January 19, 2024

Office of Legal Policy
Department of Justice
950 Pennsylvania Ave. NW
Washington, DC 20530-0001

Re: Policing Technologies At Issue In Proposed Executive Order 14074

ABOUT NACDL

The National Association of Criminal Defense Lawyers (NACDL) is the preeminent organization in the United States advancing the goal of the criminal defense bar to ensure justice and due process for persons charged with wrongdoing. NACDL serves as a leader in identifying and reforming flaws and inequities in the criminal legal system and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level. NACDL is concerned that the use of untested, unregulated, and secretive policing technologies entrenches and exacerbates existing racial disparities, interferes with defense attorneys' ability to zealously represent their clients, and erodes defendants' due process rights. As a membership organization, NACDL is in a unique position to reflect the concerns of criminal defense lawyers across the country and by extension, the impacts of advanced policing technologies on the people they represent.[1]

NACDL's Fourth Amendment Center, specifically, has created resources and provided litigation assistance for the technologies at issue in Executive Order 14074 on Advancing Effective, Accountable

[1] In preparing this comment, NACDL conducted a survey of its members: defense attorneys across the country. Based on survey responses, NACDL conducted a number of follow-up interviews. Both the survey and the interviews were administered on the condition of anonymity to protect the privacy of individual attorneys. Throughout this comment, NACDL cites survey results and interview quotes.

Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety (EO 14074).[2] As in all its work, NACDL's guiding objective in submitting this comment is to address racial disparities and mass incarceration that are in the criminal legal system.

COMMENT

"It doesn't seem like anyone has answered a preliminary question — whether any of these technologies should be used at all. We've jumped immediately into assuming these are reliable and thus justifiable without putting any thought into that."[3]

The policing technologies at issue in EO 14074 create serious harms for individual criminal defendants, their lawyers, and the criminal legal system more broadly. Not only are the technologies designed to expand policing power, thereby exacerbating existing racial disparities within the criminal legal system and contributing to mass incarceration, but they are unreliable and opaque, adding unique due process concerns to an already flawed system.

---

[2] *See, e.g.,* Facial Recognition Primer, NACDL Fourth Amendment Center, available at https://www.nacdl.org/getattachment/5e6ea7e9-634a-45e5-866c-7172e201d155/face-rec-primer.pdf; Model Motion to Suppress Facial Recognition Evidence, NACDL Fourth Amendment Center, available at https://www.nacdl.org/getattachment/ac234f36-95d0-4b7c-8a0e-6bf422b5ecaf/redacted-facial-recognition-motion-8-28-18_flattened-5-.pdf; Police Face Recognition, NACDL Fourth Amendment Center, available at https://www.nacdl.org/getattachment/c5577827-601d-4331-83ad-4c2c8193af59/one-pager_face-recognition_handout_20190322.pdf; Brief of Amici Curiae, *Lynch v. Florida*, No. SC2019-0298 (Sup. Ct. March 11, 2019) (facial recognition); Resolution on Facial Recognition Technology, NACDL, available at https://www.nacdl.org/Content/NACDL-Facial-Recognition-Resolution,-4AC-Draft (Oct. 23, 2023); Forensic Genetic Genealogy Searches: What Defense Attorneys Need to Know, NACDL, available at https://www.nacdl.org/Article/Nov2020-ForensicGeneticGenealogySearchesWhatDefens; DNA – Probabilistic Genotyping, NACDL, available at https://www.nacdl.org/Content/DNA-Probabilistic-Genotyping; Recommendations on Data-Driven Policing, NACDL's Task Force on Predictive Policing, available at https://www.nacdl.org/Content/Recommendations-on-Data-Driven-Policing (Oct. 24, 2020); Garbage In, Gospel Out: How Data-Driven Policing Technologies Entrench Historic Racism and 'Tech-Wash' Bias in the Criminal Legal System, NACDL's Task Force on Predictive Policing, available at https://www.nacdl.org/getattachment/eb6a04b2-4887-4a46-a708-dbdaade82125/garbage-in-gospel-out-how-data-driven-policing-technologies-entrench-historic-racism-and-tech-wash-bias-in-the-criminal-legal-system-09142021.pdf (Sept. 2021).

[3] The quotes that appear at the beginning of each section are drawn from NACDL survey responses and follow-up interviews with defense attorneys across the country.

The federal government has acknowledged both the serious injustices and the astronomical costs generated by our system of mass incarceration.[4] Further, it has enacted legislation and passed executive orders designed to facilitate decarceration and address injustice within the criminal legal system.[5] Before diving into a focused assessment of the specific policing technologies referenced in EO14074, it is worth asking whether the use of these technologies facilitates the goals of reducing incarceration and racial disparities. Throughout this comment, NACDL urges the Department of Justice (DOJ) and Department of Homeland Security (DHS) to consider how the deployment of forensic[6] policing technologies—especially those that rely on proprietary algorithms built and managed by secretive companies—might accelerate and exacerbate, rather than redress, mass incarceration and racial disparities.[7]

In this comment, NACDL aims to highlight the serious dangers that these policing technologies pose and propose recommendations for mitigating those dangers. First, it outlines the constitutional and practical barriers that these policing technologies create for criminal defendants and their lawyers due to their unreliability and opacity. Then, it proposes recommendations, including the adoption of strict

[4] *See* First Step Act of 2018, available at https://www.congress.gov/115/plaws/publ391/PLAW-115publ391.pdf; Executive Order on Reforming Our Incarceration System to Eliminate the Use of Privately Operated Criminal Detention Facilities (Jan. 26, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/26/executive-order-reforming-our-incarceration-system-to-eliminate-the-use-of-privately-operated-criminal-detention-facilities/.

[5] *Id.*

[6] The word "forensic" is not intended to imply that these technologies have foundational validity.

[7] *See, e.g.,* NACDL Comment to the Office of Science and Technology Policy on Facial Recognition Technology (January 15, 2022), available at https://www.nacdl.org/getattachment/d0b14369-8e40-444f-8f95-3335b7acc6a6/nacdl-comments-to-the-office-of-science-and-technology-policy-on-biometric-technologies-january-2022.pdf; 21st Century Policing: The Rise and Reach of Surveillance Technology, Action Center on Race and the Economy & The Community Resource Hub for Safety and Accountability, Action Center on Race and the Economy & The Community Resource Hub for Safety and Accountability (2021), available at https://acrecampaigns.org/wp-content/uploads/2021/03/acre-21stcenturypolicing-r4-web.pdf.

oversight protocols, foundational validity requirements, rejection of technologies with a demonstrated racial bias, and comprehensive training and education for all actors within the criminal legal system.

For the reasons below, the report produced by the DOJ and the DHS in response to Executive Order 14074 should caution against the reflexive deployment of novel and untested policing technologies absent serious consideration of the ways in which they replicate and amplify systemic inequities while undermining the purported function and purpose of the criminal legal system.

A. Forensic Policing Technologies Create Constitutional and Practical Barriers for Criminal Defendants and Their Lawyers.

"Not having this information up front causes problems in these cases that often are not realized until a final resolution has been made."

NACDL has unique insight into the experience of the criminal defense bar, and by extension the people that defense attorneys represent. It therefore offers this comment to help explain how the deployment of novel policing technologies might affect those communities. It is appropriate to consider the defense perspective when evaluating the impact and value of policing technologies for two reasons. First, criminal defense lawyers have an intimate understanding of how various policing techniques affect their clients. Second, as constitutionally mandated actors in the criminal legal system, it is imperative that defense attorneys be able to zealously represent their clients.[8] Their perspectives on how the deployment of these technologies might affect the due process and equal protection rights of their clients are therefore essential in determining if or how these technologies should be rolled out. NACDL draws on the lived

[8] *See Gideon v. Wainwright*, 372 U.S. 335 (1963).

experiences of criminal defense lawyers and their clients, as well as available research and its own expertise on policing technologies, to draw the conclusions it presents below.

1. The policing technologies under consideration are unreliable.

"[They are] unreliable and will lead to false arrests and convictions."

All the technologies at issue in EO 14074 have documented reliability and accuracy problems.[9] The widespread deployment of unreliable and inaccurate policing technologies is dangerous for obvious reasons. If police rely on complex forensic technologies to perform essential functions like suspect generation and identification—especially those built on proprietary or black box algorithms—it is essential that those tools be reliable. Otherwise, police risk making mistakes like misidentifying suspects or responding with force to non-criminal events. These mistakes are likely to undermine both the actual crime-solving function of police and the credibility and fairness of the criminal legal system in the eyes of the public.

Criminal defense attorneys surveyed and interviewed by NACDL reflected significant concerns about the reliability of these technologies, especially in the context of how they are used by police. One respondent said that "there are definite concerns that should be addressed about genetic phenotyping and its tendency to over-focus investigations on one individual as opposed to using it as a tool. There needs to be greater education of [law enforcement officers] on the proper use of these tools to prevent [police]

[9] *See, e.g.,* Clare Garvie, A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations, Center on Privacy & Technology at Georgetown Law (2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf (facial recognition technology); John Butler et al., Executive Summary, "DNA Mixture Interpretation: A NIST Scientific Foundation Review" (2021), https://www.nist.gov/system/files/documents/2021/06/09/NISTIR_8351-draft_Executive_Summary.pdf (forensic DNA technologies); Aaron Sankin & Surya Mattu, "Predictive Policing Software Terrible at Predicting Crimes," Wired (Oct. 2, 2023) (predictive policing), https://www.wired.com/story/plainfield-geolitica-crime-predictions/.

from using [them] improperly." In a follow up interview, a defense attorney explained that these policing technologies "make[my clients] targets of investigations, often leading to arrests for things they have not done. It creates further suspicion in their communities. It also makes the police more likely to treat my clients and the people in their communities as different, or other."

On a technical level, none of these technologies are sufficiently reliable or accurate. For example, the studies that establish the purportedly impressive accuracy of facial recognition technology (FRT) algorithms are conducted in highly controlled settings that do not in any way resemble the criminal context.[10] Indeed, there are no studies that assess the reliability of FRT as it is applied.[11] There is, however, a significant body of research that suggests that due to "cognitive bias, low-quality evidence or manipulated evidence, and underperforming technology," FRT as it is applied in criminal investigations is likely quite unreliable.[12] Many relevant studies come directly from federal agencies, such as the National Institute of Standards and Technology and the DHS Science & Technology Directorate's Maryland Test Facility.[13]

Many government agencies, perhaps in acknowledgement of FRT's shortcomings, purport to use the technology for producing investigative leads, not for generating probable cause.[14] However, defense attorneys surveyed by NACDL report that in practice, the government uses FRT in a far more expansive

[10] *See, e.g.,* "NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding" (July 13, 2021), https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-softwares-accuracy-flight-boarding; Garvie, A Forensic Without the Science at 15–16, *supra* n.9.
[11] *Id.* at 15.
[12] *Id.* at 16–17; *see also id.* at 18–35 (outlining in detail the various sources of inaccuracy in FRT).
[13] *See* NIST, *Face Recognition Vender Test Part 3: Demographic Effects* (Dec. 2009), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; *see* Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems,* IEEE (Feb. 2019), https://mdtf.org/publications/demographic-effects-image-acquisition.pdf.
[14] *See* Report to Congressional Requesters, Facial Recognition Technology: Current and Planned Uses by Federal Agencies, U.S. Government Accountability Office, available at https://www.gao.gov/assets/gao-21-526.pdf.

capacity. One attorney interviewed reported that "one of the biggest problems is that [the government] propagandize[s] this by saying the tools are investigative leads and doesn't acknowledge that this steers the investigation. It creates tunnel vision for the investigation, especially for facial recognition. They then look for evidence to pin on the person that one of these leads has identified." Another attorney revealed that the government "often launders the facial recognition match through a different ID procedure," which leads courts to "deny our ability to challenge the FRT," making it extremely challenging to litigate probable cause in a hearing.

The other technologies under consideration are all significantly under-studied compared to FRT. But even preliminary research has revealed serious inaccuracies and inconsistencies regarding the use of those technologies in a criminal context, many of which mirror the same problems inherent in criminal investigative applications of FRT. The reliability of forensic genetic genealogy (FGG) and probabilistic genotyping techniques are highly dependent on sample quality, the degree of relatedness, and other factors.[15] The accuracy of predictive phenotyping techniques is highly variable depending upon the feature in question, the quality of the DNA sample, and other factors.[16]

The fact that prosecutors, judges, juries, and defense attorneys all lack a sufficient understanding of the difference between "regular DNA" evidence and these more complex types of DNA analysis leads to improper reliance on novel, untested technologies. One attorney explained that often his colleagues are

[15] *See* Rori Rholfs et al., The Influence of Relatives on the Efficiency and Error Rate of Familial Searching, 9(1) PLOS ONE 10 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3743829/ (describing highly variable accuracy in genotyping depending upon degree of relatedness); Butler, Executive Summary (describing limitations of probabilistic genotyping).

[16] Peter Schneider, The Use of Forensic DNA Phenotyping in Predicting Appearance and Biogeographic Ancestry, Dtsch Arztebl Int. (2019), available at https://pubmed.ncbi.nlm.nih.gov/31941575/ (describing limitations of predictive phenotyping technology in criminal investigations).

not even aware that the DNA evidence they have received is "probabilistic genotyping," rather than "regular DNA" evidence. And this limitation is not exclusive to defense lawyers. "Prosecutors will do the same thing: misinterpret DNA results. They'll look at a probabilistic genotyping report and [conclude that it is] so much more certain than DNA analysis, and then the defense is on the hook for correcting the prosecution's understanding of the technology and its results. But if they don't have a good understanding, or don't understand how complex it is, they might rely on the prosecution's interpretation that might also be incorrect. The lack of understanding is creating a huge problem."

Another attorney observed that there is a "lack of transparency about how probabilistic genotyping works as opposed to standard DNA testing, given that it begins with a presumption of guilt." And because there is inadequate information about "how the systems are used, or even just work, available to all players in the game, [] it usually goes undisputed." Another attorney expressed concerns about explaining this probabilistic genotyping to juries: "We had to . . . fight like hell to get the underlying data. In hindsight, after learning more about the [probabilistic genotyping] technology, we now know there's a lot more information we should have requested and fought for about the software and its use than we did. Information about the policies [was] also next to impossible to come by . . . so it's been a struggle to become adequately familiar with it in a way that allows defense attorneys to present a compelling case . . . at a jury trial."

"Predictive policing" and other data-driven policing technologies are the worst of all, with some tools accurately prediction crimes less than one percent of the time.[17] It is worth noting that while EO 14074 distinguishes between person- and place-based predictive policing, that distinction is largely

[17] Sankin & Mattu, "Predictive Policing Software Terrible at Predicting Crimes."

artificial. All "predictive policing" technologies are unreliable and inaccurate for similar reasons: namely, that the input data is biased so as to completely invalidate the reliability of the outputs. NACDL has chosen to use the term "data-driven policing" rather than "predictive policing" because it better captures the type of tool or practice at issue—namely, tools that use data to determine where, how, and who to police—and to avoid the shifting sands of policing tech terminology.[18] Not only are these tools wildly unreliable, but they are commensurately. When asked about "predictive policing" tools, one attorney said that "not only do they not work, they set up even well-meaning officers to look at someone in a way that maybe they don't deserve to be looked at. If your predictive policing software says this person is violent, you're more likely to look at them that way, which is more likely to lead to wrongful investigations, convictions, or to lead to someone being shot."

Law enforcement has repeatedly made the mistake of deploying untested forensic technologies that turns out to be junk science, a crisis that has been explored in depth by federal bodies.[19] Breathalyzers, hair microscopy, burn pattern analysis, bitemark analysis technology, and more have all been proven to be unreliable.[20] And yet police continue to use unreliable technologies and courts continue

---

[18] *See* Garbage In, Gospel Out at 2, *supra* n. 2.

[19] *See* National Research Council, *Strengthening Forensic Science in the United States: A Path Forward* (Nat. Academies Press 2009), http://www.nap.edu/catalog/12589; *see* President's Council of Advisors on Science and Technology, *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods,* Exec. Office of the President (Sept. 2016), *available at* https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[20] *See* Stacy Cowley & Jessica Silver-Greenberg, "These Machines Can Put You in Jail. Don't Trust Them.," N.Y. Times (Nov. 3, 2019), https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html (breathalyzers); Rene Ebersole, "How the Junk Science of Hair Analysis Keeps People Behind Bars," Mother Jones (Dec. 15, 2023), https://www.motherjones.com/politics/2023/12/how-the-junk-science-of-hair-analysis-keeps-people-behind-bars/#:~:text=A%20new%20report%20by%20the,hundreds%20of%20millions%20of%20dollars; Microscopic Hair Comparison Analysis Review Project: A Milestone in the Quest for Forensic Science, NACDL, available at https://www.nacdl.org/Article/May2015-TheMicroscopicHairComparisonAn; Ed Pilkington, "A Bite Mark, a Forensic Dentist, a Murder: How Junk Science Ruins Innocent Lives (Apr. 28, 2022),

to admit unreliable evidence.[21] It is much harder to unring the bell on the use of these technologies than it is to exercise caution in the first instance. This is an opportunity to learn from past mistakes. Before sanctioning widespread use of under-tested and certifiably unreliable technologies, policymakers should consider the harms that a premature deployment of these tools will do to both individuals and the criminal legal system. In an interview with NACDL, a defense attorney described those harms:

> The problem we see, even [if] we can achieve best case scenario — a case dismissed or maybe plead to minor misdemeanor — even if we can get this result, the damage of the accusation itself can never be undone . . . Being arrested is a trauma [my clients] have to live with for the rest of their lives. And sometimes people lose their kids, who are put into the foster system while they are incarcerated. They lose their jobs, or their homes. This happens a lot. Every kind of algorithmic scheme is going to sound objective to someone making a release decision, but to the person affected, it's personal.

The concerns relayed in this comment are far broader than just the technologies that are under consideration in EO 14074. There is a long history of introducing novel technologies into policing without first completing even the most basic foundational validation studies, impact assessments, or educating judges, prosecutors, and defense attorneys. A defense attorney expanded on this idea:

> We're seeing a similar pattern with every new technology that's being rolled out. There will be years of denying it exists, then denying [police] have it, and then only after many cases where we ask and ask and ask, playing this game where we try to get them to disclose, do we finally discover they have it. It's a bad horror movie that we live through over and over again . . . I can't tell you how many cases it's impacting. But I can tell you it's been going on in [my jurisdiction] for the 12–15 years I've been pushing these issues. And every time we think we get one across the finish line there are two or three more technologies that are coming down the pipeline. The idea that the problem is with one specific technology is not the whole picture. The problem is the pattern where law enforcement

---

https://www.theguardian.com/us-news/2022/apr/28/forensics-bite-mark-junk-science-charles-mccrory-chris-fabricant (bitemark evidence);

[21] "'Junk' Forensic Science Lands Thousands of Innocents in Prison, Crime Report (Apr. 28, 2022), https://thecrimereport.org/2022/04/28/junk-forensic-science-lands-thousands-of-innocents-in-prison/.

> continues to use these invasive technologies without making anyone aware of it; then prosecutors play along to keep this info from the defense, which ultimately then keeps it from public domain. Because if we're not raising the issue, outside of a handful of incredible investigative reporters, there's no other avenue for this information to become known by the public.

While the fact that these policing technologies are inaccurate is troubling, it is even more concerning that inaccuracies fall along racial and gender lines. FRT, for example, has divergent error rates when disaggregated across demographic categories, with many algorithms producing significantly higher error for minority subjects.[22] Communities that are already overpoliced, over-incarcerated, and subject to discriminatory policing tactics, are further harmed and disadvantaged by the deployment of technologies that quietly embed a long history of discriminatory policing into novel—and seemingly "neutral"—techniques.[23] That the outputs of these algorithmic tools tend to further burden minority communities is no accident. FRT algorithms were historically trained on databases consisting primarily of white male subjects and are limited in their ability to distinguish between people of color.[24] Predictive

[22] *See, e.g.,* Alex Najibi, "Racial Discrimination in Face Recognition Technology, Science in the News, Harvard University (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.
[23] *See* The Origins of Modern Day Policing, NAACP, https://naacp.org/find-resources/history-explained/origins-modern-day-policing.
[24] Thaddeus Johnson & Natasha Johnson, "Police Facial Recognition Technology Can't Tell Black People Apart," Scientific American (May 18, 2023), https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/.

phenotyping is predicated on a foundation of suspect and discriminatory racial classifications.[25] And "predictive policing" algorithms are trained on historical data that entrenches existing biases.[26]

Defense lawyers witness and grapple with the racist implications of these technologies as they do their best to represent their clients. One lawyer said:

> The technologies themselves may be racially neutral but when you're programming it with data that's being collected from a society where racism is a problem and has been for hundreds of years, you can't expect racial component to peel itself out. By filtering criminal justice through the technology, it's supposed to 'cleanse' the racial and discriminatory components when all it does is magnify them . . . I can see the direct impact this has on the clients. Communities of color are being disproportionately overpoliced in every facet . . . [police are] using data [that] law enforcement agencies are generating themselves, and of course when you dedicate more resources to policing a particular community, shock: you'll find more crimes.

Because these novel policing technologies—which are often unreliable and inaccurate even in controlled research settings—are built on a foundation of faulty and biased input data, their use in communities that are already traumatized and mistreated by discriminatory policing practices threatens to

[25] Filipa Queirós, The Visibilities and Invisibilities of Race Entangled With Forensic DNA Phenotyping Technology, J. of Forensic and Legal Medicine 68, available at https://www.sciencedirect.com/science/article/pii/S1752928X19300873.

[26] Garbage In, Gospel Out at 8–9, *supra* n. 2; *see also* Will Heaven, "Predictive Policing Is Still Racist—Whatever Data It Uses," MIT Technology Review (Feb. 5, 2021), https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/; 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/; Renata O'Donnell, Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause, 94 NYU L. Rev. 544 (2019), available at https://www.nyulawreview.org/wp-content/uploads/2019/06/NYULawReview-94-3-ODonnell.pdf; Aaron Sankin et al., "Crime Prediction Software Promised to be Free of Biases. New Data Shows It Perpetuates Them," Markup (Dec. 2, 2021), https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

violate citizens' constitutional equal protection rights,[27] exacerbate existing inequities in the criminal legal system, and further undermine the credibility and integrity of law enforcement.

2. The Secretive Nature of Policing Technologies Undermines Access, Transparency, and Fairness in the Criminal Legal System.

"The times I got access to source code it was pure luck, not skill, not law. It should not be that we only get this information in a few out of a hundred or thousands of cases. It shouldn't just come down to luck. A process of Googling and luck is not a good way to protect innocent people from going to prison."

All the policing technologies discussed in this comment rely on proprietary algorithms.[28] Some of them rely on black box algorithms.[29] The opacity of these tools—generated by corporate secrecy and sometimes by the incomprehensibility of the technology itself, and endorsed by the government—creates practical and constitutional barriers for the criminally accused and their lawyers.[30] Furthermore, government secrecy about if, when, and how these tools are deployed deepens mistrust in surveilled communities and creates insurmountable challenges for defense attorneys who cannot even know what information to request from prosecutors.

---

[27] O'Donnell, Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause, *supra* n. 26.
[28] *See, e.g.,* Gabrielle M. Haddad, Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom, 23 Vanderbilt J. of Entertainment & Tech. L. 4 (2021); Jennifer Lynch, "Forensic Genetic Genealogy Searches: What Defense Attorneys & Policy Makers Need to Know, Electronic Frontier Foundation (July 26, 2023), https://www.eff.org/wp/forensic-genetic-genealogy-searches-what-defense-attorneys-need-know; Lauren Kirchner, "Powerful DNA Software Used in Hundreds of Criminal Cases Faces New Scrutiny," Markup (March 9, 2021), https://themarkup.org/news/2021/03/09/powerful-dna-software-used-in-hundreds-of-criminal-cases-faces-new-scrutiny; Garbage In, Gospel Out at 9, *supra* n. 2.
[29] *See* Katherine Kwong, The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence 31 Harvard J. L. & Tech. 1 (2017), available at https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech275.pdf. In the case of black box algorithms, which are not the primary focus of this section, there is no amount of disclosure that mitigates the constitutional concerns associated with the technology because there is no way to understand how it works or why it produces the outputs it does.
[30] Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343 (2018).

Any successful constitutional challenge requires that defense attorneys understand which surveillance tools are in use and how they work.[31] It is increasingly challenging for defense attorneys—as well as prosecutors and judges— to perform their responsibilities competently given the sheer quantity and complexity of technology-driven criminal investigations. And even when there is widespread knowledge about government use of a given forensic policing tool, defense attorneys need access to information about governing protocols and competency standards for police. After all, the reliability of many of these tools depends heavily on how they are used. Across the country, police departments use novel surveillance technologies without notifying the communities in which they operate or the defense lawyers responsible for advocating on behalf of criminal defendants.[32]

NACDL's survey results indicated that 45% of respondents were unaware of law enforcement use of FRT in their jurisdictions. When NACDL investigated those jurisdictions to evaluate whether law enforcement was indeed using FRT, it found that at least 22% of the defense attorneys who were unaware of FRT use in their jurisdictions were, in fact, working in jurisdictions with FRT policing programs. This means that almost a quarter of lawyers are unaware that their clients may have been identified by a deeply flawed and unreliable policing tool. The statistic is even higher for probabilistic genotyping. Across all tools, under 30% of respondents said that information about law enforcement use of a given policing technology was publicly available.

[31] *See, e.g.,* "When Google Searches For You: Challenging Geofence Warrants," NACDL (Dec. 3, 2021), https://www.nacdl.org/Content/When-Google-Searches-for-You-Challenging-Geofence; ALPR Primer, NACDL, https://www.nacdl.org/getattachment/49944c94-b295-475e-b575-36bda695286f/2016-4-28_alpr-primer_final.pdf.
[32] *See* Jonathan Manes, Secrecy & Evasion in Police Surveillance Technology, 34 Berkeley Tech. L. J. 503 (2019).

The absence of comprehensive disclosure about the use of these tools violates defendants' constitutional due process rights.[33] In criminal cases, the cards are already stacked against criminal defendants. This asymmetry is magnified tenfold when the prosecution introduces evidence that the defense cannot examine, evaluate, and challenge. The technology might be unreliable or have been misapplied, but without knowing whether it was used in the first place or how it works, it is impossible to put forth a robust challenge. One defense attorney described the paradoxical implications of insufficient disclosure by prosecutors and police, saying, "It's the failure to disclose, but it's also a lack of any kind of objective study of these methods. Because what functionally happens on the ground is we argue that these things shouldn't come in [to court] because they're not appropriate under local evidentiary standards. But it's this Catch-22 because it's impossible to show this to the court when you don't have any supporting documentation or error rates or anything because they're often not doing [studies] or if they [are], they're not disclosing them."

Under the Confrontation Clause, defendants have a right to confront evidence introduced against them, a right that is bypassed completely when the government offloads its policing work to private third parties and refuses to facilitate the disclosure of information about the tool and its application in a given case.[34] One defense lawyer said, "I can't begin to imagine how many people's lives have been impacted by the tech, where they're taking plea deals instead of waiting and waiting. This lack of transparency is

---

[33] *See* Julie Pattison-Gordon, "Justice-Focused Algorithms Need to Show Their Work, Experts Say," Government Technology (May 12, 2022), https://www.govtech.com/computing/justice-focused-algorithms-need-to-show-their-work-experts-say; Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, *supra* n. 30.

[34] *See* Emma Lux, Facing the Future: Facial Recognition Technology Under the Confrontation Clause, 57 Am. Crim. L. Rev. Online 20 (2020), available at https://www.law.georgetown.edu/american-criminal-law-review/aclr-online/volume-57/facing-the-future-facial-recognition-technology-under-the-confrontation-clause/.

causing exponentially more work on the defense community and it's impossible to know the extent to which this is impacts people rights, from making informed decisions about their cases to being able to challenge the new technology." The burden of these discovery battles falls squarely on the shoulders of criminal defendants whose choices often include either sitting in jail while the fight for information inches along or taking an unfair and coercive plea deal.

The complexity, unreliability and secrecy underpinning these technologies is a dangerous and potent brew. The systemic scarcity of information about these technologies means that defense attorneys often do not or cannot challenge its use in court. In a survey response, one lawyer reported that "most attorneys in my area are completely unfamiliar with [face recognition] and do not litigate it, but rather accept the findings." This is especially troubling considering the serious reliability and accuracy concerns described above.[35] And even attorneys who wish to learn about these technologies and how to challenge them in court may have trouble doing so. One lawyer reported that their "attorney continuing education classes do not include seminars regarding the use of technology in our cases."

The opacity of these policing technologies is a major barrier to thorough, fair, and constitutional criminal legal proceedings. At the very least, government and private actors should be required to disclose the use of these technologies, the way they were made, and the way they work. Without access to this essential information, it is undeniable that their widespread deployment is highly prejudicial and unconstitutional.

[35] *See also* Elizabeth Joh & Thomas Joo, The Harms of Police Surveillance Technology Monopolies, 99 Denv. L. Rev. Forum 1 (2022) (outlining harms of secretive police surveillance programs, particularly insofar as this secrecy enables police to cede critical policing decisions to private companies).

B. Recommendations

"The takeaway is to slow down until everyone understands what it is and how to use it and what the limitations are."

Because these policing technologies are so problematic for the reasons described above, NACDL calls on DOJ and DHS to: 1) carefully consider whether federal law enforcement agencies should use these technologies at all; 2) condition federal funding on strict and expansive validation and disclosure requirements; and 3) increase requirements on companies providing the technology to open their systems to external validation and review by the criminal legal system.[36]

Taking into account evidence of the unreliability, bias, and inscrutability of these technologies, DOJ and DHS should conclude that outright bans on FRT, probabilistic genotyping, forensic genetic genealogy, predictive phenotyping, and predictive policing technologies are justified.[37] In the absence of such a ban on any or all of the technologies at issue in EO 14074, NACDL recommends implementing the following protocols:

- **Prohibit the use of any tool that has a demonstrated racial bias.** Human bias in policing is well-documented. Automating that bias, or contracting it away, does not eradicate it. Police should not be allowed to use any tool that has a demonstrated racial bias – either that is a function of the tool itself or a result of how it is deployed.

- **Implement strict data retention policies**. Police should be required to dispose of personal information not at issue in an ongoing proceeding within a restricted period of time. Information about advanced technologies and their use relevant to an ongoing proceeding must be retained in a manner that facilitates appropriate disclosures to the defense. Law

[36] Conditioning federal funding on these types of requirements is not novel. For example, DHS has conditioned funding for fusion centers, units designed to promote information sharing between various intelligence agencies, on adherence to a variety of protocols, including validation studies and competence requirements. *See* Fusion Center Performance Program, Dep't of Homeland Sec. (2023), available at https://www.dhs.gov/homeland-security-grant-program-hsgp.

[37] *See, e.g.,* Resolution on Facial Recognition Technology, NACDL (Oct. 23, 2023), https://www.nacdl.org/Content/NACDL-Facial-Recognition-Resolution,-4AC-Draft.

enforcement agencies should not be permitted to contract with third-parties who do not follow their own strict data retention policies.

 Require rigorous third-party validation of policing technologies. Law enforcement agencies should not be permitted to use a tool that has not been established as reliable—not only in controlled testing environments—but also in the real-life contexts in which they are deployed.[38]

 Require mandatory disclosure of the use of policing technologies – in general and in individual criminal cases. Law enforcement agencies should be required to disclose to the general public in their jurisdictions what surveillance technologies they are using. If those technologies are operated by third-party companies, the public has a right to know which companies are involved. Prosecutors must also disclose the use of these policing tools in each individual case so that defense attorneys can challenge that evidence in court.

 Prohibit government contracts with companies that assert trade secrets. The primary barrier for defense attorneys attempting to understand and challenge policing technologies is the obfuscation of what those technologies are and how they work. In addition to disclosure requirements, governmental agencies should be barred from contracting with companies that shield that information from the defense using trade secrets law. This is what protective orders are for.

 Require comprehensive training and education about these tools. If these tools are deployed, then police, prosecutors, judges, and defense attorneys alike need to understand what they are and how they work. Any federal funding for these tools should be conditioned on expansive education programs for anyone within the criminal legal system that might encounter these tools.

CONCLUSION

NACDL urges DOJ and DHS to resist the siren song of novel policing technologies. Police use of these tools will undermine the goals of decarceration and racial justice, erode the constitutional rights of the accused in criminal cases, and further degrade the privacy interests of the general population. For these reasons, NACDL respectfully asks DOJ and DHS to recommend against the deployment of these

[38] Federal Rule of Evidence 702 requires that there be foundational validity for a given methodology. Without such validation, evidence should not be introduced against a defendant.

technologies. In the absence of an outright rejection of these tools, DOJ and DHS should advocate for the adoption of strict oversight protocols, foundational validity requirements, rejection of technologies with a demonstrated racial bias, required disclosures, and comprehensive training and education for all actors within the criminal legal system.

If you have any questions or concerns, please contact:

Jumana Musa
Director, Fourth Amendment Center
National Association of Criminal Defense Lawyers
202.465.7658
jmusa@nacdl.org

Respectfully submitted,

National Assocation of Criminal Defense Lawyers