House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

Hearing:
Artificial Intelligence and Criminal Exploitation: A New Era of Risk

Date of Testimony:
July 16, 2025

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

Chairman Biggs, ranking member McBath, members of the Subcommittee: Thank you for inviting me to testify on the topic of law enforcement use of artificial intelligence.

In my remarks today, I would like to make two main points:

- ***First***, although AI has shown real promise in enhancing public safety, we still know far too little about which tools actually work, which do not, and what is needed to use them effectively. A lack of research and evaluation of these issues is hampering efforts by policymakers and law enforcement to assess whether and how best to devote resources to these tools. Police officials regularly describe the swarm of vendors that approach them and the difficulty they encounter trying to determine what works well and what does not.
- ***Second***, the use of AI in policing can pose serious risks to civil rights and civil liberties — including the potential for significant erosions of privacy due to the vast quantities of data about individuals that AI systems can collect and analyze. These risks may well take on constitutional proportions — some recent judicial decisions suggest that certain uses of AI could have potential Fourth Amendment implications. Although much is yet unsettled, it is eminently possible that certain tools might be declared unconstitutional years after they are used, imperiling countless

convictions. This underscores the need for regulation, both to protect individual rights and provide legal certainty to those in law enforcement.

By way of background, I am the Jacob D. Fuchsberg Professor of Law and Affiliated Professor of Politics at New York University School of Law. For over thirty years I have taught a number of courses relevant to this hearing, including Constitutional Law, Criminal Procedure, and Democratic Policing. I am the author of numerous publications about policing, in both the scholarly and public realms, including my book, *Unwarranted: Policing Without Permission*, which argues in favor of sensible regulation of policing practices on the front end to avoid problems on the back end. It is my longstanding view that sound public safety calls for sensible regulation; the goal is to make sure policing and public safety are effective, equitable, and democratically accountable.

Perhaps most germane, I also am the Faculty Director of the Policing Project at New York University School of Law, a nonprofit, nonpartisan organization dedicated to promoting public safety through transparency, equity, and democratic accountability. We conduct research, but also do work on the ground all over the country, to promote effective, democratically-accountable public safety. Ours is an all-stakeholders approach. Everywhere we work, we welcome to the table all stakeholders who will come in good faith to create safe communities. We regularly work with both communities facing serious issues with crime, and with policing agencies. Our approach is reflected in our Advisory Board, which surely is unique in including public officials, activists, policing leaders, and civil liberties and racial justice advocates, among others. By listening to, and working with, all stakeholders, we hope to move the needle toward greater public safety that is just, non-discriminatory, and effective. If you are interested in the full scope of our work, you can learn more at our website, www.policingproject.org.

One of our primary areas of study and work — and one of my principal areas of research — is the use of artificial intelligence and data analytics by law enforcement. AI is driving a profound transformation in policing and public safety. New AI-enabled tools promise an abundance of novel capabilities — to predict where crime will occur, to identify unknown suspects, to track individuals' movements, and so forth.[1] Some of these tools, such as face

[1] *See How Policing Agencies Use AI*, POLICING PROJECT, https://www.policingproject.org/ai-explained-articles/2024/9/6/how-policing-agencies-use-ai (last visited July 3, 2025).

recognition technology and vehicle surveillance systems, have become commonplace.[2] Others are just emerging — from robots that can conduct patrols and alert police to suspicious activity, to systems that can generate police reports based on body-worn camera data.[3]

Based on our extensive study of these tools and engagement with law enforcement, advocates, and industry, we wish to make two key points in our testimony.

First, although AI has shown real promise in enhancing public safety, we still know far too little about *which* tools actually work, which do not, and what is needed to use them effectively. The "which" and the "how" are related. Like any tool, AI can make life better, or be ineffective and perhaps cause harm. Often the harm can be ameliorated, and the tool's use optimized, through guidance on proper use.

Undoubtedly, AI shows tremendous promise. In recent years, agencies have begun using AI to detect online child grooming and identify child sexual abuse material, leading to the rescue of victims and the arrest of offenders.[4] Sophisticated algorithms can analyze vast quantities of data to detect financial crimes — the U.S. Treasury Department recovered $1 billion in fraudulent funds in 2024 alone through the use of such tools.[5] AI-enabled forensic techniques

---

[2] *See, e.g.*, Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short,* N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html; Danielle Abril, *Drones, Robots, License Plate Readers: Police Grapple with Community Concerns as They Turn to Tech for Their Jobs,* WASH. POST (Mar. 9, 2022), https://www.washingtonpost.com/technology/2022/03/09/police-technologies-future-of-work-drones-ai-robots.

[3] *See, e.g.*, Jeffrey Mays, *400-Pound N.Y.P.D. Robot Gets Tryout in Times Square Subway Station*, N.Y. TIMES (Sept. 22, 2023), https://www.nytimes.com/2023/09/22/nyregion/police-robot-times-square-nyc.html; Barbara Booth, *Police Departments Across U.S. Are Starting to Use Artificial Intelligence to Write Crime Reports*, CNBC (Nov. 26, 2024), https://www.cnbc.com/2024/11/26/police-departments-are-using-ai-to-write-crime-reports.html.

[4] *See, e.g.*, Shira Ovide, *Scanning Technology is Coming to Detect Child Porn. Here's What it Means,* WASH. POST (June 24, 2025), https://www.washingtonpost.com/technology/2025/06/24/child-sex-abuse-crime-fighting-technology; Olivia Solon, *Microsoft Launches Tool to Identify Child Sexual Predators in Online Chat Rooms*, NBC NEWS (Jan. 9, 2020), https://www.nbcnews.com/tech/tech-news/microsoft-launches-tool-identify-child-sexual-predators-online-chat-rooms-n1112881.

[5] *See* Matt Egan, *AI Helped the Feds Catch $1 Billion of Fraud in One Year. And it's Just Getting Started*, CNN (Oct. 17, 2024), https://www.cnn.com/2024/10/17/business/ai-fraud-treasury; Matt Egan, *AI is Uncle Sam's New Secret Weapon to Fight Fraud*, CNN (Feb. 28, 2024),

have played a critical role in solving cold cases — such as the case of Joseph James DeAngelo, also known as the "Golden State Killer," who was identified through use of AI-enabled DNA analysis tools.[6] Anyone truly concerned for safety — from community safety to national security — should support sound uses such as these.

At the same time, there remains a troubling lack of clarity about which technologies work and which do not. Many of the law enforcement leaders we speak to express confusion about the flood of new AI tools entering the market: do these systems actually deter crime and improve case closure rates overall? If so, by how much — are they worth the substantial investment in time, money, and training? Are their benefits limited to certain types of crimes or certain contexts? The absence of evidence-backed guidance makes it extraordinarily difficult for agencies and policymakers to make informed decisions about how to keep their communities safe.[7]

There is a clear solution to this problem: Congress should help fund rigorous, independent research to evaluate the real-world capabilities of AI tools used in public safety. Again, the goal is not only to figure out what works and what does not, what is potentially risky and what not, but also if there are simple regulations that can maximize the promise of these tools while minimizing or eliminating the harms.[8] This federal investment would help fill critical knowledge gaps, support evidence-based decision-making by law enforcement agencies, and ensure that new tools are adopted only when they demonstrably

---

https://www.cnn.com/2024/02/28/business/artificial-intelligence-fraud-treasury-ai/index.html.

[6] *See* Tebah Browne & Barry Scheck, *Regulating Forensic Investigative Genetic Genealogy: The Case for Judicial Oversight and the Bipartisan Model Legislation Passed in Maryland,* A.B.A. (June 11, 2024), https://www.americanbar.org/groups/judicial/resources/judges-journal/2024-spring/regulating-forensic-investigative-genetic-genealogy.

[7] *See* Barry Friedman et al., *Policing Police Tech: A Soft Law Solution,* 37 BERKELEY TECH. L.J. 701, 710-11 (2022) (noting the lack of empirical study of surveillance technologies); Chris Slobogin & Sarah Brayne, *Surveillance Technologies and Constitutional Law,* 6 ANN. REV. CRIMINOLOGY 218, 220–21 (2023) (same).

[8] For example, there is a crucial absence of evidence-backed guidance regarding how long surveillance data should be retained, and whether shorter data retention periods would compromise investigations. *See* AXON AI & POLICING TECHNOLOGY ETHICS BOARD, AUTOMATED LICENSE PLATE READERS 34 (2019), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf (discussing this issue in the context of license plate readers).

serve the public good. By prioritizing effectiveness alongside innovation, Congress can help ensure that AI in policing lives up to its promise.

In addition, unless and until Congress itself is prepared to legislate, it should allow, and indeed encourage, state experimentation regarding the regulation of AI-enabled policing and public safety tools. The states have been called "laboratories of democracy" for a reason — as they take different approaches, we have the opportunity to discern which might make sense at the national level. And although there is an active debate regarding whether states should regulate certain aspects of the AI ecosystem such as the foundation models upon which AI tools are built, there is no sound reason to prevent states from regulating their own public safety agencies' use of AI, or tools that are specially built for those agencies. Policing and public safety are, of course, constitutional responsibilities of state and local government. Different regulatory approaches might stimulate experimentation and innovation, and provide an opportunity to learn.

Second, the need for learning and regulation is particularly crucial given the serious risks to civil rights and civil liberties that some of these systems pose.[9] Errors in AI systems such as face recognition technology have led to individuals being wrongfully arrested and charged with serious crimes.[10] Similar errors with license plate readers have led to entirely blameless individuals being held at gunpoint by officers who were alerted improperly due to system errors.[11] There are multiple instances in which officers have misused AI systems for personal purposes, such as surveilling romantic interests.[12] The use of these powerful

[9] *See generally Understanding AI Risk,* POLICING PROJECT, https://www.policingproject.org/ai-explained-articles/ai-explained/understanding-ai-risk.

[10] *See* Douglas MacMillan et al., *Arrested by AI: Police Ignore Standards After Facial Recognition Matches,* WASH. POST (Jan. 13, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition; Douglas MacMillan et al., *Police Seldom Disclose Use of Facial Recognition Despite False Arrests,* WASH. POST (Oct. 6, 2024), https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest.

[11] *See* Livia Albeck-Ripka, *City in Colorado Pays $1.9 Million to Black Family Wrongfully Detained by Police*, N.Y. TIMES (Feb. 5, 2024), https://www.nytimes.com/2024/02/05/us/aurora-family-police-settlement.html.

[12] *See* David Maass & Cooper Quintin, *New ALPR Vulnerabilities Prove Mass Surveillance is a Public Safety Threat;* ELEC. FRONTIER FOUND. (June 18, 2024), https://www.eff.org/deeplinks/2024/06/new-alpr-vulnerabilities-prove-mass-surveillance-public-safety-threat.

tools in investigations rarely is disclosed to criminal defendants, raising concerns about wrongful convictions.[13] When tools are used without transparency or adequate guardrails in place, there sometimes is backlash when the word gets out.[14] We are seeing that today around the use of license plate readers.[15] All of this can erode public trust in the tools as well as the agencies that deploy them.[16]

The advent of AI has led to one particularly alarming privacy risk, which is that today vast amounts of data are being collected — and often sold to policing agencies — about each and every one of us, without regard to whether we are suspected at all of any wrongdoing.[17] That data includes where we go, whom we see, what we purchase, and so on. Certain data brokers claim to have thousands of points of data about each of us.[18] Collecting this much data indiscriminately would have far less value without the ability of AI to analyze it. But with AI, we all become suspects.

The notion that the government might collect — and potentially retain indefinitely — intimate details about the lives of all its citizens has few, if any, historical precedents in a democratic society. And as I write elsewhere, one thing

---

[13] *See, e.g.*, MacMillan, *Police Seldom Disclose Use of Facial Recognition Despite False Arrests, supra* note 10.

[14] *See, e.g.*, Mihir Zaveri, *N.Y.P.D. Robot Dog's Run Is Cut Short After Fierce Backlash,* N.Y. TIMES (Apr. 28, 2021), https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html.

[15] *See, e.g.,* Elizabeth Evans & Angela Shen, *Austin's Automatic License Plate Reader Program Will End June 30*, FOX7 AUSTIN (June 3, 2025), https://www.fox7austin.com/news/austin-city-manager-removes-item-automatic-license-plate-readers.

[16] *See* Anthony Rodriguez, *Balancing Innovation with Responsibility,* IACP: POLICE CHIEF ONLINE (Apr. 9, 2025), https://www.policechiefmagazine.org/balancing-innovation-responsibility-ai-outreach. (noting that a "lack of transparency can undermine public trust and impede accountability when things go wrong").

[17] *See, e.g.,* Joseph Cox, *How an ICE Contractor Tracks Phones Around the World*, VICE (Dec. 3, 2020), https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps; Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html; Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data. *See generally Advance Notice of Proposed Rulemaking Regarding Commercial Surveillance Hearing Before the F.T.C.* (2022) (statement of Barry Friedman, Jacob D. Fuchsberg Professor of Law, N.Y.U. School of Law).

[18] *See* Steve Kroft, *The Data Brokers: Selling Your Personal Information,* CBS NEWS (Mar. 9, 2014), https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information.

we can be certain of is that the Framers of the U.S. Constitution and the Fourth Amendment loathed such indiscriminate government intrusions.[19] So-called "Writs of Assistance" — a form of General Warrants — were a motivating cause of the colonies declaring Independence.[20] The world has changed since 1791, of course — but to allow the use of such tools without appropriate oversight to limit agency and officer discretion is in tension — if not outright conflict — with long-settled understandings of the Fourth Amendment.

In fact, absent democratic oversight, some of these tools and practices ultimately may be found to violate the Constitution. These are early days and courts are only beginning to grapple with the complex issues raised by the use of AI in policing. But in at least a few recent cases involving the use of AI-enabled investigative tools, courts have signaled that such use may have Fourth Amendment implications.[21] This proposition gains support from a related set of precedents outside of the AI context, in which courts have found certain data collection practices overbroad (i.e., the collection was insufficiently "particular" in the words of the Fourth Amendment) or overly intrusive on the privacy of innocent third parties.[22] As I have argued elsewhere, the constitutionality of such

---

[19] *See* Barry Friedman, *The Constitutionality of Indiscriminate Data Surveillance*, U. PA. L. REV. (forthcoming, on file with author) (manuscript at 55–57).

[20] *See id.* at 31–32; Carpenter v. United States, 585 U.S. 296, 303 (2018) (James Otis's 1761 speech condemning writs of assistance was the first act of opposition to the arbitrary claims of Great Britain and helped spark the Revolution itself.)

[21] *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 339–40 (4th Cir. 2021) (en banc) (aerial surveillance program capturing the outdoor movements of all individuals within a large region of Baltimore violated the Fourth Amendment); Virginia v. Bell, No. CR230001500-00; 01; 02 (Va. Cir. Ct. May 10, 2024) (holding that "collection and storage of license plate and location information" through license plate readers "constitutes a search within the meaning of the Fourth Amendment"). *See generally* Schmidt v. City of Norfolk, No. 2:24CV621, 2025 WL 410080 at *7–9 (E.D. Va. Feb. 5, 2025) (holding that plaintiffs plausibly alleged that a city's license plate reader program intruded upon a reasonable expectation of privacy and was unconstitutional); Commonwealth v. McCarthy, 142 N.E.3d 1095, 1109 (Mass. 2020) (sufficiently pervasive deployment of ALPRs may implicate the Fourth Amendment, but finding that the ALPR program being challenged in the case had not reached that level). Each of these cases relies upon *Carpenter v. United States*, a case in which the Supreme Court held that it was unconstitutional for the government to obtain a large quantity of cell phone location data without a warrant — data which, in the Court's words, "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *See* Carpenter v. United States, 585 U.S. 296, 311 (2018) (cleaned up).

[22] *See In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 7 (D.D.C. 2013) (imposing minimization requirements where the government's "overly broad" warrant application included seizure of data regarding third parties unrelated to the case); *In re* Application of the U.S. for an Ord. Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL

data collection may ultimately hinge on whether it is constrained by clear, democratically enacted rules that prevent the unjustified or arbitrary use of the data.[23] That is, after all, the core purpose of the Fourth Amendment: to guard against the kind of unchecked, suspicionless searches that the Framers considered among the gravest abuses of government power.[24]

For this reason, the absence of regulation creates significant legal uncertainty for law enforcement. If the unregulated use of AI tools ultimately is found unconstitutional, it could jeopardize years of convictions in cases in which such tools were used. The result may be a wave of legal challenges, placing immense strain on prosecutors, defense attorneys, and the courts alike.

These problems demand legislative attention. Lawmakers should require that agencies establish clear guardrails to ensure the responsible use of AI. At a minimum, agencies should be required to adopt formal use policies and disclose the tools they deploy to the public and to criminal defendants. In an article I have coming out in the University of Pennsylvania Law Review I describe other essential requirements, including data retention rules, and predicates for querying data that has been collected indiscriminately.[25] Congress can impose these requirements directly on federal law enforcement agencies; given its power under the Commerce Clause, it may well be able to do the same for state and local agencies, but at a minimum, Congress should consider making federal grants for the purchase of AI tools contingent on the adoption of such measures.[26] To support this effort, we have developed a model statute requiring such disclosure and accompanying guidance on agency use policies, which we encourage the Committee to review.

Artificial intelligence is at an inflection point. AI has the potential to transform public safety in highly desirable ways — but only if its use is backed by evidence

---

6871289, at *1, *4 (N.D. Ill. Nov. 9, 2015) (imposing minimization requirements where the government's proposed data collection would capture "an inordinate number of innocent third parties' information"); United States v. Pilling, 721 F. Supp. 3d 1113, 1128 (D. Idaho 2024) (warrant which authorized search of "vast swaths of data" in defendant's iCloud account without "particularly identify[ing] the things to be seized" violated the Fourth Amendment).

[23] *See* Friedman, *supra* note 19, at 44–47.

[24] *See id*; Barry Friedman & Cynthia Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 287, 310 (2016).

[25] *See* Friedman, *supra* note 19, at 44-47.

[26] *See* Barry Friedman, Rachel Harmon, & Farhang Heydari, *The Federal Government's Role in Local Policing,* 109 VA. L. REV. 1527, 1583 (2023).

and used in a manner that protects individual liberties and core constitutional values. Several states already have taken action to promote the responsible deployment of AI by public agencies.[27] Congress, too, has a vital role to play in ensuring this comes to pass. By investing in research and incentivizing agencies to adopt formal policies and disclose their AI use, lawmakers can help ensure that AI enhances — not undermines — public safety and public trust.

[27] *See, e.g.*, H.B. 1688, 169th Leg., Gen. Court (N.H. 2024) (enacted) (prohibiting state agencies from using AI to manipulate, discriminate, or surveil members of the public); S.B. 818, Reg. Sess. (Md. 2024) (enacted) (requiring the adoption of certain policies and procedures concerning the development, procurement, deployment, use, and assessment of AI systems by state government agencies); H.B. 149, 89th Leg., Reg. Sess. (Tex. 2025) (enacted) (establishing certain disclosure requirements on the use of AI by government agencies).