May 28, 2024

Re: Data-Driven Policing Technologies at Issue in Executive Order 14110 Section 7.1(b)

The National Association of Criminal Defense Lawyers' (NACDL) top line recommendation on data-driven policing tools is that police departments must not utilize data-driven policing technologies because they are ineffective; lack scientific validity; create, replicate and exacerbate "self-perpetuating cycles of bias"; hyper-criminalize individuals, families, and communities of color; and divert resources and funds from communities that should be allocated towards social services and community-led public safetSy initiatives.

While NACDL does not believe these technologies should be used, it is clear that these technologies are being considered or have been implemented in cities and towns across the country. The recommendations in the attached letter are harm mitigation tactics to lessen the negative impact of this technology.

NACDL calls on DOJ 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. These restrictions are not novel; many other countries have instituted much stricter regulations on data-driven policing technologies, including designating certain AI systems as "high risk." This designation imposes particularly strict regulations on AI systems used in consequential contexts, including "law enforcement that may interfere with… fundamental rights." The European Union is ahead of the United States in assessing the risks of data-driven policing and crafting responsive regulations. NACDL urges DOJ to reference these regulations in formulating its recommendations on data-driven policing technologies.

If you have any questions or concerns, please contact:

Jumana Musa
Director, Fourth Amendment Center
National Association of Criminal Defense Lawyers
1660 L St. NW #12, Washington, DC 20036
202.465.7658
jmusa@nacdl.org

May 28, 2024

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

Re: Data-Driven Policing Technologies at Issue in Executive Order 14110 Section 7.1(b)

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. The use of untested, unregulated, and secretive data-driven 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]

[1] In preparing comments previously submitted to DOJ and DHS on EO 14074, NACDL conducted a survey of its members: defense attorneys across the country. Based on survey responses, NACDL conducted several follow-up interviews. Both the survey and the interviews were administered on the condition of anonymity to protect the privacy of individual attorneys. NACDL cites survey results and interview quotes in these comments.

NACDL's Fourth Amendment Center specifically works with defense attorneys on the legal issues that arise from data-driven policing technology use in their cases.[2] As in all its work, NACDL's guiding objective in submitting this comment is to address racial disparities and mass incarceration that are inherent in the criminal legal system.

COMMENT

Per the Department of Justice (DOJ) request for input and NACDL's relevant expertise, these comments focus on data-driven policing technologies.[3] While these comments refer to both "predictive" and "data-driven" policing technologies, NACDL advocates for 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.[4] Data-driven policing technologies create serious harms for individual criminal defendants, their lawyers, and the criminal legal system more broadly, not to mention historically over-policed communities. These technologies represent a radical change in policing power, enabling police to comb through data and criminalize individuals in ways that were not previously possible. This change not only exacerbates existing racial disparities within the criminal legal system and contributes to mass incarceration, but also renders policing less reliable and more opaque, adding unique due process concerns to an already flawed system.

[2] See, e.g., 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-11162021.pdf (Sept. 2021).

[3] DOJ staff indicated in meetings with civil society that it was breaking the report-writing requirement from Executive Order (EO) 14074 down into multiple, technology-focused reports, with the report on predictive, or data-driven, policing being combined with its response to § 7.1(b) of EO 14110.

[4] *See* Garbage In, Gospel Out, *supra* n. 1.

The federal government has acknowledged both the serious injustices and the astronomical costs generated by our system of mass incarceration.[5] Further, it has enacted legislation and passed executive orders designed to facilitate decarceration and address injustice within the criminal legal system.[6] Before diving into a focused evaluation of data-driven policing technologies, it is worth asking whether the use of these technologies facilitates the goals of reducing incarceration and racial disparities. As it contemplates the various consequences of deploying data-driven policing technologies, NACDL urges DOJ to implement unbiased, effective, and foundationally validated solutions. NACDL encourages DOJ to consider that many of the problems in the criminal legal system are better addressed by non-technological policy changes. DOJ should also consider not only how the tech tools work but how they might accelerate and exacerbate, rather than redress, mass incarceration and racial disparities.[7]

In this comment, NACDL aims to highlight the serious dangers that data-driven policing technologies pose and propose recommendations for mitigating those dangers. First, it defines data-driven policing for the purpose of establishing exactly which technologies are at issue and how they function. Then, it outlines the constitutional and practical barriers that these policing technologies create for criminal defendants and their lawyers due to their unreliability and opacity. Finally, it proposes recommendations. NACDL does not believe these unproven tools have a place in policing, but with the understanding that law enforcement agencies across the

[5] 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/.

[6] *Id.*

[7] *See, e.g.,* 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://communityresourcehub.org/wp-content/uploads/2021/04/acre-21stcenturypolicing-r3.pdf.

country continue to employ them NACDL advocates mitigation measures including the adoption of strict 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, DOJ should caution against the reflexive deployment of novel and untested data-driven policing technologies absent serious consideration of the ways in which they replicate and amplify systemic inequities while undermining the function and purpose of the criminal legal system.

A. What Is Data-Driven Policing?

Data-driven policing encompasses the many surveillance technologies, tools, and methods employed by law enforcement to anticipate and prevent crime. At its core, predictive algorithms in policing programs are the "data-driven incarnation" of what criminologists have been attempting to achieve for decades: to analyze past events, infer broader patterns, and to then use those insights to "prevent" future crime.[8] According to a report published by the RAND Corporation, predictive methods in policing can generally be divided into four broad categories: (1) methods for predicting crimes, or approaches used to forecast places and times with an increased risk of crime; (2) methods for predicting offenders, or approaches that identify individuals at risk of offending in the future; (3) methods for predicting perpetrators' identities by creating profiles that accurately match likely offenders with specific past crimes; and (4) methods for predicting victims of crimes by identifying groups, or in some cases, individuals who are most likely to become victims of crime.[9]

[8] Lindsey Barrett, Reasonably Suspicious Algorithms: Predictive Policing at the United States Border, 41 N.Y.U. Rev. of L. & Soc'y 327, 334 (2018).
[9] Walter L. Perry et al., Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND Corporation (2013).

To implement these methods, data-driven policing employs a variety of algorithms. Since the developers of data-driven policing technologies often assert trade secret evidentiary privileges to deny public access to the inner workings of their technologies, the types of machine learning used in such programs are relatively unknown. Related, because many of these tools built on these algorithms are relatively new, or are continuing to change alongside advancements in technology, all are "are relatively untested, with only a handful of studies, reports, or empirical validation across jurisdictions."[10] Once predictions are made, "there is, generally, no standard for how police should use the predictions,"[11] meaning the technology gives an objective façade to highly subjective policing tactics.

Place-based data-driven policing programs are built upon the premise that crime is not evenly dispersed geographically, and that certain places are expected to experience higher rates of crime over a certain period of time. Like "hot spot policing," or the identification of geographically bound spaces associated with a proportionally greater number of criminal incidents or heightened victimization risk, place-based crime forecasting visualizes the spatial and temporal distribution of crime to purportedly "predict" areas with future criminal activity. The use of data-driven algorithms in place-based crime forecasting produces harmful, self-perpetuating feedback loops of crime predictions, in which officers would repeatedly patrol neighborhoods that had been disproportionately targeted by law enforcement in the past and were thus overrepresented in the historical crime data used to train and build predictive crime algorithms.[12]

[10] Andrew Guthrie Ferguson, Predictive Policing Theory, 24 Cambridge Handbook of Policing in the U.S. 492 (ed. Tamara Rice Lave & Eric J. Miller) (2019).
[11] Upturn, Stuck in a Pattern (2016), https://www.upturn.org/reports/2016/stuck-in-a-pattern/.
[12] *See* Rashida Richardson, Jason Schultz, and Kate Crawford, Dirty Data, Bad Prediction: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. 15, 40–41 (2019); *see also* Garbage In, Gospel Out *supra* n.1.

Police departments also rely on person-based data-driven policing programs to predict who is most likely to commit crimes, in addition to who is likely to become the victim of a crime. The algorithms behind these programs are designed to interrogate massive troves of data gathered in myriad ways, with inputs ranging from police-generated crime reports to publicly available social media posts. The outputs are then used to make critical decisions about patrols, or life-altering designations about who is subject to suspicion, surveillance, and intervention by law enforcement. These programs are enabled by law-enforcement databases and have been shown to lead to the increased monitoring and arrests of predominantly young Black and Brown men.

Among these databases are gang databases, which are localized within cities or similar jurisdictions, and encompass a broad swath of identifying data on individuals known, suspected, believed, or assumed to be gang members, associated with gang members, or affiliated with gang members. BIPOC people comprise the vast majority of individuals listed on these databases, with Black men being the most overrepresented group.[13] Individuals can be certified as gang members simply based on their appearance or location, or even their likes, comments, and connections on social media, often without being notified of their inclusion in such a database or given the opportunity to challenge that designation. In addition to being over-inclusive, hyper-racialized, and non-transparent, NACDL found that these databases are riddled with errors, and have even included young children and infants.[14]

Though data-driven policing programs are purportedly designed to lower citywide violence levels and are marketed as intervention opportunities for the benefit of communities,

[13] *See* Andy Ratto, Nina Loshkajian, Eleni Manis, Guilt by Association: How Police Databases Punish Black and Latinx Youth, Surveillance Technology Oversight Project (Sept. 5, 2023), https://www.stopspying.org/guilt-by-association.

[14] *See* Garbage In, Gospel Out, *supra* n.1.

empirical research studies have repeatedly found that such tools function to expand policing and criminalization of Black and Brown communities.[15] Some programs have resulted in heightened risk of arrest, in addition to enhanced federal and state sentencing options, for designated individuals swept into their broad net. For example, individuals included in gang databases are subject to increased police surveillance and monitoring and can also face enhanced criminal charges upon arrest.

Person-based data-driven policing programs have historically been shrouded in secrecy. Police departments frequently use social media monitoring tools and techniques to surveil individuals and then combine that information with historical crime data to categorize people as members of a “gang” or “crew,” drawing conclusions about their “future dangerousness” without their knowledge. In this manner, police layer information gleaned from social media on top of historical crime data—of both individuals and their friends and family—to make assumptions about their propensity to engage in criminal activity. This involves sifting through vast amounts of data in a very short period of time to draw conclusions that are both deeply flawed and biased. Data obtained through social media posts and text messages are increasingly being used to not only populate gang databases, but as primary evidence in criminal investigations, with no effective means of oversight to limit the extent of surveillance.

It is worth noting that while policymakers often attempt to distinguish between person- and place-based data-driven policing, that distinction is largely artificial. All “predictive policing” technologies are dangerous for similar reasons: they rely on biased—and often racist—input data, they deploy unreliable analytical techniques, and they attempt to legitimize the

[15] *See* City of Chicago Office of Inspector General, Advisory Concerning the Chicago Plice Department’s Predictive Risk Models (Jan. 2020), available at https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf.

impossible endeavor of divining where crime will occur and who will commit it before it even happens.

B. Data-Driven Policing Technologies Create Constitutional and Practical Barriers for Criminal Defendants and Their Lawyers.

NACDL has unique insight into the experience of the criminal defense bar, and by extension the people that defense attorneys represent.[16] These comments explain how the deployment of data-driven policing technologies might affect those communities. It is appropriate to consider the defense perspective when evaluating the impact and value of data-driven policing for two reasons. First, criminal defense lawyers have an intimate understanding of how data-driven policing technologies 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.[17] 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 experiences of criminal defense lawyers and their clients, as well as available research and its own expertise on data-driven policing technologies, to draw the conclusions it presents below.

1. Data-driven policing technologies are unreliable.

"[They are] unreliable and will lead to false arrests and convictions."[18]

Data-driven policing technologies have documented reliability and accuracy problems.[19] The widespread deployment of unreliable and inaccurate policing technologies is dangerous for

[16] Throughout these comments, NACDL pulls quotes from a 2024 survey it conducted of defense attorneys across the country on their experience of advanced policing technologies in their work.

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

[18] Survey response from a Maryland public defender, Nov. 21, 2023. Notes on file with author.

[19] *See, e.g.*, Aaron Sankin & Surya Mattu, "Predictive Policing Software Terrible at Predicting Crimes," Wired (Oct. 2, 2023), https://www.wired.com/story/plainfield-geolitica-crime-predictions/; Sarah Brayne, Alex Rosenblat, and Danah Boyd, "Predictive Policing," (October 27, 2015), available at https://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf.

obvious reasons. If police rely on complex, opaque data-driven techniques that 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 law enforcement's stated mission of solving crime, the credibility and fairness of the criminal legal system in the eyes of the public, and the constitutional rights of people accused in criminal cases.

Data-driven policing tools have some of the worst reliability statistics of any forensic policing technology, with some tools accurately predicting crimes less than one percent of the time.[20] Not only are these tools wildly unreliable, but they are commensurately biased. 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."[21]

Law enforcement has repeatedly made the mistake of deploying untested forensic technologies that turn out to be junk science, a crisis that has been explored in depth by federal bodies.[22] Breathalyzers, hair microscopy, burn pattern analysis, bitemark analysis technology,

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

[21] Interview with a public defender in New York, Jan. 1, 2024, notes on file with author.

[22] 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
.

and more have all been proven to be unreliable.[23] And yet police continue to use unreliable technologies and courts continue to admit unreliable evidence.[24]

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 pled 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.[25]

These harms disproportionately burden people of color because predictive algorithms are trained on historical data that entrenches existing biases.[26]

[23] 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/; 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), https://www.theguardian.com/us-news/2022/apr/28/forensics-bite-mark-junk-science-charles-mccrory-chrisfabricant (bitemark evidence).

[24] "'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/; *see also* Georgia Gee, "Internal Emails Reveal How a Controversial Gun-Detection AI System Found Its Way to NYC, WIRED (May 13, 2024), https://www.wired.com/story/evolv-gun-detection-nyc-subways-emails/ (documenting NYC's deployment of Evolv systems that have a reported 85% false positive rate and appears to flag three-ring binders, umbrellas, and other innocuous, everyday items as potential weapons).

[25] Interview with a defense attorney in Wisconsin, Jan. 4, 2024. Notes on file with author.

[26] Garbage In, Gospel Out at 8–9, *supra* n. 1; 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-

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 the 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.[27]

Because data-driven policing technologies 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 violate citizens' constitutional equal protection rights,[28] 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."[29]

Data-driven policing tools rely on proprietary algorithms.[30] The opacity of these tools—generated by corporate secrecy and sometimes by the incomprehensibility of the technology

crimepredpol/; 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.

[27] Interview with a public defender in Minnesota, Jan. 4, 2024. Notes on file with author.

[28] O'Donnell, Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause, *supra* n. 25.

[29] Interview with a public defender in Virginia, Jan. 2, 2024. Notes on file with author.

[30] *See* Garbage In, Gospel Out at 9, *supra* n. 1.

itself—creates practical and constitutional barriers for the criminally accused and their lawyers.[31] 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. One defense attorney reflected:

> "[The technology] is often the most difficult thing in a case for people to understand, both defense attorneys and their clients. We get a single line in a police report or somewhere else, and it's my job to explain to people what the evidence is or what it means, and in many case we won't know—no one knows, not other attorneys, not even our experts, other than a broad guess. We can't explain to our clients, let alone challenge the evidence, if we don't know what that evidence is."[32]

Any successful constitutional challenge requires that defense attorneys understand which tools are in use and how they work.[33] 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 data-driven 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 their clients.[34] Despite these challenges, it is worth noting that defense lawyers are constitutionally mandated to provide effective assistance under the Sixth Amendment. And in

[31] Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343 (2018).

[32] Interview with a public defender in Virginia, Jan. 2, 2024. Notes on file with author.

[33] 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.

[34] *See* Jonathan Manes, Secrecy & Evasion in Police Surveillance Technology, 34 Berkeley Tech. L. J. 503 (2019).

cases involving data-driven policing, effective assistance may involve navigating these significant roadblocks to challenge the reliability of data-driven evidence, whether under *Frye/Daubert* or Rule 702.[35]

Because law enforcement outsources its data-driven policing work to private companies who shield themselves from discovery by citing trade secrets law, the government often evades substantive disclosure during the discovery process.[36] In outsourcing its policing work, the government not only neglects its responsibility to be accountable for performing and auditing its own stated mission, but it also creates an asymmetry of information in criminal cases. Furthermore, these harms are compounded by the fact that data-driven policing tools are often used in concert with other unreliable and opaque policing technologies—like facial recognition technology, probabilistic genotyping, forensic genetic genealogy, and more—which serves only to further consolidate secret decision-making power and to entrench surveillance tech companies as powerful monopolists.

The absence of comprehensive disclosure about the use of these tools violates defendants' constitutional due process rights.[37] In criminal cases, the cards are already stacked against criminal defendants. Secretive policing tools exacerbate existing inequities within the criminal legal system. It is well-established that pretrial risk assessment tools are biased and require strict oversight if they are to be used at all.[38] Because the accused are so often coerced into accepting a

[35] *See Frye v. United States*, 293 F.1013 (1923); *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993); Fed. R. Evid. 702.

[36] *See generally* Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, *supra* n. 30.

[37] *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-theirwork-experts-say; Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, *supra* n. 30.

[38] *See* Lyle Moran, "Pretrial Risk-Assessment Tools Should Only Be Used If They're Transparent and Unbiased, Warns ABA House," ABA Journal (Feb. 14, 2022), https://www.abajournal.com/news/article/resolution-700#google_vignette.

plea deal, they are limited in their ability to challenge the use of data-driven policing tools.[39] 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."[40]

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.[41] 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 causing exponentially more work on the defense community and it's impossible to know the extent to which this impacts people's rights, from

[39] The Trial Penalty: The Sixth Amendment Right to Trial on the Verge of Extinction and How to Save It, NACDL Trial Penalty Recommendation Task Force (2018), available at https://www.nacdl.org/getattachment/95b7f0f5-90df-4f9f-9115-520b3f58036a/the-trial-penalty-the-sixth-amendment-right-to-trial-on-the-verge-of-extinction-and-how-to-save-it.pdf.

[40] Interview with a defense attorney in Wisconsin, Jan. 4, 2024. Notes on file with author.

[41] *See* Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System at 1376, *supra* n. 30.

making informed decisions about their cases to being able to challenge the new technology."[42] 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 paucity of information about data-driven policing tools available to defense lawyers and their clients is reflected in the public sphere as well. As it is currently leveraged, the federal grant-making process risks contributing to the opacity and lack of accountability surrounding advanced policing technology in the United States. Rather than a police department seeking funds from a state or local elected body holding the power of the purse, and at least in theory beholden to the taxpaying public, private companies often now pitch federal grant research and drafting support as part of what they offer.[43] In other words, a private company may locate available federal funds and then help draft the proposal needed for a department to acquire their product, bypassing any oversight and accountability afforded by the jurisdiction's budgeting process. Companies at times assist in drafting sole source procurement justifications as well, allowing an agency to avoid transparency and fiscal accountability benefits of competitive bidding.[44]

[42] Interview with public defender in Minnesota, Jan. 4, 2024. Notes on file with author.

[43] *See, e.g.* Police Grants 101, on PoliceGrantsHelp.com (featured sponsors advertising free grant research, alert notices, and application reviews from sponsored companies for the acquisition of license plate readers, body cameras, and more.) A recent series of marketing emails from Motorola Solutions, for example, stated: "$1.8B in grant funding is currently available as part of the FY24 FEMA Preparedness Grant Programs. Do you need help with your application" and "To help support your FY24 grant application, we've partnered with the grant experts at Lexipol to provide free grant reviews so that your organization can put your best application forward … Which Motorola Solutions product(s) are you looking for grant funding to help purchase?" Emails from Motorola Solutions regarding "Reminder: Request free grant assistance" and "Thank you for your interest in Grant Assistance!" (May 1 and 13, 2024), on file with author.

[44] *See, e.g.,* Email from Taser (now Axon) to "United States state, local and municipal law enforcement agencies" regarding "Sole Source Letter for TASER International, Inc.'s Conducted Electrical Weapons," (June 11, 2015), on file with author.

This process also means that law enforcement agencies are not just outsourcing policing work to private companies, but also the decision in the first instance to acquire advanced equipment and technology. It is a supply-driven market; a company can promote a product and find the funds to ensure its seamless acquisition without any legislative or public input or evaluation of an actual, demonstrated problem that the technology purports to solve.

The complexity, unreliability and secrecy underpinning data-driven policing 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. This is especially troubling considering the serious reliability and accuracy concerns described above.[45] 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 undermines constitutional rights.

[45] *See* 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).

C. Recommendations

"The takeaway is to slow down until everyone understands what it is and how to use it and what the limitations are."[46]

NACDL's top line recommendation on data-driven policing tools based on years of research by its Task Force on Predictive Policing is that police departments must not utilize data-driven policing technologies because they are ineffective; lack scientific validity; create, replicate and exacerbate "self-perpetuating cycles of bias"; hyper-criminalize individuals, families, and communities of color; and divert resources and funds from communities that should be allocated towards social services and community-led public safety initiatives.

While NACDL does not believe these technologies should be used, it is clear that these technologies are being considered or have been implemented in cities and towns across the country. The following recommendations are harm mitigation tactics to lessen the negative impact of this technology.

NACDL calls on DOJ 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.[47] These restrictions are not novel; many other countries have instituted much stricter regulations on data-driven policing technologies, including designating certain AI systems as "high risk."[48] This designation imposes particularly strict regulations on AI systems used in

[46] Interview with public defender in Maryland, Jan. 3, 2024. Notes on file with author.

[47] 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-grantprogram-hsgp.

[48] *See* EU Artificial Intelligence Act, Art. 5: Prohibited Artificial Intelligence Practices, available at https://artificialintelligenceact.eu/article/5/.

consequential contexts, including "law enforcement that may interfere with… fundamental rights."[49] The European Union is ahead of the United States in assessing the risks of data-driven policing and crafting responsive regulations. NACDL urges DOJ to reference these regulations in formulating its recommendations on data-driven policing technologies.

Taking into account evidence of the unreliability, bias, and inscrutability of these technologies, DOJ should conclude that an outright ban on data-driven policing technologies is justified. In the absence of such a ban on data-driven policing technologies, 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 as a function of the tool itself or as a result of how it is deployed.

- **Implement strict data retention policies.** Police departments should be required to promulgate and adhere to strict data retention policies that maximize protection of sensitive information against breaches and misuse. 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. Young people between the ages of 18 and 25 should be provided notice of their presence on any databases that law enforcement departments access and utilize, including gang-databases, strategic subject lists, and other data collected through social media monitoring. Individuals must be provided the opportunity, through a private attorney or, if they cannot afford an attorney, an appointed attorney, to challenge their inclusion in and seek removal from such databases. They should also be allowed to challenge their inclusion in the underlying data and law enforcement's interpretation of that data that feeds the creation of predictive policing systems. Any data, records, or other information contained in any law enforcement database through any data-driven policing technology and/or social media monitoring should be sealed and purged when the individual reaches 25 years of age. Law 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.[50]** 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

[49] *Id.*

[50] 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.

they are deployed.[51] Those validation studies must be independent and must be accessible by the defense.

- **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 data-driven policing 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. Protective orders can help facilitate this necessary disclosure.

- **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 exhorts DOJ to resist the siren song of data-driven 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 to recommend against the deployment of these technologies. In the absence of an outright rejection of these tools, DOJ 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.

[51] *See* Abraham Meltzer, When an Algorithm Violates the Law: Deconstructing a Study Supposedly Showing that an Artificial Intelligence Algorithm Makes Better Bail Decisions than Do Judges, 38 Syracuse J. Sci & Tech. L. 3 (2023); Elizabeth Joh, Ethical AI in American Policing, Notre Dame J. on Emerging Tech. (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4096953.

If you have any questions or concerns, please contact:

Jumana Musa
Director, Fourth Amendment Center
National Association of Criminal Defense Lawyers
1660 L St. NW #12
Washington, DC 20036
202.465.7658
jmusa@nacdl.org

Respectfully submitted,

National Association of Criminal Defense Lawyers