STATEMENT OF

Kia Hamadanchy

Senior Policy Counsel

National Political Advocacy Division

American Civil Liberties Union

For a Hearing on

"A Continued Pattern of Government Surveillance of U.S. Citizens"

Before the

United House of Representatives

House Judiciary Committee

Subcommittee on Crime and Federal Government Surveillance

April 8, 2025

Chairman Biggs, Ranking Member McBath, and members of the Subcommittee. Thank you for the opportunity to testify today on behalf of the American Civil Liberties Union (ACLU) regarding the myriad of government surveillance programs that impact Americans of all backgrounds. At the start of my testimony, I want to express the optimism and hope of the ACLU that this Subcommittee and this Congress can use the next twelve months to put into federal statute not only long-overdue protections against misuse of foreign surveillance authorities, but also protections for everyone across our country from the increasingly pervasive and largely unaccountable surveillance state. We commit to working with you towards these reforms.

Under the Fourth Amendment, we all have the right to be free from unreasonable searches and seizures by the government. Yet in recent decades, we have seen a massive expansion of the government's surveillance apparatus in ways that threaten those rights, fueled by emerging technologies and often operating with limited oversight or transparency. Using, and sometimes misusing, authorities like Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, along with the government's purchase of massive quantities of data from commercial data brokers, the federal government has access to vast amounts of personal information and communications, often without warrants or the kinds of robust safeguards needed to protect individual privacy and constitutional rights. Both Democratic and Republican administrations have abused these authorities and overstepped constitutional limitations. Recent advances in artificial intelligence threaten to accelerate both the scope and invasiveness of many of these surveillance programs.

I. Section 702 of the Foreign Intelligence Surveillance Act

A little over a year from now, on April 20, 2026, Section 702 of the FISA is scheduled to expire. While Section 702 requires that surveillance must be "targeted" at foreigners overseas, large quantities of the communications that Americans exchange with people abroad are also swept up and stored for future investigations. The result is that the government collects Americans' international phone calls, text messages, emails, and other digital communications, all without a warrant. And to this day, despite repeated bipartisan requests from Congress, intelligence officials have refused to provide basic transparency about the number of U.S. persons whose communications are collected under the program.

The FBI, NSA, and CIA then conducts searches of their Section 702 databases for the communications of Americans—without having to demonstrate probable cause, as the Fourth Amendment would otherwise require. The FBI conducted more than 57,000 of these warrantless searches, through what is known as the "backdoor search" loophole, in 2023 alone. A recent report from the Privacy and Civil Liberties Oversight Board (PCLOB) found very little justification as to the value for the close to 5 million U.S. person queries conducted by the FBI from 2019 to 2022.[1] The reality is that Section 702 has been abused under presidents from both political parties, and it has been used to unlawfully query the communications of individuals and groups across the political spectrum.

[1] Privacy & Civ. Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2023), (here).

Last year, Congress reauthorized Section 702 with the Reforming Intelligence and Securing America Act (RISAA) for two years. The ACLU opposed this legislation because it did not close the backdoor search loophole and because its major changes were to codify internal FBI procedures that had already been shown to be insufficient. The central change introduced was a restriction on searches conducted solely to uncover evidence of criminal wrongdoing. This requirement does not apply to queries intended, even in part, to gather foreign intelligence. As a result, of the 57,094 warrantless searches the FBI performed in 2023, only 17 would have been affected by this change. Notably, some of the most serious misuses of Section 702, such as surveillance of Black Lives Matter protestors, tens of thousands of political campaign donors, and even sitting members of Congress, involved a purported foreign intelligence purpose.

While the most recent Joint Assessments from Department of Justice (DOJ) and Office of the Director of National Intelligence (ODNI) included several new examples of improper queries, including the chief of staff to a member of Congress, those assessments predate the most recent reauthorization. Important questions this subcommittee should be asking regarding the changes in RISAA include:

- How many "sensitive" queries, such as those using terms associated with elected officials, politicians, media organizations and figures, and religious organizations and figures, has the FBI conducted since reauthorization? How many "batch job" queries has the FBI conducted since reauthorization?
- Has the government sought any new Section 702 certifications post-reauthorization? If so, how has that affected the scope of collection in terms of the number of collected communications or the number of Section 702 targets?
- What kinds of compliance issues have arisen since reauthorization?

And while we await further reporting from the intelligence community on the impact of RISAA, there are several developments since reauthorization I would like to note.

a. **Unconstitutional Queries**

In December, the District Court for the Eastern District of New York ruled in a criminal case, *United States v. Hasbajrami*, that the warrantless searches the FBI conducted under Section 702 violated the Fourth Amendment.[2] This decision stemmed from a 2019 Second Circuit Court of Appeals ruling, which held that querying U.S. persons' data collected under Section 702 triggers separate Fourth Amendment scrutiny.[3] This ruling is the first of its kind and one of the rare cases where criminal defendants have received notice of Section 702 surveillance.

Congress should be asking the FBI whether it has changed any policies or practices in response to the court's reasoning or conclusions addressing the warrant requirement. The FBI may respond that the opinion addressed only queries that occurred in 2011, but that does not change that the court's reasoning about the warrant requirement for queries and limited scope of the

[2] United States v. *Hasbajrami*, No. 11-cr-00623-LDH, slip op. (E.D.N.Y. Jan. 21, 2025).
[3] *United States v. Hasbajrami*, No. 15-2684, slip op. (2d Cir. Dec. 18, 2019).

foreign intelligence exception to that requirement. In particular, the court focused on the fact that there were no exigent circumstances to justify the warrantless queries at issue. Today, many of the FBI's Section 702 queries for Americans' communications do not involve exigent circumstances, and for these searches, *Hasbajrami*'s reasoning would require the FBI to get a warrant.

b. Failure to Provide Notice of Section 702 Surveillance

There are also continuing signs that the government is failing to provide notice of Section 702 surveillance in criminal prosecutions.[4] The latest example is related to disclosures by the FBI beginning in February 2024—first in a Politico article and later in a public speech by FBI Director Christopher Wray— ahead of the reauthorization vote.[5] The Politico article cited FBI officials who described three newly declassified examples that purported to demonstrate the value of backdoor searches of Americans under Section 702.

And then in April in a speech before the American Bar Association, then FBI Director Christopher Wray further discussed one of these examples involving the use of Section 702 backdoor searches to allegedly thwart a planned attack on critical infrastructure. Although FBI officials publicly touted this example as proof that warrantless queries are essential, neither the Politico article nor Director Wray identified the specific case at issue. And no criminal defendant appears to have received notice of the surveillance, despite statutory and constitutional requirements that entitle individuals to notice when the government relies on evidence obtained or derived from Section 702.

Given the details presented in the Politico article and Director Wray's speech, only one criminal prosecution appeared to fit FBI officials' description, based on the ACLU's review of federal criminal dockets around the country. The defendant in that case subsequently filed a motion to compel the government to provide notice of use of Section 702.[6] After reviewing secret government submissions, the judge ruled that no notice was required because he was satisfied that the government would not use evidence gathered pursuant to Section 702.[7]

It is unclear how the judge reached that conclusion. But one possibility is that the FBI officials overstated the value of the backdoor 702 searches in the investigation. That would be consistent with PCLOB's finding that these searches have very little justification as to the value of these searches. Another possibility is that the government may have engaged in the practice of parallel construction, which it has used to evade notice requirements by recreating evidence initially

---

[4] For an overview of the long-running Section 702 notice problems, see: Sarah Taitz & Patrick C. Toomey, Concealing Surveillance: The Government's Disappearing Section 702 Notices, Just Security (Sept. 27, 2023), (here).

[5] John Sakellariadis, FBI Reveals Controversial Spy Tool Foiled Terror Plot as Congress Debates Overhaul, Politico (Feb. 13, 2024), (here).

[6] Gaby Del Valle, ACLU Challenges Section 702 Surveillance in Neo-Nazi's Prosecution, The Verge (June 27, 2024), (here).

[7] Dylan Segelbaum, *Judge Satisfied Evidence from Spy Tool Won't Be Used Against Neo-Nazi in Alleged Power Grid Plot*, Balt. Banner (Aug. 9, 2024), (here).

obtained through controversial surveillance techniques using alternative means.[8] Regardless, the government's failure to provide notice of this Section 702 surveillance—in *any* prosecution—even as the FBI publicly promoted its use of Section 702 queries warrants additional oversight from Congress.

Indeed, based on the ACLU's review of public court dockets, DOJ does not appear to have provided any Section 702 notices whatsoever since 2018.[9] This subcommittee should closely scrutinize why that is the case, and whether parallel construction is being used to evade this important protection.

c. **Transparency and Oversight**

Additionally, DOJ and FBI committed to various changes as a condition of reauthorization, which included increased transparency, audits, and higher-level approvals for certain queries. Given the many changes at both agencies, and the fact that numerous officials have been reassigned from key oversight roles, Congress must closely examine whether the assurances given are actually being followed through on.

This is compounded by the firings of the pro-reform board members of PCLOB, badly undermining independent oversight of Section 702. This comes even though these board members had previously demonstrated their independence from the Biden Administration in issuing their 2023 report, which called upon the government to seek individualized judicial approval before searching Section 702 data for the private communications of Americans. As Congress considers reauthorization of Section 702, it should also consider strengthening the oversight capability of the PCLOB. Senator Ron Wyden and now Director of National Intelligence Tulsi Gabbard have previously introduced such legislation that would serve as a good starting point.

Section 702 is of particular importance to this Subcommittee because it is an issue that Congress has no choice but to address over the course of the next year. And maybe just as importantly, the reauthorization is coming at a time when there is bipartisan leadership in Congress—and on this Subcommittee—for true reform. But Section 702 is not the only form of government surveillance that raises concerns, and I would like to briefly touch on a few related topics.

II. Commercial data purchases by law enforcement and intelligence agencies

In recent years, we have seen the ever-growing practice of law enforcement and intelligence agencies circumventing constitutional protections by purchasing access to data that they would

[8] As confirmed by the PCLOB's 2023 report.

[9] When Congress passed Section 702 in 2008, it explicitly mandated that defendants in criminal cases be notified when evidence used against them came from this program. The Constitution also requires this type of notice. However, from 2008 to 2013, DOJ failed to uphold this obligation. It did so by quietly adopting an overly restrictive interpretation of the phrase "derived from" Section 702 surveillance—so restrictive, in fact, that it concluded no defendant was entitled to notice. In response to public scrutiny, DOJ revised its policy and began reviewing past prosecutions to determine which should have included notice of Section 702 surveillance. As a result of this reassessment, between October 2013 and April 2014 six defendants received belated notice. And from 2014 to 2018, five more individuals received similar delayed notice.

otherwise need a warrant to obtain, including location and internet search records. Federal agencies that have purchased such data include the FBI, the Drug Enforcement Administration, Immigration and Customs Enforcement, Customs and Border Protection, the Secret Service, the Department of Homeland Security, and the Department of Defense. *The Wall Street Journal* has also reported that the Internal Revenue Service "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."[10]

According to former deputy director of the CIA Michael Morell, "[t]he information that is available commercially would kind of knock your socks off. If we collected it using traditional intelligence methods, it would be top secret sensitive. And you wouldn't put it in a database, you'd keep it in a safe."[11]

Information vulnerable to purchase by the government in this manner includes:

- Information from individuals' visits to health clinics[12], as well as reproductive tracking applications installed on people's phones;[13] and
- Information regarding people's race, ethnicity, gender, sexual orientation, income, and political and religious affiliations.[14]

More recently, the Office of the Director of National Intelligence released a partially declassified report that details the intelligence community's purchase of commercially available information. The report found that the intelligence community is collecting increasing amounts of commercially available information, but did not know how much it is collecting, what types, or what it was doing with the data. While the Biden Administration issued a new policy framework last year, it does not adequately address the problem as it applies only to the intelligence community and leaves agencies wide latitude to create their own guidelines for gathering and using this data. More critically, it does not prevent agencies from buying information that would otherwise require judicial oversight such as a warrant.

This is allowed to occur because of gaps in the law. Current law prohibits email, social media and internet service providers from disclosing this sensitive data to law enforcement without a court order. However, the Electronic Communications Privacy Act does not address situations in which law enforcement obtains the same data without a court order from data brokers and other entities that do not have a direct relationship with consumers.

In response to a 2023 Inspector General report, DHS stopped purchasing cell phone location data. This is a good step, but it is unclear as to whether the Trump Administration plans on restarting the practice. Moreover, the only way to ensure that protections against federal agencies

---

[10] Byron Tau, IRS Used Cell Phone Location Data to Try to Find Suspects, WALL ST. J. (Jun. 19, 2020) (here).
[11] Byron Tau, U.S. Spy Agencies Know Your Secrets. They Bought Them., Wall St. J. (Mar. 8, 2024), (here).
[12] Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, Vice (May 3, 2022), (here).
[13] Joseph Cox, Data Marketplace Selling Info About Who Uses Period Tracking Apps, Vice (May 17, 2022), (here).
[14] Joseph Cox, How the U.S. Military Buys Location Data from Ordinary Apps, Vice (Nov. 16, 2020), (here).

circumventing the Fourth Amendment by purchasing data across government is through legislation like the Fourth Amendment is Not for Sale Act--which passed the House Judiciary Committee without a single no vote and passed the full House last year. We urge that you take up this legislation and pass it once more as soon as possible.

III. Reverse Warrants

Reverse warrants, such as reverse location (also known as geofence) warrants and reverse keyword warrants, allow law enforcement to secure information that implicates large numbers of people who are not suspected of any wrongdoing. Prosecutors have sought reverse location warrants to sweep up the location data of an unspecified and unlimited number of persons within a defined area during a specific time period without identifying any specific person as to which there is probable cause to believe they have committed or will imminently commit a crime. Similarly, keyword warrants seek to identify every person who searched for a particular word or phrase during a specified time of interest, again without identifying any specific person as to which there is probable cause to believe they have committed or will imminently commit a crime.

These broad, suspicionless, dragnet searches are deeply problematic and are tantamount to the Revolutionary War-era general warrants that lead our nation's Founders to prohibit their use through the adoption of the Fourth Amendment. Accordingly, the Fifth Circuit Court of Appeals recently held, in *U.S. v. Smith*, that reverse location warrants "are modern-day general warrants and are unconstitutional under the Fourth Amendment."[15]

Google, which historically has been one of if not the most frequent recipient of reverse warrants because it collected large quantities of both location data from Android devices and search history from its search engine, reported a sharp increase in law enforcement use of these warrants.[16] Between 2018 and 2020, reverse location warrant requests from federal authorities to Google surged by over 1,100 percent. During the same period, requests from state and local agencies also spiked dramatically, rising by over 800 percent in California, 900 percent in Florida, more than 1,200 percent in Michigan, nearly 1,900 percent in Missouri, and over 5,300 percent in Massachusetts.

Recognizing the dangers, the ACLU has led advocacy and legal efforts to stop the use of reverse warrants. In 2022, our state affiliates in New York and Utah helped push for legislative bans. Those efforts laid the groundwork for a broader campaign launched in 2023, through which we supported bills to ban reverse warrants in additional states including California, Missouri, and

---

[15] United States v. Smith, 110 F.4th 817 (5th Cir. 2024). The Court warned that this technology could enable "near perfect surveillance" and that "the potential intrusiveness of even a snapshot of precise location data should not be understated" given that "location tracking can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences." While the Supreme Court recognized in 2018 in *Carpenter v. United States* that the government needs a warrant to access cell phone location history, in a separate case, a panel of the Fourth Circuit ruled in *United States v. Chatrie*, that this did not apply to a warrant to collect Google location history information. The en banc Fourth Circuit granted rehearing of this case, and a decision from the full court is expected soon

[16] *Supplemental Information on Geofence Warrants in the United States*, Google (2021), (here).

Delaware. At the same time, the ACLU has filed multiple amicus briefs in key court cases arguing that these searches are unconstitutional.

And in response to the threat reverse warrants posed to their customers, Google has changed how Android phones collect and store user location data.[17] Instead of automatically transmitting "Location History" to Google's servers, this data is now only stored locally on a user's device, making it inaccessible to Google by default, similar to Apple's approach with iPhones. As a result, when law enforcement seeks location data through a reverse warrant, Google will no longer be able to provide the information it once could. Because Google is uniquely positioned with access to a large user base, crucial for these types of broad reverse location searches, the inability to obtain data from the company will likely lead to a temporary decline in the use of reverse location warrants until new sources of location data are identified and targeted.

While, notwithstanding the ruling of the Fifth Circuit, the constitutionality of reverse location and keyword warrants will likely need to be decided by the Supreme Court. Until that time, there is no reason why Congress could not protect our civil liberties by instituting a federal ban on the use of such warrants.

IV. Cross Agency Data Linkage

On March 20, 2025, President Trump issued Executive Order 14243, titled "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos." This Executive Order directs federal agencies to facilitate the sharing and consolidation of agency records, with the stated goal of combating waste and fraud. However, the broad and unregulated access to sensitive data not only breaches privacy, but risks the creation of a database that contains a single, searchable profile of every American, without transparency or clear legal limits. And while data consolidation and sharing could potentially improve government operations, it must be done in a way that balances efficiency with robust privacy protection. Otherwise, this could risk the eventual creation of a vast and unaccountable surveillance system capable of tracking every citizen's activities, movements, and associations.

A similar program was proposed by the Department of Defense in the early 2000s. The Terrorist Information Awareness (TIA) program was designed to mine vast amounts of personal data from a variety of sources, including commercial databases, travel records, and financial transactions, in the name of national security. This program was loudly criticized across the political spectrum, and in response to efforts led by Senator Wyden and with the support of Senator Grassley, Congress halted funding for TIA. More than 20 years later, the new threat is from a potentially far more expansive and invasive program.

Building a centralized system for federal data, as envisioned under the Executive Order, creates similar risks, and threatens to create a single point of vulnerability where personal information could be exploited for improper surveillance or wrongful government action. Functionally this data consolidation will enable centralized dossiers on nearly everyone in the United States that would leap over the firewalls around agency data that prevent misuse and abuse.

---

[17] *Updates to Location History and new controls coming soon to Maps*, Google (2023), (here).

Consolidating such data could lead to biometric information gathered by one law enforcement agency, or during air travel, being merged with or easily accessible to other law enforcement agencies, and the reverse could also be true. Records related to firearms, maintained by federal firearms licensees, the FBI, or the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), might be reviewed by other federal entities, potentially to assess eligibility for government programs such as Social Security or Medicare--and the FBI and ATF could similarly access Social Security and Medicare records, including medical files. Likewise, IRS data reflecting contributions to organizations like the ACLU, NAACP, NRA, or the Heritage Foundation could become accessible to law enforcement. While such broad data sharing risks violating well-established privacy safeguards, it is essential for Congress to actively monitor these practices and ensure that these privacy laws are upheld while blocking the creation of a centralized government dossier on nearly every individual in this country.

V. Increased use of Artificial Intelligence in Surveillance

All these surveillance programs run the risk of being supercharged by the rapid growth and use of artificial intelligence (AI) by the federal government. To be clear, national security and law enforcement agencies have long integrated AI into their operations. And while there have been recent efforts to promote greater accountability and fairness in AI across federal agencies, national security has largely been left out of those reforms.

These agencies currently operate with minimal transparency and weak or unenforceable accountability structures. The public remains largely unaware of how agencies like FBI, CIA, and NSA are using AI, due in part to exceptions in existing guidance on federal uses of AI. Even less is known about what, if any, civil liberties safeguards are in place. For instance, the ODNI issued high-level ethical principles for AI use, including pledges to be "transparent and accountable," but little concrete information has been shared publicly.[18]

In contrast, DHS has made important strides in transparency under guidance for federal uses of AI that the Trump Administration has reaffirmed. In December and throughout 2025, DHS released updated and considerably more comprehensive AI use case inventories, but questions remain around AI classified as "national security systems." These agencies are moving rapidly to deploy AI systems, but at the same time civil rights and civil liberties protections are not moving at the same speed.

As an initial matter, this Subcommittee should undertake a comprehensive review of AI technologies used for surveillance under its jurisdiction and assess their impact on privacy and civil liberties. This review should detail the purpose, functionality and existing safeguards like privacy protocols or risk assessments on these systems. And wherever possible, information should be made public, especially regarding unclassified systems.

[18] ODNI, Intelligence Community Principles of Artificial Intelligence (2020) (here); ODNI, Artificial Intelligence Ethics Framework for the Intelligence Community (June 2020) (here).

More than four years ago, the National Security Commission on Artificial Intelligence warned that intelligence agencies were aiming to embed AI at every stage of the intelligence cycle.[19] These systems are now very likely being used to identify surveillance targets, analyze intercepted communications, and manage large volumes of collected data. However, there is still little transparency about the real-world impact of these practices.

The NSA stands out in this context.[20] It has described itself as a leader in integrating AI into intelligence gathering and has acknowledged using these tools for tasks like identifying threats, summarizing large datasets, and processing audio.[21] Yet, there is a lack of information about how AI is used to select surveillance targets or analyze intercepted communications, activities that often involve Americans' data. There are real concerns that AI is being used to automate target selection, and potentially initiating surveillance without adequate human review.[22]

The intelligence community and law enforcement agencies acknowledge the ethical risks posed by AI, but public disclosure and accountability remain limited. This Subcommittee should use its oversight powers to evaluate current AI practices within surveillance programs and recommend halting any uses that endanger constitutional rights.

a. Facial Recognition Technology

One example of such a tool is facial recognition technology. The ACLU has consistently taken the position that the use of face recognition technology poses serious threats to civil liberties and civil rights, making it dangerous both when it fails and when it functions.[23] Accordingly, the ACLU has repeatedly called for a federal moratorium on the use of facial recognition.[24]

---

[19] Nat'l Sec. Comm'n on A.I. (NSCAI), Final Report at 110 (2021) (here).
[20] National Security Agency/Central Security Service, Our Mission (visited July 1, 2024) (here).
[21] Artificial Intelligence: Next Frontier is Cybersecurity, NSA.gov (July 23, 2021) (here); Jay Stanley, Will ChatGPT Revolutionize Surveillance?, ACLU (Apr. 19, 2023) (here); An Interview with Paul M. Nakasone, Joint Force Quarterly, 92 at 4 (Jan. 2019) (here); Justin Doubleday, NSA Working on New AI 'Roadmap' as Intel Agencies Grapple with Recent Advances, Federal News Network (July 14, 2023) (here); Matt Kapko, 3 Areas of Generative AI the NSA Is Watching in Cybersecurity, Cybersecurity Dive (May 1, 2023) (here); Carolyn Shapiro, The Intelligence Community Is Developing New Uses for AI, FedTech (Oct. 4, 2022) (here).
[22] Nat'l Sec. Comm'n on A.I. (NSCAI), Final Report at at 108–10, 143–45. (2021) (here).
[23] ACLU, Re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Executive Order 14074, Section 13(e)), (Jan. 19, 2024) (here). ACLU, Response to U.S. Commission on Civil Rights Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology (April 8, 2024) (here).
[24] More than 20 jurisdictions—including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont—have enacted legislation halting most or all law enforcement or government use of face recognition technology. Others, such as the states of Maine and Montana, have enacted significant restrictions on law enforcement use of the technology. And law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited use of Clearview AI, an FRT vendor that markets a particular privacy destroying system built on a database of tens of billions of non-consensually collected faceprints.

As an initial matter, facial recognition technology is often unreliable and frequently produces possible matches that are incorrect.[25] Even in best case scenarios, these systems are not designed to deliver definitive identifications. Instead, they generate what is essentially an "algorithmic best guess" of who a person might be, which often results in incorrect matches.[26] A variety of factors influence how accurate facial recognition technology is, including how the algorithm was trained, the composition of the image database it is matched against, and characteristics of the input image, such as the lighting, angle, and image quality.[27]

The most troubling issue is that facial recognition technology systems consistently demonstrate disproportionately high error rates when applied to people of color and women, compared to white men.[28] Supporters of law enforcement's use of facial recognition technology often counter concerns about its risks by pointing out that officers are told the technology is only meant to provide investigative leads and must be supplemented by further inquiry to establish probable cause for an arrest. Yet, law enforcement records from around the country show that this guidance is insufficient to prevent serious violations of individual rights. Cases of wrongful arrests linked to facial recognition technology illustrate this problem clearly. In at least five of seven documented incidents, officers were explicitly advised that the technology's results did not amount to a definitive identification or grounds for arrest but still proceeded to detain innocent individuals.

This suggests that officers often treat facial recognition matches as conclusive evidence, disregarding or misunderstanding the limitations of the technology.[29] These issues are further exacerbated by a lack of transparency, especially when it comes to disclosing the use of facial recognition to courts and defendants in criminal proceedings. Just recently, for example, a Cleveland judge had to throw out evidence in a homicide case after police concealed their use of facial recognition technology when applying for a search warrant.[30] And recent pronouncements by the Department of Commerce's National Institute of Standards and Technology (NIST), which claim the accuracy of facial recognition technology has dramatically improved, are based more upon inexplicably broad standards for a successful match than actual technological advancements.

---

[25] Because FRT systems conducting one-to-many searches are generally configured to produce multiple possible matches, even when the algorithm identifies a true match, it will also necessarily generate numerous false matches.

[26] Eyal Press, Does A.I. Lead Police to Ignore Contradictory Evidence?, The New Yorker (Nov. 13, 2023) (here); see also Nat'l Acad. of Sci., Facial Recognition: Current Capabilities, Future Prospects, and Governance at 48–49 (2024) (here).

[27] Nat'l Acad. of Sci., Facial Recognition: Current Capabilities, Future Prospects, and Governance at 47 (2024) (here).

[28] Id. at 24, 56–57.

[29] This may be in part due to automation bias, as well as poor training, perverse incentives to close cases, and other factors. See, e.g., Shira Ovide, A Case for Banning Facial Recognition, N.Y. Times (June 9, 2020), (here).

[30] Lucas Daprile, Cleveland Police Used AI to Justify a Search Warrant. It Has Derailed a Murder Case, Cleveland.com (Jan. 25, 2025), (here).

Despite these significant shortcomings, facial recognition technology used by government agencies is on the rise. Most known deployments involve attempting to match individuals to still images or identifying them in photographs, often in criminal investigations. However, the prospect of continuous video surveillance using facial recognition is becoming more real, especially as federal agencies responsible for national and homeland security increasingly explore and adopt AI-powered facial recognition tools.[31] For example, the FBI employs facial recognition technology in intelligence gathering and national security contexts, including identifying individuals connected to open assessments, preliminary investigations that don't require any suspicion of wrongdoing, as long as they serve a recognized purpose such as preventing crime or terrorism.[32]

And while the ACLU continues to maintain its position calling for a federal moratorium on the use of this technology, I would like to briefly highlight a landmark settlement in the case of Robert Williams, who was wrongfully arrested by Detroit police in 2020 after officers relied on inaccurate facial recognition technology. The settlement sets a new standard by establishing the most robust set of policies and restrictions on law enforcement's use of this technology. These new rules are intended to reduce the risk of false arrests, particularly for people of color and women, who face disproportionately high error rates with facial recognition systems.

Mr. Williams was arrested outside his home in Farmington Hills as his wife and young daughters looked on. He was accused of shoplifting watches from a store in Detroit, but the accusation stemmed from a faulty facial recognition match. His case is one of at least three known instances in which Detroit police wrongly arrested someone based on facial recognition technology.

Highlights of the settlement include:

- A ban on making arrests solely based on the outcome of a facial recognition match or a photo lineup that immediately follows such a match. This is crucial because when facial recognition technology generates a false match, that result often looks similar to the suspect, meaning that a witness viewing a photo lineup is likely to mistakenly think that the computer-generated false-match lookalike is the perpetrator.
- A requirement that lineups cannot be conducted solely based on a facial recognition investigative lead without additional, independent, and credible evidence before being used to justify a suspect's involvement in a crime.

---

[31] See, e.g., ACLU, Comment re: DHS Information Collection Request (Dec. 6, 2021) (here); see also GAO, Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections (GAO-22-106100) (June 29, 2022) (here) (indicating that DOD, DHS, DOJ, and DOS had reported using facial recognition technology for national security and defense related purposes). Section 5708 of the FY2020 National Defense Authorization Act mandated that the Director of National Intelligence submit a report on the use of facial recognition technology. This report has never been made public despite it being required to have been submitted in an unclassified form.

[32] House Oversight and Reform Committee: Facial Recognition Technology - Ensuring Transparency in Government Use (June 4, 2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, FBI) (here); U.S. Senate AI Insight Forum: National Security (Dec. 6, 2023) (statement of Patrick Toomey, Deputy Director, National Security Project, ACLU) (here).

- Mandatory training for officers on the limitations and risks of facial recognition tools, including the technology's tendency to misidentify people of color at higher rates.
- A review of all cases dating back to 2017 where facial recognition was used to obtain arrest warrants.
- Ongoing court oversight for the next four years to ensure compliance with the settlement terms.

The multiple wrongful arrests by police in this case and in other American cities are a demonstration that facial recognition technology poses inherent risks when used by law enforcement. The best way to prevent misuse is through a moratorium on its use, but in places where such laws are not yet in place, Detroit's new standards are an important step forward in reducing wrongful arrests and minimizing the harms associated with this flawed technology.

VI. Conclusion

As you consider these issues, the Committee should remember that whether a tool is convenient for the government does not answer the question as to whether that tool is constitutional. It would of course be easier for law enforcement and national security agencies if they never had to secure a warrant for any search. But the purpose of the Fourth Amendment is not to make the government's job easier or more convenient.

This Committee and this Congress have an unparalleled opportunity, over the next twelve months, to protect all Americans by fundamentally reforming Section 702, starting with imposing a warrant requirement. We look forward to working with you in getting those long-overdue reforms to the President's desk by next April. At the same time, we strongly urge this Committee to also address the massive and growing privacy problems for Americans raised by the broader surveillance ecosystem.