this is not always possible,

[294] Compliant labs are required to submit external audits to the FBI at least once every two years. *See* FBI, National DNA Index System (NDIS) Operational Procedures Manual (Version 4) 9 (May 1, 2016), https://ucr.fbi.gov/lab/biometric-analysis/codis/ndis-procedures-manual [hereinafter NDIS Operational Procedures Manual].
[295] DOJ Off. of Inspector Gen., *Combined DNA Index System Audits*, https://oig.justice.gov/reports/codis-ext.htm (last visited Jan. 21, 2024).
[296] FBI, *Biometrics and Fingerprints*, https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis-2 (last visited Jan. 21, 2024).
[297] DOJ Off. of Inspector Gen., *Combined DNA Index System Operational and Laboratory Vulnerabilities, Audit Report 06-32* (May 2006), https://oig.justice.gov/reports/FBI/a0632/exec.htm.
[298] FBI, Quality Assurance Standards for Forensic DNA Testing Laboratories 17 (September 1, 2011), https://ucr.fbi.gov/lab/biometric-analysis/codis/quality-assurance-standards-for-forensic-dna-testing-laboratories (Standard 8.2).
[299] *Id.* at 26 (Standard 15.1).
[300] *Id.* at 9 (Standard 3.2); *see also* Nat'l Acads. of Scis., Eng'g, & Med, *The Evaluation of Forensic DNA Evidence* 4 (1996), https://doi.org/10.17226/5141 ("Recommendation 3.2. Laboratories should participate regularly in proficiency tests, and the results should be available for court proceedings.").
[301] PIA, No. DHS/ALL/PIA-080, *supra* note 286, at 4.

especially at the investigation stage. It is common sense that using methods that increase sensitivity to detecting a positive result will necessarily also increase the likelihood of finding a match where there is none (a false positive).[302] Samples that may contain multiple sources of DNA or may be degraded (e.g. by environmental factors) are less reliable, as is a moderate stringency search ("partial match").[303] Similarly, RapidDNA analysis may expedite an law enforcement agency's investigation but should not be considered as reliable as analysis conducted by an actual lab technician in a controlled environment.[304] Familial searches can produce multiple hits without any true matches,[305] which has implications not only for accuracy and reliability but also for disparate impact and privacy, civil rights, and civil liberties.

In processing any DNA sample, the privacy interests of the person included in the DNA database are relevant (whether that is a suspect, a victim, or an unknown person at a crime scene).[306] Beyond mere identification, some methods of DNA analysis may expose a person's HIV status or gender identity (this is especially relevant in the context of an incarcerated person).[307] In the case of

[302] Rich Press, *DNA Mixtures: A Forensic Science Explainer*, NIST (Apr. 3, 2019), https://www.nist.gov/feature-stories/dna-mixtures-forensic-science-explainer ("When using high-sensitivity methods, however, forensic scientists are more likely to detect and get profiles from irrelevant DNA. That means that the risk of incorrectly associating a person with a crime has gone up in recent years.").

[303] *Frequently Asked Questions on CODIS and NDIS*, *supra* note 285, at 31 ("How successful are partial matches at locating potential suspects?").

[304] Joseph Goldstein, *Guilty Until Proven Innocent: The Failure of DNA Evidence*, 12 Drexel L. Rev. 597, 622 (2020); Zaretsky, *supra* note 293, at 346. Rapid DNA testing in particular has been shown to be error-prone. *See, e.g.*, Swed. Nat'l Forensic Ctr., *Experiences from operating the RapidHIT System* 3 (2017), https://nfc.polisen.se/siteassets/dokument/informationsmaterial/rapporter/nfc-rapport-2017-02_experiences-from-operating-the-rapidhit-system.pdf.

[305] Lucy Grogan, *Ethical Implications of CODIS* 38 (Aug. 2019) (M.A. thesis, Grand Valley State Univ.), https://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1940&context=theses).

[306] Claire Abrahamson, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 Fordham L. Rev. 2539, 2563 (2019), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5611&context=flr.

[307] Christine Guest, *DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights*, 68 Am. U.L. Rev. 1015, 1041 (2019) (citing to *Powell v. Schriver,*175 F.3d 107 (2d Cir. 1999)).

familial searches using CODIS[308] and especially FGG, however, the privacy interests of individual family members as well as separately of the family unit as a whole are also implicated.[309] This is especially significant where purported consent is concerned, as an individual may be wholly unaware that a relative's genetic data has been subject to FGG. The National Institute of Justice, in its module about the prohibition on DNA Dragnets, glibly notes that "there is no constitutional prohibition on requesting DNA samples from large numbers of people who are not detained or arrested, provided the consent is obtained voluntarily."[310] This is exacerbated by the lack of an effective mechanism by which an individual may revoke consent to indefinite storage of their genetic information, see Section VI(a)(ii)(3) *infra*, and by consent obtained through law enforcement agency deception.[311]

We offer recommendations for addressing these concerns in Section VI(b) *infra*.

[308] Abrahamson, *supra* note 306, at 2563 (citing to Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 Harv. J.L. & Tech. 309, 328 (2010)).

[309] Abrahamson, *supra* note 306, at 2563; Grogan, *supra* note 305, at 42 ("The fear associated with 'genetic surveillance' is that persons will be viewed as guilty by association, through simply being related to an individual who committed a crime, and this view will allow for a family's privacy to be violated continually through 'lifelong genetic surveillance.'").

[310] Nat'l Inst. of Just., *Principles of Forensic DNA for Officers of the Court: Digital Dragnets* (June 20, 2023), https://nij.ojp.gov/nij-hosted-online-training-courses/principles-forensic-dna-officers-court/10-collection-dna-evidence-suspects-and-arrestees/key-legal-issues-surrounding-collection-dna-evidence/dna-dragnets.

[311] Jon Schuppe, *'They lied to us': Mom says police deceived her to get her DNA and charge her son with murder*, NBC News (Feb. 22, 2020), https://www.nbcnews.com/news/us-news/they-lied-us-mom-says-police-deceived-her-get-her-n1140696. The Orange County DNA database represents coercive law enforcement collection of DNA in exchange for dropping minor charges. *See* Andrea Roth, *"Spit and Acquit": Prosecutors as Surveillance Entrepreneurs*, 107 Cal. L. Rev. 405, 408, 418–19 (2019), https://static1.squarespace.com/static/640d6616cc8bbb354ff6ba65/t/64507bad1cc7885293f37c0e/1682996142222/2+-+Roth.pdf.

ii. Data mining.

Permitted triggers for DNA collection and entry into a government database are overinclusive. Newborns,[312] immigrants,[313] victims,[314] juvenile offenders,[315] non-convicted (even exonerated) arrestees,[316] DNA taken from questioned suspects who were never arrested,[317] and DNA from non-violent crimes[318] are just a few examples of populations and situations in which it may be inappropriate to add DNA to a database.[319] Procedurally, "spit and acquit" programs coupled with retaining samples indefinitely, as well as ineffective expungement programs, are also problematic, if only because they prioritize growth of the government's DNA databases over an individual's

[312] Natalie Ram, *America's Hidden National DNA Database*, 100 Tex. L. Rev. 1253, 1256 (2022) (citing to Julie Watts, *CBS13 Investigates: CA Still Storing Newborn DNA Without Consent. Golden State Killer Case Raising New Concerns*, CBS Sacramento (Dec. 7, 2020), https://sacramento.cbslocal.com/2020/12/07/newborn-dna-california-consent-gsk-killer/).
[313] Zaretsky, *supra* note 293, at 329.
[314] Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. Rev. 1491, 1550 (2015).
[315] Kevin Lapp, *As Though They Were Not Children: DNA Collection from Juveniles*, 89 Tul. L. Rev. 435, 474 (2014).
[316] Jordan Mason, *No Longer Innocent Until Proven Guilty: How Ohio Violates the Fourth Amendment Through Familial DNA Searches of Felony Arrestees*, 69 Clev. St. L. Rev. 185, 188 (2020).
[317] Elaine Ortyl, *DNA and the Fourth Amendment: Would A Defendant Succeed on A Challenge to A Familial DNA Search?*, 45 Am. J.L. & Med. 421, 427 (2019) (citing to Jan Ransom & Ashley Southall, *N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database.*, N.Y. Times (Aug. 15, 2019), https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html) ("Around 30,000 of the profiles [in the NYPD's database] come from DNA left behind by individuals on water cups and other objects while being questioned at a police station."). The author further noted that: "New York is not alone in this operation — the article authors note that California, Connecticut, and Maryland also have similar genetic databases." *Id.* at 442 n. 70 (citing to same the N.Y. Times article).
[318] Gabrielle A. Sulpizio, *Your Body, Your DNA: Addressing the Constitutionality of Databanked DNA Under the Fourth Amendment*, 10 Charleston L. Rev. 417, 438 (2016).
[319] In some instances, it may be inappropriate to even collect DNA, discussed *infra*.

rights,[320] not to mention the predictable disparate impact they have. These databases also represent attractive targets to cyber criminals.

1. Building DNA databases.

There are obvious issues with retaining an individual's DNA in a database prior to that individual's conviction, as there has not yet been a determination of that individual's guilt or innocence. Conducting a DNA swab test of an arrestee is permitted without a warrant under *Maryland v. King* in the context of violent crimes.[321] However, the documented shortcomings in expungement of that genetic information from a government database[322] seem to counsel against incorporation of that sample into a database prior to conviction, especially if no charges are ever brought or if the defendant is exonerated. This has implications for public trust as well, particularly in the context of non-violent crimes.[323] We discuss additional concerns for specific populations such as newborns, juveniles, non-citizens, and victims *infra*. Additionally, "spit and acquit" programs coerce individuals into turning their genetic data over to law enforcement,[324] which exacerbates

[320] Wayne A. Logan, *Government Retention and Use of Unlawfully Secured DNA Evidence*, 48 Tex. Tech. L. Rev. 269, 275–76 (2015) **(**quoting a California Supreme Court Justice in saying "If [the police] may use the direct fruits of illegal arrests in the prosecution of the individual for another offense, they will have a decided incentive to arrest anyone whom they 'suspect' may be involved in illegal activity, regardless of whether that suspicion is legally sufficient for an arrest"**)**; Kelly Ferrell, *Twenty-First Century Surveillance: DNA "Data-Mining" and the Erosion of the Fourth Amendment*, 51 Hous. L. Rev. 229, 242 (2013) (arguing "the only conceivable governmental interest served by sampling preconviction arrestees is to vastly expand the federal database as part of a DNA data-mining strategy") (quoting Brief of Amici Curiae ACLU et al. Supporting Respondent at 5–6, *Maryland v. King*, 133 S. Ct. 1958 (2013) (No. 12-207)).

[321] *Maryland v. King*, 569 U.S. 435, 439 (2013).

[322] Discussed in Sec. VI(a)(ii)(3) *infra*.

[323] *See* Sulpizio, *supra* note 318, at 438. Some states limit searches of their database to violent crimes, but others allow automatic access. *See* Jennie F. O'Hara, *23, Me, and the Police: The Fourth Amendment Implications of Familial DNA Searching*, 30 Geo. Mason U. Civ. Rights L.J. 177, 186–87 (2020) (citing to Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 Wake Forest L. Rev. 767, 779 (1999)).

[324] Ortyl, *supra* note 317, at 427 (citing to Lauren Kirchner, *DNA Dragnet: In Some Cities, Police Go From Stop-and-Frisk to Stop-and-Spit,* ProPublica (Sept. 12, 2016), https://www.propublica.org/article/dna-dragnet-in-some-cities-police-go-from-stop-and-frisk-to-stop-and-spit. This is especially true when applied to traffic stops or being stopped on the street, as is currently the case in Florida. *See id.*; *see generally* Roth, *supra* note 311.

existing disparities regarding marginalized groups that may have disproportionately greater contact with the criminal justice system and may have disproportionately fewer resources to effectively challenge weak cases or improper procedure and therefore be more susceptible to coercive tactics,[325] discussed further in Section VI(a)(iv) *infra*. Additionally, the federal requirement for a process to request expungement—which has its own problems described in Section VI(a)(ii)(3) *infra*—only applies to DNA profiles; the Violent Crime Control and Law Enforcement Act does not explain how to expunge DNA samples, which means it's possible that *samples* could be stored indefinitely even if (to assume a counterfactual) *profiles* are appropriately expunged every time.[326] Under the exclusionary rule doctrine, police may retain and use for investigative purposes photos and fingerprints secured through unlawful arrest.[327] DNA collection could become part of the routine booking procedure, making it collectable from anyone arrested rightly or wrongly.[328] Some jurisdictions are already building DNA databases this way.[329]

2. *DNA is collected earlier than necessary.*

Although it seems manifestly clear that DNA should not be added to a law enforcement database prior to conviction,[330] we also argue that initial collection of that DNA should occur later in

[325] *See, e.g.*, Ram Subramanian et al., *In the Shadows: A Review of the Research on Plea Bargaining* 15 (September 2020), https://www.vera.org/downloads/publications/in-the-shadows-plea-bargaining.pdf; Somil Trivedi & Jared Keenan, *Coerced Out of Justice: How Prosecutors Abuse Their Power to Secure Guilty Pleas*, ACLU (July 8, 2021), https://www.aclu.org/news/criminal-law-reform/coerced-out-of-justice-how-prosecutors-abuse-their-power-to-secure-guilty-pleas.

[326] *See* Christen Giannaros, *Unprecedented Infringement: Debunking the Constitutionality of DNA Collection from Mere Arrestees in Light of* Maryland v. King, 28 J. Civ. Rts. & Econ. Dev. 455, 460 (2016). Moreover, even where a state requires that the sample be destroyed, if that state does not allow for the sample to be tested until the first scheduled arraignment, its collection and expungement each represent needless administrative costs. *See* Goldstein, *supra* note 304, at 608.

[327] Logan, *supra* note 320, at 271.

[328] *Id.*

[329] *See* Lauren Kirchner, *DNA Dragnet: In Some Cities, Police Go From Stop-and-Frisk to Stop-and-Spit*, ProPublica (Sept. 12, 2016), https://www.propublica.org/article/dna-dragnet-in-some-cities-police-go-from-stop-and-frisk-to-stop-and-spit.

[330] The plain text of the statute at issue in *Maryland v. King* did not even permit testing until arraignment, did not permit tests for familial matches, and mandated destruction in the absence of a conviction.

the process. DNA evidence cannot itself indicate guilt or innocence but rather merely suggests presence or proximity. Indeed, in one study in which individuals shook hands for two minutes and later handled knives, DNA testing of 20% of the knives indicated not the DNA of the person who actually handled the knife but rather that the DNA of the person with whom they shook hands was the primary or sole DNA contributor.[331] At present, DNA is effectively immutable so there are also no concerns about identification of the individual being compromised if DNA is collected later in the process.[332] Law enforcement could still seek a warrant based on probable cause to collect DNA earlier in the process;[333] however, the risks are too great for pre-conviction collection to be standard procedure in terms of misuse of sensitive data, of indefinite retention of that data, and of the possibility of an erroneous conviction due to overreliance on DNA.[334]

3. The myth of expungement.

Experts have described the prospect of expungement from a DNA database as a myth,[335] despite federal law requiring all states that participate in CODIS to establish clear procedures for expungement.[336] One 2015 estimate was that a mere handful out of thousands of arrestee DNA profiles had ever been expunged.[337] Similar to the high probability for disparate impact in the collection phase of government DNA data mining, there is also a high probability for disparate

[331] Mary Graw Leary, *Touch DNA and Chemical Analysis of Skin Trace Evidence: Protecting Privacy While Advancing Investigations*, 26 Wm. & Mary Bill Rts. J. 251, 273 (2017). We discuss these issues further in Sec. VI(a)(v)(2) *infra*.
[332] Ferrell, *supra* note 320, at 240–41.
[333] Giannaros, *supra* note 326, at 476.
[334] Ferrell, *supra* note 320, at 242.
[335] *See generally* Elizabeth E. Joh, *The Myth of Arrestee DNA Expungement*, 164 U. Pa. L. Rev. Online 51 (2015).
[336] *See, e.g.*, NDIS Operational Procedures Manual, *supra* note 294, at 13; Zaretsky, *supra* note 293, at 350; *see also* 34 U.S.C. §§ 12592(d)(1)(A)(ii), 12592(d)(2)(A)(ii). Indeed one 2013 Urban Institute study of 28 states that collect arrestee DNA found that by the terms of their collection statutes, 27 permit those eligible to have their genetic information expunged. Joh, *supra* note 335, at 51 (citing to Julie E. Samuels et al., Urban Inst., *Collecting DNA at Arrest: Policies, Practices, and Implications* app. C (May 2013), http://www.urban.org/research/publication/collecting-dna-arrest-policies-practices-and-implications.
[337] Joh, *supra* note 335, at 52.

impact in the expungement phase. In the majority of states, "the process of expungement is burdensome, costly, and must be initiated by the arrestee."[338]

A 2012 National Institute of Justice survey found that very few expungements actually occur where expungement is not automatic and this can result in biometric data of individuals who were never formally charged or who were acquitted remaining in genetic databases.[339] Some states do not track legal outcomes of cases, which can result in DNA remaining in CODIS post-acquittal.[340] Even states like Maryland that have automatic expungement may have loopholes that prioritize the database over individual rights: samples provided voluntarily are not subject to automatic expungement, nor apparently any avenue for expungement.[341]

Moreover, as of 2015, only five states prohibited the use of DNA that should have been expunged but was not.[342] The failure to properly effectuate expungement means that mere arrests (or even just being born)[343] can result in the permanent relinquishment of a person's genetic information to law enforcement,[344] prioritizing maximization of data in government databases over legal rights.

[338] Zaretsky, *supra* note 293, at 350 (citing to Joh, *supra* note 335, at 51). Only thirteen states automatically destroy the DNA sample and profile if the suspect is acquitted. *See id.* (citing to Nat'l Conf. of State Legislatures, *DNA Arrestee Laws* (2018), http://www.ncsl.org/Documents/cj/Arrestee_DNA_Laws.pdf). Only seven states provide automatic, state-initiated expungement. *See* Joh, *supra* note 335, at 54 (citing to Samuels et al., *supra* note 336 at 27-28; *see also* Goldstein, *supra* note 304, at 601–02.

[339] Mason, *supra* note 316, at 216 (quoting Samuels et al., *supra* note 336 at 23). In one prominent case, someone whose DNA was not a match to the killer requested expungement of their data; as of 2014 it was still unclear whether his DNA profile remained in a state or local database. Mercer & Gabel, *supra* note 287 at 673.

[340] Mason, *supra* note 316, at 188; *Frequently Asked Questions on CODIS and NDIS*, *supra* note 285, at 24. ("What are the expungement requirements?").

[341] *See, e.g.*, Goldstein, *supra* note 304, at 601–02.

[342] *See* Alexandra Nieto, *Familial Searching: How Implementing Minimum Safeguards Ensures Constitutionally-Permissible Use of This Powerful Investigative Tool*, 40 Cardozo L. Rev. 1765, 1800 (2019) (citing to Logan, *supra* note 320, at 281–82).

[343] *See* Ram, *supra* note 312, at 1256.

[344] Joh, *supra* note 335, at 51.

4. *Cybersecurity implications.*

Indefinite storage of genetic information in digital databases has important cybersecurity implications as well. It is sought after by cyber criminals in commercial contexts,[345] as well as in government[346] contexts. Even federal agencies are not perfectly cyber secure,[347] and government agencies at the local level are more likely to have even fewer resources to safeguard their digital databases.[348] Data minimization is an important principle in both privacy and cybersecurity which counsels that bad actors can't breach data that was properly and timely disposed of or was never collected.[349] Data minimization applies to limitations on how data is used and with whom it is shared as well, not just to collection and retention policies.

[345] Justin Sherman, *The Danger in Genetic-Data Breaches: You Can't Change Your DNA*, Barron's (Dec. 13, 2023), https://www.barrons.com/articles/genetic-data-23andme-breach-regulation-privacy-15af683d; Smith, *supra* note 290.

[346] A breach of the Office of Personnel Management discovered in 2014 included security clearance and fingerprint information. Off. of the Dir. of Nat'l Intel., Cyber Aware Case Study: OPM, https://www.dni.gov/ncsc/e-Learning_CyberAware/pdf/Cyber_Aware_CaseStudy_OPM.pdf (last visited Jan. 19, 2024); *see also* Aliya Sternstein, *DHS insider hacking case reveals serious network security vulnerabilities*, NextGov/FCW (Sept. 12, 2011), https://www.nextgov.com/digital-government/2011/09/dhs-insider-hacking-case-reveals-serious-network-security-vulnerabilities/49757/ (skilled staffers knowingly creating vulnerabilities in a database containing data sought by identity thieves). Internationally, the breach of a government biometric database can make and has made millions of individuals subject to fraud and identity theft. *See* Saira Hussain et al., *EFF Files Comment Opposing the Department of Homeland Security's Massive Expansion of Biometric Surveillance*, EFF (Oct. 22, 2020), https://www.eff.org/deeplinks/2020/10/eff-files-comment-opposing-department-homeland-securitys-massive-expansion (citing Vidhi Doshi, *A security breach in India has left a billion people at risk of identity theft*, Wash. Post (Jan. 4, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/).

[347] *See, e g.*, Off. of the Dir. of Nat'l Intel., *supra* note 346; *see also* John Hewitt Jones, *FBI confirms Law Enforcement Enterprise Portal compromise in cyberattack*, FedScoop (Nov. 15, 2021), https://fedscoop.com/fbi-confirms-law-enforcement-enterprise-portal-compromise-in-cyberattack/.

[348] Colin Wood, *Local governments don't have enough cyber funding, survey finds*, StateScoop (Nov. 15, 2023), https://statescoop.com/pti-cybersecurity-survey-local-government/. Law enforcement emails in particular have been targeted and compromised. *See, e.g.*, *Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"*, KrebsonSecurity (Mar. 29, 2022), https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/; Adrienne N. Kitchen, *Genetic Privacy and Latent Crime Scene DNA of Nonsuspects: How the Law can Protect an Individual's Right to Genetic Privacy While Respecting the Government's Important Interest in Combatting Crime*, 52 No. 2 Crim. L. Bulletin Art 5 at PDF p. 6.

[349] John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, EPIC (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.

iii. Mission creep.

Historically, law enforcement agencies have ignored limitations placed on their use of an available technology, for example directing surveillance on First Amendment-protected activities when authorization to use those technologies was limited to the most heinous crimes.[350] Statements that equate DNA to fingerprinting by virtue of it being solely used for identification purposes are misleading and further erode public trust when those promises are broken. This kind of scope creep is not only problematic from a compliance standpoint, but also demonstrably chills free speech as well as reduces the likelihood that individuals will report crimes or engage in commercial activities for fear of undisclosed law enforcement surveillance or unexpected criminal justice repercussions.

1. Used for all kinds of "crimes".

Once the infrastructure is in place for law enforcement agencies to use a technology to solve any type of crime, it becomes too easy for them to exceed the scope of authorization for that technology and begin using it for other types of crimes and for other purposes entirely.[351] For example, using newborn screenings (required for the child's health) for criminal investigative purposes;[352] similarly, screening pregnant patients for drugs and sharing the results with law

[350] *See, e.g.*, Powers *supra* note 91; EPIC, *4th Circuit Rules That Baltimore Warrantless Aerial Surveillance Program Violates Fourth Amendment* (June 24, 2021), https://epic.org/4th-circuit-rules-that-baltimore-warrantless-aerial-surveillance-program-violates-fourth-amendment/; Kreag, *supra* note 314, at 1530–31; Robert Williams, *I Did Nothing Wrong. I Was Arrested Anyway.*, ACLU (July 15, 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway. There are also concerns with LOVEINT-related risks wherein law enforcement agents abuse their access for personal stalking purposes. *See, e.g.*, Comments of EPIC, et al., *In re* Supporting Survivors of Domestic and Sexual Violence (NPRM), WC Docket No. 22-238; WC Docket No. 11-42; WC Docket No. 21-450 at App'x 2 (Apr. 12, 2023), https://epic.org/documents/in-the-matter-of-supporting-survivors-of-domestic-and-sexual-violence-nprm/; Alina Selyukh, *NSA staff used spy tools on spouses, ex-lovers: watchdog*, Reuters (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-toolson-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927.

[351] Abrahamson, *supra* note 306, at 2547 (noting a vast expansion of qualifying crimes for inclusion in CODIS).

[352] Ram, *supra* note 312, at 1256.

enforcement agencies in order to coerce those women to enter drug treatment.[353] In at least one instance, the facts have strongly suggested that a miscarriage was treated as a fetal death and prosecuted using DNA testing.[354]

These problems are exacerbated by FGGS and by direct-to-consumer (DTC) databases. Law enforcement agencies could use FGGS to generate investigative leads, to investigate lower level crimes, and even to identify protestors or abortion seekers.[355] DTC genetic databases contain profiles on millions of individuals unaffiliated with any law enforcement connection, and in some instances affirmatively offer that data to law enforcement agencies to assist in solving crimes such as robbery.[356] Notably, public support for use of private genetic information, like public support for access to cell phone records and social media accounts, diminishes greatly when the purpose is to identify perpetrators of non-violent crimes.[357]

In the DHS context, there is reason to believe the government's interest is in "searching for evidence that [noncitizens have] committed crimes unrelated to the crime of ... arrest", to see if detainees' DNA profiles match data in CODIS.[358] This allows for government searches without probable cause. The collected samples may also be used to support law enforcement investigations by other agencies, and to generate further investigative leads.[359]

[353] We do not dispute the value of making pregnant mothers aware of their options and the risks of each option, but this should be done by a medical professional they trust, not by an officer of the law. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67 (2001).
[354] Zabel, *supra* note 292, at 95–96.
[355] Jennifer Lynch, *Forensic Genetic Genealogy Searches: What Defense Attorneys & Policy Makers Need to Know*, EFF (July 26, 2023), https://www.eff.org/wp/forensic-genetic-genealogy-searches-what-defense-attorneys-need-know.
[356] Zabel, *supra* note 292, at 96.
[357] Abrahamson, *supra* note 306, at 2584–85; Clive Thompson, *The Myth of Fingerprints*, Sci. Mag. (Apr. 2019), https://www.smithsonianmag.com/science-nature/myth-fingerprints-180971640/ ("Normally, you might think of DNA as the province solely of high-profile crimes—like murder investigations, where a single hair or drop of blood cracks a devilish case. Nope: These days, even local cops are wielding it to solve ho-hum burglaries.").
[358] Zaretsky, *supra* note 293, at 341.
[359] *Id.*

2. *Not merely for identification purposes; not the same as fingerprints.*

The Supreme Court has determined that because DNA testing is primarily used for identification purposes, it is equivalent to fingerprinting.[360] This is flawed because DNA can be and often is used for other purposes, because DNA contains vast amounts of private information,[361] and because until relatively recently it was not even practical to use DNA for identification purposes due to the long lag time between collection and receiving results back from the lab[362] (more recent, more rapid methods are not without reliability tradeoffs).[363]

Fingerprints, unlike DNA, cannot determine a person's race or ancestry. Although the data in CODIS does not itself provide this information, the data in CODIS when coupled with the genetic data in commercial databases can reveal this information.[364] Similarly, CODIS data when combined with information from commercial DNA databases can unearth genetic predispositions for certain diseases.[365] Just as law enforcement agencies seek to use FGG to explore possible branches of a family tree, absent enforced prohibitions to the contrary, we should expect these agencies to leverage

[360] *Maryland v. King*, 567 U.S. 1301 (2012).

[361] Kitchen, *supra* note 348, at PDF p. 10 ("Jurisprudence upholding DNA databases is flawed for two main reasons. First, courts treat DNA as they treat fingerprints, but this premise is flawed because fingerprints and DNA vastly differ—DNA has nearly unlimited uses beyond identification, including genetic profiling, while fingerprints can be used solely to identify individuals. Second, courts treat DNA as abandoned property and ignore privacy interests regarding the vast amounts of private information contained within DNA."); Zaretsky, *supra* note 293, at 340.

[362] *Maryland v. King*, 567 U.S. at 476 (Scalia, J., dissenting) ("DNA testing does not even begin until after arraignment and bail decisions are already made. The samples sit in storage for months, and take weeks to test.").

[363] EFF Comments on DHS Proposed Rule on Collection and Use of Biometrics 26–34 (Oct. 13, 2020) https://www.eff.org/document/eff-comments-dhs-proposed-rule-collection-and-use-biometrics-october-2020; *see also supra* Sec. VI(a)(v); Swedish Nat'l Forensic Ctr., *supra* note 304 (detailing serious problems with certain Rapid DNA analyzers, including "numerous issues with the system related to the hardware, firmware, software as well as the cartridges. The most severe issues are the retrieval of an incorrect DNA profile, PCR product or sample leakage and the low success rate. In total 36% of the runs had problems or errors effecting two or more samples resulting in a 77% success rate for samples consisting of . . . amounts where complete DNA profiles are expected.").

[364] Guest, *supra* note 307, at 1046; Zabel, *supra* note 292, at 58 (2019) (citing to Michael Edge et al., *Linkage Disequilibrium Matches Forensic Genetic Records to Disjoint Genomic Marker Sets*, 114 Proc. Nat'l Acad. Scis. 5671, 5672 (2017)).

[365] Guest, *supra* note 307, at 1019.

this information where available to narrow the pool of suspects based on genetic information exposed through more expansive DNA analysis, such as health-related data.[366] Advocates for DNA collection argue that the majority of collected DNA is "junk DNA," meaning it only has forensic utility and does not provide additional information about a person. However, recent scientific advancements show that this DNA may provide sensitive information with advancements in DNA interpretation.[367]

Most significantly, DNA can determine familial association. Without their knowledge or consent, relatives of a lead or suspect (who may not even know of their existence) may find themselves caught up in an investigation.[368] In no other context would it be lawful for a government actor to implicate an arrestee's family members in crimes unrelated to the crime for which the arrestee was charged;[369] and this government conduct should be appropriately constrained in this context. If the argument is that DNA testing is necessary for identification, then it should not be permissible to use it for the investigation of other crimes absent a warrant.[370] This is exacerbated where the "crime" is not a crime at all but merely entering the country, which could expose relatives to enhanced surveillance purely by virtue of their genetic association to the non-citizen.[371]

[366] Zabel, *supra* note 292, at 70.

[367] *See* Jennifer Welsh, *Stanford Medicine-led study clarifies how 'junk DNA' influences gene expression*, Stan. Med. (Sept. 26, 2023), https://med.stanford.edu/news/all-news/2023/09/junk-dna-diseases.html; Jake Buehler, *The Complex Truth About 'Junk DNA'*, Quanta Mag. (Sept. 1, 2021), https://www.quantamagazine.org/the-complex-truth-about-junk-dna-20210901/.

[368] James W. Hazel & Christopher Slobogin *"A World of Difference"? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 Duke L.J. 705, 724 (2021).

[369] Mason, *supra* note 316, at 208 (citing to Scalia's dissent in *Maryland v. King*).

[370] Scarlett L. Montenegro, *Criminalizing Asylum: DNA Testing Asylum Seekers Violates Privacy Rights*, 29 Am. U. J. Gender Soc. Pol'y & L. 123, 137 (2020), https://digitalcommons.wcl.american.edu/jgspl/vol29/iss1/4/.

[371] J. Lyn Entrikin, *Family Secrets and Relational Privacy: Protecting Not-So-Personal, Sensitive Information from Public Disclosure*, 74 U. Miami L. Rev. 781, 875–76 (2020).

As a legal matter, unlike fingerprints and photographs, extraction and analysis of DNA, as *King* itself makes clear, does constitute a Fourth Amendment search.[372]

3. *Chilling effects.*

In the aftermath of 9/11, excessive police surveillance of Muslim communities resulted in a significant chilling effect on First Amendment-protected activities.[373] During Baltimore protests of the death of Freddie Gray in police custody, surveillance technologies were used to identify and apprehend protestors with outstanding arrest warrants.[374] Regarding DNA evidence specifically, in 2012 the NYPD collected DNA from a chain used by Occupy Wall Street protestors.[375] Beyond chilling political expression and other Constitutionally-protected rights, ongoing and comprehensive police surveillance of poor people and people of color can impact self-determination, self-expression and freedom of association, including daily decisions about whether to spend time outside with friends, or what route to take to school or work, so as to minimize the opportunity for an unwelcome encounter with police.[376]

Unchecked law enforcement surveillance can also chill reporting of crimes,[377] use of medical tests for public health purposes,[378] and use of direct-to-consumer genetic services (thereby undermining one key value of those databases to law enforcement agencies).[379] For victims of crime in particular, the use of DNA evidence and accompanying questions has historically lead to the

[372] Logan, *supra* note 320, at 275.
[373] Hussain et al., *supra* note 346 (citing to Diala Shamas & Nermeen Arastu, *Mapping Muslims: NYPD Spying and Its Impact on American Muslims*, Muslim Am. C.L. Coal. (MACLC) & Creating L. Enf't Accountability & Resp. (CLEAR) Proj. (2013), https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf).
[374] Proj. On Gov't Oversight, *Tell Congress: Protect Our Constitutional Rights* (Aug. 22, 2023), https://www.pogo.org/take-action/tell-congress-protect-our-constitutional-rights.
[375] Kreag, *supra* note 314, at 1530–31.
[376] *Id.* at 1531–32.
[377] Leary, *supra* note 331, at 277–78.
[378] Ram, *supra* note 312, at 1302, 1305.
[379] Zabel, *supra* note 292 at 61; Guerrini, *supra* note 293, at 17.

prosecution discrediting the victim or deciding not to pursue the case due to irrelevant information such as use of birth control, presence of a sexually-transmitted disease, sexual history, or drug use.[380] Additionally, while it may be necessary for police to collect DNA as part of an investigation, this genetic information should not be added to databases.[381] It is unfair to force victims to choose between giving up their privacy to a lifetime of genetic surveillance or giving up their ability to seek justice for a crime perpetrated against them.[382]

The DOJ should take active steps to prevent scope creep, equivocation that represents DNA as equivalent to fingerprints, and law enforcement misuse that causes chilling effects; this can be achieved through measures such as strictly enforced purpose limitations, discussed further in Section VI(b) *infra*.

iv. Disparate impact.

Genetic databases can only register matches for information that's in the database, meaning that it is more likely that communities that are more represented in the database will turn up as possible matches and as a result be implicated in a future crime.[383] This is especially problematic

[380] Leary, *supra* note 331, at 261–62.

[381] Indeed, DOJ has sometimes commented on labs that have transgressed this rule. *See, e.g.*, Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 Minn. L. Rev. 541, 559 (2016) ("What is more, based on even the limited audits conducted to date, it is known that states frequently upload DNA profiles not authorized by law (e.g., those of victims).") (citing to Erin E. Murphy, *Inside the Cell: The Dark Side of Forensic Data* 140–41 (2015) (noting that audits of 22 of the roughly 190 laboratories nationwide revealed an error rate of six percent)).

[382] Kreag, *supra* note 314, at 1493.

[383] Zaretsky, *supra* note 293, at 347; Abrahamson *supra* note 306, at 2547; Christian B. Sundquist, *Genetics, Race and Substantive Due Process*, 20 Wash. & Lee J. Civ. Rts. & Soc. Just. 341, 380 (2014); Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 Cal. L. Rev. 1847, 1899 (2020) (citing to Rori V. Rohlfs et al., *Familial Identification: Population Structure and Relationship Distinguishability*, PLoS Genetics 2 (Feb. 9, 2012), https://doi.org/10.1371/journal.pgen.1002469) (noting that errors in assumptions about allele frequency distributions can cloud assessment of relatedness, that Native Americans and some immigrant groups are more likely to be falsely implicated in familial searches or partial match searches).

where being put into a database has no correlation to actually having been convicted of a crime,[384] in stark opposition to the idea of presumption of innocence.[385] These issues are exacerbated by permitting investigation methods that lower the threshold that triggers a lead (e.g. partial matches, FGGS, etc.).[386] The risk of false positives in low threshold searches also increases as database size increases;[387] and database size may not actually meaningfully help solve the crime at issue.[388] There are several examples of DNA "matches" that led to suspicion or false arrests, some not even using the riskier FGGS method,[389] but as the threshold is relaxed, these risks predictably increase.[390]

As noted above, "spit and acquit" programs, which coerce individuals into turning their genetic data over to law enforcement,[391] also exacerbate existing disparities. Marginalized groups that may have disproportionately greater contact with the criminal justice system and may have disproportionately fewer resources to effectively challenge weak cases or improper procedure will

[384] Divya Ramjee et. al., *The Challenges of Forensic Genealogy: Dirty Data, Electronic Evidence, and Privacy Concerns*, 98 Denv. L. Rev. 157, 162 (2020); Saira Hussain & Matthew Guariglia, *The U.S. Government's Database of Immigrant DNA Has Hit Scary, Astronomical Proportions*, EFF (Sept. 25, 2023), https://www.eff.org/deeplinks/2023/09/us-governments-database-immigrant-dna-has-hit-scary-astronomical-proportions; Kreag, *supra* note 314, at 1497 (citing to Jane Bambauer, *Hassle,* 113 Mich. L. Rev. 461, 482 (2014) and to Rachel A. Harmon, *The Problem of Policing*, 110 Mich. L. Rev. 761, 792–93 (2012)).

[385] Kitchen, *supra* note 348, at PDF p. 4 ("DNA databases go against the presumption of innocence because law enforcement continually and repeatedly search the databases, essentially turning every person whose genetic profile is contained therein into suspects for unlimited future crimes.").

[386] *See* Sulpizio, *supra* note 318, at 434 (quoting the co-founder of the Innocence Project in saying: "[N]o one should be allowed to embark on a fishing expedition "trolling and trawling the DNA database for evidence until you find what you want.").

[387] Amy A. Liberty, *Defending the Black Sheep of the Forensic DNA Family: The Case for Implementing Familial DNA Searching in Minnesota*, 38 Hamline L. Rev. 467, 481–82 (2015).

[388] Jeremiah Goulka et al., *Toward a Comparison of DNA Profiling and Databases in the United States and England*, RAND Corp., 1, 20 (2010), https://www.rand.org/content/dam/rand/pubs/technical_reports/2010/RAND_TR918.pdf (the ability of police to solve crimes using DNA is "more strongly related to the number of crime-scene samples than to the number of offender profiles in the database").

[389] *See, e.g.*, Lynch, *supra* note 355.

[390] Ramjee et. al., *supra* note 384, at 171–72.

[391] Ortyl, *supra* note 317, at 427 (citing to Lauren Kirchner, *DNA Dragnet: In Some Cities, Police Go From Stop-and-Frisk to Stop-and-Spit,* ProPublica (Sept. 12, 2016, 8:00 AM), https://www.propublica.org/article/dna-dragnet-in-some-cities-police-go-from-stop-and-frisk-to-stop-and-spit). This is especially true when applied to traffic stops or being stopped on the street, as is currently the case in Florida. *See id.*

therefore be more susceptible to coercive tactics that result in disproportionately greater representation in these databases.[392] This has potential psychological and sociological implications, as Prof. Jason Kreag noted nearly a decade ago:

> The message is not, "we are all in this together. We are gathering everyone's DNA." Rather, the message is, "I identified you as a potential future criminal. We need your DNA on file, forever, to be able to catch you when you most assuredly act on your criminal instincts." Even if our ability to predict future criminal behavior improves dramatically, this message carries the potential for perverse and lasting effects on citizens targeted by police.[393]

FGGS is a difference of kind, not a mere difference of degree, from other types of genetic searches, as it puts entire families under lifelong[394] surveillance, again with disparate impacts.[395] As noted immediately above, because certain populations are more likely to appear in a DNA database than others, law enforcement agencies are more likely to detect familial matches for members of those populations than for other populations. Especially where law enforcement agencies seek consent to collect DNA and add it to a database, this seems to provide a systematic method by which the government targets members of a few populations for lifelong genetic surveillance, while subjecting other populations to less rigorous genetic scrutiny.

[392] Subramanian et al., *supra* note 325; Trivedi & Keenan, *supra* note 325.

[393] Kreag, *supra* note 314, at 1535. Kreag also cites to the work of Professor David Sklansky in the context of officers who repeatedly invade citizens' privacy interests, as well as to the work of Professor Cecelia Klingele who warns against systems that reinforce the idea that those implicated in the criminal justice system "are inherently different and, perhaps, less human than people who have not been arrested or convicted." *Id.*; *see also* Zaretsky, *supra* note 293, at 352 (noting disproportionate impact for Latinx individuals of being coded as criminals).

[394] Arguably even longer than one lifetime, as the genetic information of future generations is implicated in familial searches of databases of genetic information.

[395] Alexandra Aherne, *Support of Familial DNA Testing in Illinois Criminal Investigation*, 38 N. Ill. U.L. Rev. 553, 578 (2018) (citing to Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J. L. Med. & Ethics 248, 255 (2006)); Giannaros, *supra* note 326, at 475 (citing to Jeffery Rose, *Genetic Surveillance for All?,* Slate (Mar. 17, 2009)).

1. *Additional disparate impact concerns for specific populations.*

Considerations about disparate impact in DNA analysis are not limited to disproportionate contact with the criminal justice system, but also entail disproportionately severe negative consequences suffered by some populations that are not suffered by others. For example, collection of biometric information of children poses "lifelong data risks" to those future adults,[396] even if initially collected for the purposes of authentication for health research purposes before being handed over to law enforcement.[397]

It's remarkable to think that at one time the DOJ wrote that fingerprinting is "one of the most intrusive procedures in the juvenile justice process,"[398] while today DNA collection could be considered nonintrusive.[399] Voluntary collection of DNA from juveniles present unique questions of consent.[400] Involuntary collection of DNA from juveniles also presents serious issues, as many states permit DNA collection for offenses as minor as misdemeanor delinquency findings.[401] Regardless of which crimes trigger inclusion in a database, DNA profiling is a permanent consequence that runs contrary to the "fresh start" our system is designed to offer juvenile offenders, with no demonstrable rehabilitative or deterrent effect.[402] At least one international court has recognized the risk of stigmatization caused by collecting DNA from juveniles.[403] Juveniles bear the burden of requesting expungement in all but one state.[404]

[396] UNICEF, Faces, Fingerprints & Feet 19 (July 2019), https://data.unicef.org/resources/biometrics/.
[397] Ram, *supra* note 312, at 1256.
[398] Lapp, *supra* note 315, at 483 (citing to *Juvenile Records and Recordkeeping Systems*, DOJ Bureau Just. Statistics, v (Nov. 1988), http://www.bjs.gov/content/pub/pdf/jrrks.pdf).
[399] *Id.*
[400] Lapp, *supra* note 315, at 487 (citing to *State v. Butler* 302 P.3d 609, 614 (Ariz. 2013)).
[401] Kevin Lapp, *Compulsory DNA Collection and A Juvenile's Best Interest*, 14 U. Md. L.J. Race, Religion, Gender & Class 50, 56–57 (2014).
[402] Lapp, *supra* note 315, at 441.
[403] *Id.* at 477 (citing to *S & Marper v. United Kingdom*, 2008-V Eur. Ct. H.R. 167 (2008)).
[404] *Id.* at 445 (citing to Julie E. Samuels et al., *Collecting DNA from Juveniles*, Urb. Inst. 13 (Apr. 2011), http://www.urban.org/UploadedPDF/417487-Collecting-DNA-from-Juveniles.pdf).

Non-citizens are also particularly vulnerable to harms resulting from DNA collection by law enforcement agencies. Because of a recent 2020 rule change, DHS collects DNA from detained immigrants, both at the border and in the immigration detention system, putting family members already in the country at increased risk.[405] There are no special laws to protect lawful asylum seekers, and non-citizens may not be able to enjoy a right to expungement[406] (although see Section VI(a)(ii)(3) *supra* why that may be largely illusory anyway). Moreover, DHS's poor track record of maintaining their databases creates a serious risk of unwarranted arrest and DNA collection. A federal court has found that independent investigations of DHS databases meant to track violative conduct of immigrants exposed error rates as high as 42%.[407] Immigration officers have no probable cause of a serious offense to justify extracting DNA from immigrants lawfully seeking asylum.[408] The U.N. Human Rights Committee has voiced concerns about long-term retention of DNA profiles and samples used to create those profiles,[409] a view echoed by scientists, bioethicists, legal scholars, and human rights advocates.[410] Statistics presented by DHS about incidents of fraud amongst immigrating families misleadingly suggest a severe problem where in reality they amount to fewer than half of one percent of all family crossings.[411]

The government should err closer to the side of public trust and civil liberties where the stakes are as high as lifelong genetic surveillance of an individual and their entire family.

[405] Montenegro, *supra* note 370, at 140. Notably, deportation is a civil, not a criminal, proceeding. *Id.* at 139.
[406] Zaretsky, *supra* note 293, at 326, 329.
[407] Hussain et al., *supra* note 346.
[408] Montenegro, *supra* note 370, at 137.
[409] Zaretsky, *supra* note 293, at 323.
[410] *Id.*
[411] Hussain et al., *supra* note 346.

v. Reliability.

While DNA analysis has facilitated positive outcomes for wrongfully-convicted defendants,[412] it is far from perfect. There have been wrongful arrests based on DNA analysis.[413] While results from single-source DNA matching in a controlled lab environment are generally reliable, the same cannot be said of partial match analysis or of FGGS which is inherently a scattershot approach.[414] The distribution of DNA profiles throughout a population is likely still unknown.[415] There are additionally questions about process, and about lab performance auditing. Riskier methods such as seeking matches with data in direct-to-consumer (DTC) genetic databases, and collecting data in the field via RapidDNA testing, exacerbate many of these issues.

1. *Process issues.*

There are a number of process questions that could impact how genetic information should be treated by law enforcement agencies, and why the DOJ and DHS should cultivate greater public trust by being explicit that DNA-based investigative methods are not perfect, which should help to mitigate overreliance and confirmation bias in government use of genetic information. For example, where a law enforcement agent is required to "exhaust standard investigative leads" before relying on a riskier method – what are standard investigative leads and what must be done before it can be said that they have been sufficiently exhausted?[416] Use of DTC databases are supposed to be a last

[412] Daniele Selby, *DNA and Wrongful Conviction: Five Facts You Should Know*, Innocence Proj. (Apr. 25, 2023), https://innocenceproject.org/dna-and-wrongful-conviction-five-facts-you-should-know/.
[413] The Legal Aid Society, *After Wrongful Arrest, LAS Calls for End to City DNA Index* (Oct. 21, 2019), https://legalaidnyc.org/news/wrongful-arrest-legal-aid-end-city-dna-index/.
[414] Zabel, *supra* note 292, at 71; Abrams & Garrett, *supra* note 292, at 782; Jessica Gabel Cino, *Tackling Technical Debt: Managing Advances in DNA Technology That Outpace the Evolution of Law*, 54 Am. Crim. L. Rev. 373, 397–98 (2017); Ramjee et. al., *supra* note 384, at 162.
[415] Bret N. Bogenschneider, *How Accurate Are Probabilistic Odds Claims in Criminal Trials? A "Warranted Skepticism" Approach*, 89 Miss. L.J. 147, 176 (2020).
[416] Shanni Davidowitz, *23andeveryone: Privacy Concerns with Law Enforcement's Use of Genealogy Databases to Implicate Relatives in Criminal Investigations*, 85 Brook. L. Rev. 185, 197 (2019).

resort used for serious crimes,[417] but what happens when a law enforcement agent puts DTC front and center in its investigations?[418] While some suspects were fortuitously able to clear themselves,[419] what about innocent suspects without ironclad defenses, or those against whom charges are brought decades later? Just because genetic material was found at the scene of a crime does not mean the DNA belongs to the perpetrator.[420] Evidence can be compromised in the collection process or may have been subject to interpretative or clerical errors.[421] The fact that there are issues with profiles being entered into databases that should not have been and genetic information being retained (and moreover used) when it should have been expunged and/or destroyed[422] demonstrates that process deficiencies do occur. There should be greater transparency and oversight as to what other process deficiencies may be occurring as well as how the DOJ will take action to remedy those problems.

2. *Quantitative issues.*

In addition to procedural questions that must be asked of law enforcement agencies conducting investigations based on genetic information, there are also quantitative considerations

[417] DOJ Interim Policy, *supra* note 291, at 4–6.

[418] Zabel, *supra* note 292, at 58–59 (citing to Paige St. John, *DNA genealogical databases are a gold mine for police, but with few rules and little transparency*, L.A. Times (Nov. 24, 2019), https://www.latimes.com/california/story/2019-11-24/law-enforcement-dna-crime-cases-privacy).

[419] Zabel, *supra* note 292, at 71 (citing to Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 Mich. L. Rev. 291, 319 (2010)).

[420] *Id.*

[421] Logan & Ferguson, *supra* note 381, at 559; Comm. on Identifying the Needs of the Forensic Scis. Cmty., Nat'l Rsch. Council, *Strengthening Forensic Science in the United States: A Path Forward* 86–87 (Aug. 2009), https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf [hereinafter "*Strengthening Forensic Science in the United States*"].

[422] Logan & Ferguson, *supra* note 381, at 559 (citing to Logan, *supra* note 320, at 280); DOJ Off. of the Inspector Gen., Audit of Compliance with Standards Governing Combined DNA Index System Activities at the Pinellas County Forensic Laboratory Largo, Florida 10 (Aug. 2017), https://www.oversight.gov/sites/default/files/oig-reports/g4017004.pdf ("For each of the profiles we discuss below, the Laboratory lacked sufficient documentation to support its NDIS eligibility determination and did not adhere to the eligibility criteria set forth by the FBI. Therefore, the profiles should not have been uploaded to NDIS.").

with the labs themselves in which the testing and analysis is performed.[423] Studies have shown lab error rates between 1% and 5% or more, which calls into question claims that DNA is accurate at the 1:1,000,000 level.[424] There are other reasons to call this statistic into question as well.[425] One prominent study of analysts in 2011 found subjective elements may influence results; in testing the same samples, twelve qualified analysts reported no match, one reported a match, and four reported inconclusive findings.[426] Due to disparities in funding and other resources, there is a lack of standardization of best practices in crime labs.[427] In Houston, even basic samples were routinely misinterpreted by police technicians.[428] Lab technicians have shown confirmation bias,[429] as have FBI forensic analysts.[430] One lab employee was able to falsify evidence used in 100 convictions.[431] It is unreasonable to expect perfection; however, where there are deficiencies or discrepancies, they must be brought to light[432] and corrective action taken.

[423] Kitchen, *supra* note 348, at PDF p. 5 ("A reported match may be inaccurate if a laboratory errs; a suspect who provides a true match may not be the source if the match is purely coincidental. A coincidental match occurs when "the genotypes are truly identical—but the forensic sample came from another individual.")(internal citations omitted); *Strengthening Forensic Science in the United States*, supra note 421, at 69 ("And, although DNA analysis is considered the most reliable forensic tool available today, laboratories nonetheless can make errors working with either nuclear DNA or mtDNA—errors such as mislabeling samples, losing samples, or misinterpreting the data.").

[424] Kitchen, *supra* note 348, at PDF p. 5; Logan & Ferguson, *supra* note 381, at 559 (citing Murphy, supra note 381, who noted a lab error rate of six percent).

[425] Upon retesting, 1:1,000,000 was found to be closer to 1:40. *See, e.g.*, Kitchen, *supra* note 348, at PDF p. 6. *See also* Cino, *supra* note 414, at 374–75.

[426] Mercer & Gabel, *supra* note 287, at 676 (citing Itiel E. Dror & Greg Hampikian, *Subjectivity and Bias in Forensic DNA Mixture Interpretation*, 51 Sci. & Just. 204, 205 (2011)).

[427] *Strengthening Forensic Science in the United States*, *supra* note 421, at 4–6, 14–19.

[428] Goldstein, *supra* note 304, at 600; Matthew Shaer, *The False Promise of DNA Testing*, Atlantic (June 2016), https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.

[429] Goldstein, *supra* note 304, at 619 (citing John Rafael Peña Perez, *Confronting the Forensic Confirmation Bias*, 33 Yale L. & Pol'y Rev. 455, 459 (2015)).

[430] In analyzing a bombing, FBI forensic analysts were influenced by bias and circular reasoning in identifying a suspect. *Strengthening Forensic Science in the United States*, *supra* note 421, at 45–47.

[431] *Id.* at 44–45.

[432] President's Council of Advisors on Sci. & Tech., *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* 75 (Sept. 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf ("Finding 2: DNA Analysis") [hereinafter "PCAST Report"].

The provenance of the samples themselves may also raise questions. In one experiment, in 85% of instances the DNA detected from a knife was not solely the DNA of the person who handled the knife directly but included the DNA of the person with whom the knife handler had shaken hands for two minutes prior to handling the knife.[433] DNA at a crime scene may not belong to a suspect, and may end up in a database like CODIS anyway.[434]

3. Riskier methods such as LCN, FGGS, DTC Searches and RapidDNA.

Certain methods of DNA testing and analysis implicate greater risks of error and greater consequences when misused by law enforcement agents. High-sensitivity methods, for example, increase the likelihood of obtaining profiles from irrelevant DNA, meaning a higher rate of false positives.[435] Accredited forensic laboratories must meet FBI Quality Assurance Standards (QAS), which includes reporting that results are inconclusive where they cannot provide a probability statistic for a DNA profile under FBI standards.[436] However private labs, to which testing and analysis work may be outsourced, are not required to maintain the same standards, which can be particularly problematic where high-sensitivity methods are used.[437] State and local databases may also suffer from poor-quality DNA samples, which may be collected in cases ranging from "property to drug crimes to quality-of-life offenses"; i.e. offenses far afield from the original scope of DNA

[433] Leary, *supra* note 331, at 261–62 (2017). In 20% of instances the non-knife-handler DNA was identified as the main or only DNA contributor. *Id.*; *see also* Kitchen, *supra* note 348, at PDF p. 5 ("Naturally shed DNA does not necessarily identify the suspect, "just the person who left the most cells or shed them the fastest," but DNA evidence leads to convictions regardless. These errors lead to nonmatches one quarter of the time.") (internal citations omitted).
[434] Leary, *supra* note 331, at 261–62; *see also* Najla Hasic, *An Invasion of Privacy: Genetic Testing in an Age of Unlimited Access*, 44 S. Ill. Univ. L.J. 517, 533–34 (2020).
[435] Press, *supra* note 302; Goldstein, *supra* note 304, at 619–20.
[436] Ramjee et. al., *supra* note 384, at 186.
[437] Ortyl, *supra* note 317, at 427.

collection and testing.[438] In Texas, correcting for this likely impacted thousands of cases; and it may be a problem present in labs nationwide.[439]

Familial searches in particular should require additional scrutiny and evaluation,[440] with clear reporting on the statistics underlying the result. One UK study found that only 17% of familial DNA searches resulted in the identification of a relative of the actual offender; an untrained legal professional or a juror may not appreciate the difference in accuracy between this type of test[441] and testing subject to FBI QAS. As of 2022, there were no specific FGG standards,[442] although a proposed guidance document was released that year.[443] In terms of direct to consumer (DTC) searches, beyond a lack of standards,[444] DTCs are not required to publish their error rates.[445] More than one study has found a high prevalence of false positives in DTC DNA profile matching.[446] Beyond questions of quality assurance with DTC databases, there are also questions of consent.[447]

Less rigorous methods risk greater margins of error. Even sterile labs can have issues with DNA testing; thus, it is of little surprise that Rapid DNA testing performed by police officers, not lab

[438] Mercer & Gabel, *supra* note 287, at 644.

[439] Kitchen, *supra* note 348, at PDF p. 5 ("In Texas, the labs were "using cutting-edge 'testing kits' that can extract tiny traces of DNA from crime scenes, but those samples were then analyzed with math that's not suited to 'weak' samples that combine DNA from many people." This issue may have affected thousands of Texas cases since 1999. These serious reliability questions led Texas prosecutors to retest cases with potentially faulty DNA—"a herculean task." The problem is present in labs across the country.") (internal citations omitted).

[440] Liberty, *supra* note 387, at 476.

[441] Zabel, *supra* note 292, at 71.

[442] Glynn, *supra* note 291.

[443] *See generally* Ray A. Wickenheiser et al., *National Technology Validation and Implementation Collaborative (NTVIC) policies and procedures for Forensic Investigative Genetic Genealogy (FIGG)*, 7 Forensic Sci. Int'l: Synergy (2023) https://www.sciencedirect.com/science/article/pii/S2589871X23000037.

[444] *But see* Elisa Jillson, *The DNA of privacy and the privacy of DNA*, FTC Bus. Blog (Jan. 5, 2024), https://www.ftc.gov/business-guidance/blog/2024/01/dna-privacy-privacy-dna.

[445] Ramjee et. al., *supra* note 384, at 175 ("DTCs are not required to publicize their error rates, and unfortunately, when error rates are not monitored or publicized, laboratories cannot take preventative measures to ensure accuracy in results.") (internal citations omitted).

[446] Nsikan Akpan, *Genetic genealogy can help solve cases. It can also accuse the wrong person.*, PBS NewsHour (Nov. 7, 2019), https://www.pbs.org/newshour/science/genetic-genealogy-can-help-solve-cold-cases-it-can-also-accuse-the-wrong-person.

[447] Ramjee et. al., *supra* note 384, at 162.

technicians, in a police station, not in a forensic lab, has lower accuracy rates.[448] Best practice suggests Rapid DNA testing should only be conducted by an independent, third-party lab and not until an arraignment or conviction.[449]

As of 2013, DHS indicated that Rapid DNA required significant privacy and civil rights policies to be developed or revised before the agency should be allowed to use it.[450] DHS released an updated Privacy Impact Assessment (PIA) for operational use of Rapid DNA testing in 2019[451] which does not address civil rights at all, claims an increase in family fraud but does not provide any actual statistics, claims it is ”highly unlikely” the system will provide an incorrect match despite known errors with Rapid DNA testing,[452] does not address the possibility of adoptive or step-parent relationships as negative matches,[453] and notes that it will update the PIA prior to DHS using Rapid DNA to detect family fraud outside the border context (e.g. among lawful permanent residents).[454]

vi. Transparency, accountability, and public trust.

Transparency and accountability to lawful and democratic processes are the pillars upon which law enforcement agencies should strive to rebuild public trust. The current dynamic is one of secrecy, of lack of oversight, of unmitigated government power, and of the costs of risky methods being externalized onto people who may not have the political power to correct that problem.

[448] Goldstein, *supra* note 304, at 622.
[449] *Id.* at 646.
[450] Erin R. Steward, *Discussion and Evaluation: The Legality and Use of Rapid DNA Technologies*, 84 UMKC L. Rev. 1133, 1150 (2016) (citing DHS, Privacy Impact Assessment for the Rapid DNA System 1, 4 (Feb. 8, 2013), https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy-pia-rapiddna-20130208.pdf).
[451] DHS, Privacy Impact Assessment for Rapid DNA Operational Use, No. DHS/ICE/PIA-050 (June 25, 2019), https://www.dhs.gov/publication/dhsicepia-050-rapid-dna-operational-use.
[452] *See* Swedish Nat’l Forensic Ctr., *supra* note 304.
[453] Trevor Kirby, *DNA Testing in Immigration Control*, Regul. Rev. (Mar. 15, 2022), https://www.theregreview.org/2022/03/15/kirby-dna-testing-immigration-control/.
[454] PIA, No. DHS/ICE/PIA-050, *supra* note 451 at 11–12. DHS may have suspended use of Rapid DNA for detecting family fraud as of May 31, 2023. *See* Letter from Sen. Rubio et al. to Hon. Alejandro Mayorkas (May 26, 2023), https://www.rubio.senate.gov/wp-content/uploads/_cache/files/17d3d5cd-2a02-4d7a-bd1a-d6fb6cc4e8bc/35EE754CF04D23187A5BA6E5DC1BC516.05.26.23---rubio-letter-to-mayorkas-re-familial-dna-testing-.pdf. Concerns about its use are still relevant in the event that the program resumes.

A lack of transparency creates the preconditions necessary for more severe problems to develop. It is difficult to hold law enforcement agencies accountable for deficiencies in DNA testing if they operate without transparency; for example, agencies have "shrouded their use" of DTC databases "in secrecy," including how samples were obtained and which databases were used.[455] Match percentages should be published and interrogated both in courts of law and in courts of public opinion;[456] error rates should be disclosed.[457] These should be explained in terms that the average person could readily understand, for example "the birthday problem": there's a 1:365 chance of a birthday on a given day but a 1:2 chance that two people share a birthday out of a group of twenty-three people.[458] Law enforcement agencies should be clear about whether a technology such as DNA testing actually led to the guilty party or whether it merely generated leads that did not advance the investigation meaningfully.[459] This can also help inform cost-benefit analysis of surveillance technologies and techniques.[460] To better cultivate public trust, DOJ should also discourage equivocation about how these tools are used, for example claiming that CODIS cannot be used for family searches, which is technically true as a policy matter, but neglecting to clarify that data from CODIS may be used in DTC database searches to identify relatives.[461]

[455] Zabel, *supra* note 292, at 59; Kreag, *supra* note 314, at 1446–47.

[456] *See, e.g.*, Andrea Roth, *Admissibility of DNA Evidence in Court* (2020), https://www.law.berkeley.edu/wp-content/uploads/2022/03/Admissibility_of_DNA_Evidence_in_Court.pdf; PCAST Report, *supra* note 432, at 45, 56.

[457] *See, e.g.*, Hussain et al., *supra* note 346; Kitchen, *supra* note 348; Ramjee et. al., *supra* note 384; *see also Strengthening Forensic Science in the United States*, *supra* note 421, at 121.

[458] Karen Norrgard, *Forensics, DNA fingerprinting, and CODIS*, 1 Nature Education 35 (2008), https://www.nature.com/scitable/topicpage/forensics-dna-fingerprinting-and-codis-736/.

[459] *See, e.g.*, CODIS-NDIS Statistics Measuring Success, FBI, https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis/codis-ndis-statistics (last visited Jan. 19, 2024) ("Ultimately, the success of the CODIS program will be measured by the crimes it helps to solve. CODIS's primary metric, the "Investigation Aided," tracks the number of criminal investigations where CODIS has added value to the investigative process."). This relates to substantiation. *See* Sec. II, Recommendation Ten *supra*.

[460] Murphy & Tong, *supra* note 383, at 1898 ("At the same time, DNA databases exhaust greater and greater resources as they move unilaterally in the direction of expansion without any meaningful analysis of costs and benefits.").

[461] Ramjee et. al., *supra* note 384, at 168–69.

A lack of oversight increases the risk of Fourth Amendment violations, as law enforcement agencies are incentivized to solve crimes, not protect civil rights.[462] This results in practices like creating false accounts in DTC databases to bypass the website's policies for use by law enforcement,[463] or arguing in court that genetic match information should be treated as confidential informants.[464] To this latter point, defendants must be able to challenge the evidence presented against them.[465]

Lack of accountability can also lead to government power exerting itself in problematic ways. In the absence of regulatory oversight, for example, it may be hard to determine whether investigators are using these methods to identify women who have had abortions or civilians who committed a simple, non-violent transgression like trespassing.[466] Similarly, local law enforcement agencies may not adhere to DOJ policy regarding FGGS, and individual officers may independently select cases in a manner that exacerbates already-disproportionate contact between the criminal justice system and members of certain communities.[467] Where DNA is treated as abandoned property, the Fourth Amendment fails to protect sensitive genetic information from state power.[468] Paths to legal remedies in FGGS especially are complicated by issues of standing, despite not having a diminished expectation of privacy;[469] and may provide no meaningful way of opting out.[470] Even

[462] Ramjee et. al., *supra* note 384, at 195; Kreag, *supra* note 314, at 1439–40; *id.* at 1541 (citing Rachel A. Harmon, *The Problem of Policing,* 110 Mich. L. Rev. 761, 811 (2012)).
[463] Hazel & Slobogin, *supra* note 368, at 729, 732.
[464] Zabel, *supra* note 292, at 61–62.
[465] DOJ, Statement on the PCAST Report Abstract 2 (Jan. 11, 2021), https://www.justice.gov/d9/pages/attachments/2021/01/11/final_doj_statement_on_the_pcast_report_abstract_01.12.21.pdf ("The best insurance against false incrimination is the opportunity to retest the evidence."); *Strengthening Forensic Science in the United States*, *supra* note 421, at 100.
[466] Goldstein, *supra* note 304, at 616.
[467] Nieto, *supra* note 342, at 1796; Kreag, *supra* note 314, at 1546.
[468] Kitchen, *supra* note 348, at PDF p. 7–8, 12–14.
[469] Davidowitz, *supra* note 416, at 211.
[470] Zabel, *supra* note 292, at 51–52.

where there are internal policies, external regulations may be necessary to detect and curtail misuse by bad actors.[471]

The power dynamic between law enforcement agencies and those most likely to be subject to genetic surveillance demands greater consideration of the costs of DNA-driven investigations and policies not only in terms of public trust, but also in terms of the actual harms caused to individuals and their families. Law enforcement agencies have no obligation to repair the damage done to a person (or their family's) reputation as a result of an investigation,[472] and have minimal incentive to do so either.[473] Federal funding of local genetic databases short-circuit what democratic process there might have been locally to reduce funding for these databases,[474] or funding may come from criminal fines to cover DNA databank fees.[475] Even where policymakers may have an appetite for regulating surveillance technologies, they are often not notified of new techniques in advance.[476]

All of these problems need to be addressed in order to adequately correct this problematic power dynamic.

b. Recommendations for DNA and genetic surveillance.

Law enforcement agencies seeking to use genetic information must adhere to the ten recommendations below; DOJ and DHS should each leverage what authority it has to compel, or where appropriate to incentivize, adherence to these principles, in the interest of protecting civil rights, civil liberties, and privacy, as well as in the interest of strengthening public trust in law enforcement agencies.

[471] Kreag, *supra* note 314, at 1543; Hazel & Slobogin, *supra* note 368, at 729, 732.
[472] Zaretsky, *supra* note 293, at 353.
[473] Kreag, *supra* note 314, at 1541–42.
[474] *Id.* at 1505–06.
[475] Abrams & Garrett, *supra* note 292, at 782.
[476] Kreag, *supra* note 314, at 1545–46.

Recommendation One: DOJ and DHS should prohibit mass surveillance.

Numerous aspects of DNA testing and analysis risk exacerbating or in some instances enabling mass surveillance. The DOJ should make it a top priority to prevent something so antithetical to America's democratic values from occurring. DOJ can achieve this with several important guardrails on when DNA can be collected, when DNA can be added to a database, and how to ensure expungement policies are fair and enforced.

The DOJ should not permit DNA collection for non-violent crimes. The DOJ should not permit DNA evidence collected by DHS to be used for other purposes, nor shared with other agencies. The DOJ should not permit data collected for public health purposes, including screenings for newborns, to be used for law enforcement purposes.

The DOJ should not let DNA collected without a warrant to be added to a database prior to a conviction. Specifically: the DOJ should not permit DNA collected voluntarily to be added to a database, and where that occurs anyway require meaningful expungement (revocation of consent). The DOJ should not permit DNA collected coercively (e.g. spit and acquit programs) to be added to a database.

Expungement should be automated and audited to make sure this occurs in a timely manner and that to-be-expunged data is not used (with penalties when to-be-expunged data is used), and clarify that expungement applies to samples not merely profiles (to the extent that samples weren't destroyed at the time that profiles were created). DNA collected from juvenile offenders to the extent that it is permitted to occur should be automatically expunged.

Recommendation Two: DOJ and DHS should protect civil rights.

With very narrow exceptions, the DOJ should not permit use of DNA collection in conjunction with protected activities such as protests and places of worship. The DOJ should take great pains to prevent chilling reporting of a crime where a victim fears how their DNA may be used. The DOJ should put guardrails in place to prevent or at least mitigate subsequent harms from coercive tactics like "spit and acquit" programs. The DOJ should investigate how it can create greater incentives to protect civil rights and not merely solve crimes. The Department must rein in these harms before they can occur, especially where the courts fail to protect civil rights by eroding standing, privacy rights in one's shed DNA, and the ability to interrogate DNA evidence.

Recommendation Three: DOJ and DHS should protect criminal defendants' constitutional rights by not entering genetic information into a database without a conviction and ensuring that the technology is subject to adversarial interrogation during criminal litigation.

To safeguard the presumption of innocence, data should not be entered into a database prior to a conviction, and should be automatically expunged and destroyed if that conviction is subsequently overturned. Labs that conduct analysis must be independent from law enforcement agencies,[477] and must disclose their match rates, proficiency audits, and other indicia that might be relevant to challenging DNA evidence in court.

Recommendation Four: DOJ and DHS should ensure technology is provably non-discriminatory prior to deployment, and ensure processes do not cause disparate impacts.

The most impactful correction is to limit entering profiles into a database only for convictions and only for the most serious crimes, not merely for any contact with the criminal justice system. Expungement must be automated, so it's not just people with excess time and money who can enjoy the right to be free from lifelong genetic surveillance. The DOJ and DHS should consider how privacy harms may be different for different populations, and incorporate this information into their Privacy Impact Assessments (PIAs). The DOJ should update its FGGS policy and publish

[477] And independent from incentives to produce convictions. *See, e.g.*, Rebecca Brown, *3 Ways Lack of Police Accountability Contributes to Wrongful Convictions*, Innocence Proj. (Aug. 17, 2020), https://innocenceproject.org/lack-of-police-accountability-contributes-to-wrongful-conviction/ ("Nearly half of state public crime labs in the country are funded, at least partially, based on the number of convictions they produce rather than the number of forensic tests performed.").

explicit guidance about how to avoid disparate impact in familial searches; requiring a warrant for familial genetic searches would go a long way.

Recommendation Five: DOJ and DHS must carry out an adequate evaluation of technology and techniques prior to deployment.

Even established methods of DNA testing and analysis are not perfect; novel forms of DNA testing raise questions about their reliability and suitability for use in criminal contexts. Labs not subject to the DOJ's authority should still be required to publish how they are measuring up to the standards they hold themselves to.

Recommendation Six: DOJ and DHS must adopt a strict data minimization framework.

Data minimization is important for privacy as well as for cybersecurity. DNA collected as part of an investigation should not be added to a database absent a conviction. The DOJ should require that data collected from a victim of crime should only be used to solve that crime, and explicitly should not be used to potentially solve another crime in the future. Generally, DNA that is collected for one purpose should not be usable for other purposes, nor shared with other agencies for unrelated matters: for example, identification of an individual is not the same as generating leads for a crime, confirming whether a parent and child are biologically related is not the same purpose as identifying other relatives of that parent and child who may be criminal suspects.

Samples should be destroyed after profiles are created. Expungement should be automated and state-initiated, to minimize the possible harm that might occur in the event of a breach. The DOJ should expunge all DNA from CODIS added by DHS prior to a criminal conviction.

Recommendation Seven: DOJ and DHS should ensure data is adequately secure.

The DOJ should provide support, both financially and in terms of its expertise, to owners and operators of genetic databases to ensure that such sensitive information enjoys heightened cybersecurity protections.

Recommendation Eight: DOJ and DHS should require independent auditing of technology.

Although DOJ requires submissions of certifications to maintain eligibility to access CODIS, the Department should be enabling and demanding greater standards for other law enforcement agency labs and for use of DTC databases. The DOJ should publish results from, or conduct if it has not performed any, recent FBI QAS audits.

Recommendation Nine: DOJ and DHS should strengthen accountability and oversight measures.

The DOJ should implement measures to enforce the above (and below) listed recommendations. For example, ensuring that FGGS is in fact only used after going through standard CODIS procedures, per its interim policy.[478] The DOJ should consider how oversight over state and local labs can prevent lab scandals that represent setbacks on all fronts, and how it can help to create safeguards, deterrents, and punitive measures to address misuse by bad actors.

Recommendation Ten: DOJ and DHS should emphasize transparency and public trust.

To advance the DOJ's goals of strengthening public trust, the Department should publish and require publication of match percentages and error rates, with exacting clarity about what types of methods the statistics apply to, so as to avoid equivocation. DNA enjoys a level of trustworthiness that is not applicable to all methods of DNA testing and analysis, including common scenarios such as mixed or degraded samples. As a matter of transparency and public trust (not merely of data minimization), DNA collected for one purpose should not be used for another. Equivocating about what crimes will be investigated using these methods, as well as failing to keep policymakers abreast of surveillance developments before they are implemented, also hurts public trust.

[478] DOJ Interim Policy, supra note 291, at 5.

c. How the DOJ can implement many of these best practices.

The DOJ has a number of carrots and sticks it can use to enforce the policies it chooses to enact. For example, it can restrict law enforcement access to CODIS,[479] the DOJ can create additional eligibility or reporting requirements for grant recipients,[480] it can create new funding streams dedicated to practices it wants to encourage, and the Department can implement oversight and accountability measures as a part of an inquiry into practices that may affect Americans' civil rights.

Many of our recommendations are consistent with already-implemented policy, for example requiring meaningful expungement practices,[481] and only entering appropriate profiles into CODIS. Additionally, the DOJ has conducted audits before, but never at a large scale and seemingly not at all within the last five or more years.[482] This is especially concerning where there is explicit reason to suspect these audits are necessary.[483]

VII. Conclusion

For too long, law enforcement agencies have expanded their use of invasive surveillance technologies without adequate safeguards, oversight, transparency, or accountability. Unfortunately, DOJ and DHS have not only failed to police their own use of these surveillance technologies, but they have done little to ensure that SLTT law enforcement agencies are complying with what

[479] FBI, *Frequently Asked Questions on CODIS and NDIS*, *supra* note 285 ("That is, if a state DNA database law permits access to the DNA samples and analyses in the state DNA database for purposes not contained in the Federal DNA Act (i.e., humanitarian purposes), and that state is participating in NDIS, then the state has agreed to comply with the more restrictive federal access provisions."); Logan & Ferguson, *supra* note 381, at 616 n. 361.

[480] *See, e.g.*, Bureau of Just. Assistance, FY 2023 Prosecuting Cold Cases Using DNA Program (Feb. 2023), https://bja.ojp.gov/funding/fy23-sol-overview-prosecuting-cold-cases.pdf; Fact Sheet, Bureau of Just. Assistance, Prosecuting Cold Cases Using DNA (Nov. 2023), https://bja.ojp.gov/doc/fs-prosecuting-cold-cases-using-dna.pdf.

[481] Goldstein, *supra* note 304, at 645–46.

[482] Logan & Ferguson, *supra* note 381, at 600.

[483] Abrams & Garrett, *supra* note 292, at 784–85.

minimal rules are in place for recipients of federal law enforcement funding. DOJ and DHS should take advantage of this opportunity to chart a new course, one based on a framework that ensures privacy, protects civil rights, and upholds civil liberties. EPIC recommends that a new framework be based on these ten principles:

- prohibiting mass surveillance;
- protecting privacy, civil rights, and civil liberties;
- protecting constitutional rights;
- proving that the technology and its implementation do not result in a disparate impact for protected classes;
- requiring adequate evaluation of the purpose, objectives, benefits, and risks of the technology;
- adopting stricter data minimization procedures;
- ensuring adequate security for retained data;
- regular independent auditing;
- strengthening accountability and oversight, and;
- advancing public trust, prioritizing transparency, and requiring substantiation for claims relating to the technology, especially related to its effectiveness.

EPIC looks forward to engaging with DOJ and DHS further on these urgent issues, and we stand by to assist your agencies however we can.

Respectfully submitted,

Jeramie Scott
Jeramie Scott
Director of the EPIC's Project on Surveillance Oversight

Ben Winters
Ben Winters
EPIC Senior Counsel

*Chris Frascella*_______
Chris Frascella
EPIC Counsel

*Chris Baumohl*________
Chris Baumohl
EPIC Law Fellow

Maria Villégas Bravo
Maria Villégas Bravo
EPIC Law Fellow