



STATEMENT OF
Kia Hamadanchy
Senior Policy Counsel
National Political Advocacy Division
American Civil Liberties Union

For a Shadow Hearing on
“Tracked and Targeted: The Unconstitutional Surveillance State”

Before the
United States House of Representatives
House Committee on Homeland Security

June 10, 2026

Ranking Member Thompson and members of the Committee, thank you for the opportunity to testify today on behalf of the American Civil Liberties Union (ACLU) regarding the myriad government surveillance programs that impact Americans of all backgrounds.

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.

Department of Homeland Security Expansion of the Surveillance Infrastructure

Within the Department of Homeland Security (DHS), in recent years Immigration and Customs Enforcement (ICE) has built one of the most expansive and invasive surveillance operations in the federal government, fueled in part by the massive increase in immigration enforcement funding provided by budget reconciliation. While many of these tools are not new and their use in some instances predates the current administration, the scale and integration of these surveillance technologies has expanded dramatically in the past year.

Facial Recognition Technology

ICE has deployed a smartphone application called Mobile Fortify that enables ICE agents to perform facial recognition searches against a dataset reportedly containing over 200 million images and to conduct fingerprint scans directly from government-issued mobile devices.¹ The app integrates multiple federal, state, and Department of Homeland Security databases, granting ICE agents access to an expansive suite of personally identifiable information.

Individuals are not given the opportunity to decline or consent and the use of this technology on anyone regardless of immigration status means that both citizens and non-citizens alike are being impacted and subject to being tracked through this biometric surveillance system.

The dangers of this technology are profound. Facial recognition systems have well-documented accuracy problems, particularly in identifying people of color and women, leading to false matches and wrongful detentions. And despite these issues ICE officials have stated that an apparent biometric match by Mobile Fortify is a 'definitive' determination of a person's status and that an ICE officer may ignore evidence of American citizenship, including a birth

¹ Joseph Cox, Inside ICE's Supercharged Facial Recognition App of 200 Million Images, 404 Media (July 17, 2025), <https://www.404media.co/inside-ices-supercharged-facial-recognition-app-of-200-million-images/>.

certificate, when the app says a person is undocumented.² There also appear to be no meaningful limits on how ICE uses this technology or what other agencies it shares results with. All for a program that has never been authorized by Congress and appears to be being deployed without any clear statutory restrictions, usage auditing, or accountability mechanisms.

According to recent reporting, Mobile Fortify has been used more than 200,000 times. And the reach of this surveillance apparatus is now poised to expand dramatically as ICE plans to distribute a related facial recognition app to potentially more than a thousand local law enforcement agencies participating in the 287(g) program.³ This represents a significant expansion of the program and Congress must act before a flawed facial recognition system known to generate false matches and designed to retain biometric data for 15 years is placed in the hands of thousands of local police officers who are neither trained nor equipped to make immigration determinations.

Automated License Plate Readers

The U.S. Border Patrol, which is part of Customs and Border Protection within DHS, has also secretly built a system of automated license plate readers across the nation that carries out dragnet surveillance of millions of Americans' movements. Border Patrol intelligence operatives monitor this data for movements they deem suspicious, though we know little about what they consider suspicious or what kinds of algorithms they are using to do so.

This system uses Border Patrol's own plate readers strung across highways from the southern border to such faraway places as Illinois and Michigan, though we do not know the full extent of their placement. The agency also accesses a similar nationwide network of plate readers run by the DEA and has been authorized to access systems operated by private companies. An important element of this program is the extent to which Border Patrol relies on local officers to assist, such as by carrying out pretext stops based on ALPR data.

DHS operates this extensive network of automated license plate readers not just near the border but far beyond it, creating a dragnet that captures data on millions of Americans who are simply going about their daily lives. Such data can reveal where people worship, seek medical care, attend political meetings, and engage in other constitutionally protected activities.

Mobile Device Surveillance and Spyware

ICE has also invested heavily in acquiring and deploying sophisticated surveillance technologies that can extract complete data from mobile devices and track individuals' locations without warrants or meaningful oversight.⁴ In August 2025, the Trump administration lifted a previous

² Joseph Cox, ICE and CBP Agents Are Scanning Peoples' Faces on the Street To Verify Citizenship, 404 Media (Oct. 29, 2025), <https://www.404media.co/ice-and-cbp-agents-are-scanning-peoples-faces-on-the-street-to-verify-citizenship/>.

³ Joseph Cox, ICE's Plan to Let Cops Around the Country Scan Faces to Verify Immigration Status <https://www.404media.co/ices-plan-to-let-cops-around-the-country-scan-faces-to-verify-immigration-status/>.

⁴ Stephanie Kirchgaessner, Ice Obtains Access to Israeli-Made Spyware that Can Hack Phones and Encrypted

hold on a contract with Paragon Solutions, an Israeli spyware company, allowing ICE to acquire access to software called Graphite that can reportedly be used to hack into any mobile phone, including encrypted applications. More recently, DHS has stated that ICE no longer holds a contract with Paragon Solutions but has declined to clarify whether ICE retains access to Paragon-developed tools through third parties, and ICE's departing acting director acknowledged in an April 2026 letter that he had approved the use of a commercial spyware tool.⁵

These tools allow ICE to access text messages, emails, photos, location history, and other sensitive data from smartphones, track individuals through their mobile devices in real time, map social networks and associations based on digital communications, and monitor applications including encrypted messaging services. Tools used by ICE against one targeted population will very likely migrate to other federal law enforcement agencies, where they could be deployed even more broadly—and there is reason to be concerned that they could be deployed against people who are not engaged in any unlawful conduct, or even people who are exercising their constitutional rights. These tools also leave Americans vulnerable to criminal hacking, by giving the government an incentive to keep vulnerabilities in widely used apps and operating systems secret instead of disclosing them to the companies so they could patch their software to protect their users from harm.

ICE has also deployed cell-site simulators, commonly known as 'Stingrays,' which mimic cell phone towers to force nearby phones to connect to them, allowing ICE to track individuals' locations. According to reports, ICE has used these devices to locate and apprehend immigrants, with the technology capable of sweeping up data from any phone in the vicinity, including those belonging to U.S. citizens who happen to be nearby.⁶

Data Fusion and Integrated Surveillance

Recent reporting has revealed that ICE is working on deploying tools in development by Palantir that integrate data from multiple government sources.⁷ A tool reportedly called ELITE populates maps with potential deportation targets, brings up dossiers on each person, and provides confidence scores on current addresses. The system draws information from sources including the Department of Health and Human Services, U.S. Citizenship and Immigration Services, and commercial investigation databases.

ICE previously signed agreements with Palantir to develop an ImmigrationOS platform, which uses artificial intelligence to identify and track potential targets. These vendor platforms fuse driver's license images, phone extractions, travel and tax records, and commercial face-search

Apps, The Guardian (Sept. 2, 2025), <https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware>.

⁵ Jude Joffe-Block, DHS says ICE has 'no relationship' with spyware maker Paragon Solutions (May 22, 2026) <https://www.npr.org/2026/05/22/nx-s1-5831577/dhs-ice-spyware-paragon>.

⁶ Thomas Brewster, How ICE Is Using Fake Cell Towers to Spy on People's Phones, FORBES (Sept. 9, 2025), <https://www.forbes.com/sites/the-wiretap/2025/09/09/how-ice-is-using-fake-cell-towers-to-spy-on-peoples-phones/>.

⁷ Joseph Cox, 'ELITE': The Palantir App ICE Uses to Find Neighborhoods to Raid, 404 Media (Jan. 15, 2026), <https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/>.

databases to create unified investigative files. ICE has also gained access to taxpayer records at the Internal Revenue Service and Medicaid records at the Centers for Medicare and Medicaid Services. Other components of DHS are integrating Social Security data, passport information, and state DMV and voter records into an unprecedented database of U.S. citizens.

The civil liberties implications extend far beyond the immigration context. The facial recognition databases ICE accesses include millions of American citizens. The location tracking tools ICE deploys can and have been used to surveil U.S. citizens engaged in lawful activity. Moreover, none of these technologies are likely to remain siloed within ICE. The infrastructure ICE builds will likely be shared with other law enforcement agencies. And the databases ICE accesses could become available to an expanding web of federal, state, and local authorities.

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 otherwise need a warrant to obtain, including location records and data that can reveal a person's web-browsing activity. 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."⁸

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."⁹

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

- Information from individuals' visits to health clinics,¹⁰ as well as reproductive tracking applications installed on people's phones;¹¹ and
- Information regarding people's race, ethnicity, gender, sexual orientation, income, and political and religious affiliations.¹²

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,

⁸ Byron Tau, IRS Used Cell Phone Location Data to Try to Find Suspects, WALL ST. J. (Jun. 19, 2020).

⁹ Byron Tau, U.S. Spy Agencies Know Your Secrets. They Bought Them., Wall St. J. (Mar. 8, 2024).

¹⁰ Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, Vice (May 3, 2022).

¹¹ Joseph Cox, Data Marketplace Selling Info About Who Uses Period Tracking Apps, Vice (May 17, 2022).

¹² Joseph Cox, How the U.S. Military Buys Location Data from Ordinary Apps, Vice (Nov. 16, 2020).

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. Indeed, the ACLU recently released a partial DHS legal analysis that we obtained under the Freedom of Information Act that shows the agency contorting itself to distinguish the cell phone location data that the Supreme Court held requires a warrant in *Carpenter v. United States*, from the equivalently sensitive and revealing location information to which the government is now purchasing access in bulk.¹³

This is happening 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 warrant or, in some cases, a court order. However, that law --- 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. The Fourth Amendment Is Not for Sale Act, which passed the House of Representatives with bipartisan support last Congress, would have closed this dangerous loophole.

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. AI allows forms of surveillance to be carried out at scale, such as contextual communications analysis, that used to require human attention and were therefore subject to natural limits. To be clear, national security and law enforcement agencies have long integrated AI into their operations. And while there have been some 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. As an initial matter, this Committee 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.

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

Section 702 of the Foreign Intelligence Surveillance Act

¹³ DHS Is Circumventing the Constitution by Buying Data It Would Normally Need a Warrant to Access, ACLU (Jan. 12, 2026), <https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access>.

Finally, I would be remiss if I did not mention Section 702 of Foreign Intelligence Surveillance Act, which is currently scheduled to expire on Friday (though surveillance under that law can continue under existing court orders until March 2027). While Section 702 requires that this 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 conduct 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.¹⁴ 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 2022.¹⁵

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. These include searches of:

- Members of Congress and their donors.¹⁶
- Journalists and political activists.¹⁷
- More than 141 individuals protesting the murder of George Floyd.¹⁸

¹⁴ Office of the Dir. of Nat’l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community’s Use of National Security Authorities: Calendar Year 2023, at 19 (2024), https://www.odni.gov/files/ODNI/documents/assessments/ODNI_CY2023_Annual_Statistical_Transparency_Report.pdf.

¹⁵ Privacy & Civ. Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2023), ([here](#)).

¹⁶ See Department of Justice and Office of the Director of National Intelligence, Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence 58, December 2021, <https://www.intelligence.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA702-Compliance.pdf> [hereinafter DOJ & ODNI, Semiannual Assessment December 2021]; 2023 PCLOB 702 Report, *supra* note 18, at 155 and [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 29.

¹⁷ Department of Justice and Office of the Director of National Intelligence, Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence 60, August 2021, https://www.intel.gov/assets/documents/702%20Documents/declassified/22nd_Joint_Assessment_of_FISA_702_Compliance_CLEARED_REDACTED_FOR_PUBLIC_RELEASE.pdf.

¹⁸ No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 27.

Congress should be demanding answers to multiple questions before extending this authority for another day, much less multiple years:

- How are artificial intelligence systems being used in conjunction with Section 702?
- Have domestic agencies like Immigration and Customs Enforcement asked the FBI to run searches for Americans' communications?
- Has such authority been used in connection with the administration's efforts to target activists and nonprofits under the banner of "domestic terrorism"?

The appointment of Bill Pulte as acting director of national intelligence only highlights these concerns. Pulte is the director of the Federal Housing Finance Agency. He has no intelligence experience. As director of the FHFA, he sent criminal referrals to the Justice Department targeting the president's political enemies, including a sitting U.S. Senator, a state attorney general and a sitting Federal Reserve governor. His appointment is a demonstration of why Congress should not reauthorize this program without real safeguards, including a warrant requirement.

The Church Committee: A Model for Accountability

The moment calls for a renewed commitment from Congress to reassert its authority to investigate and constrain the full scope of government surveillance. It can do so by establishing a new bipartisan select committee with the independence, scope, and mandate of the original Church Committee. Such a body would be empowered to examine the full architecture of modern government surveillance and the erosion of civil liberties in the digital age.

In 1975, the Senate established the bipartisan Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Otherwise known as the Church Committee, it was one of the most significant efforts in American history to investigate and restrict the authority and ability of the executive branch to infringe on our civil liberties, undermine democratic accountability, and violate our laws. It remains the gold standard for congressional oversight concerning misuse of Executive Branch power.

The creation of the Church Committee was driven by a convergence of scandal and public outrage over revelations of domestic spying and covert operations. The Watergate investigations had revealed the Nixon administration's misuse of federal agencies to target political opponents, and the exposure of programs such as COINTELPRO revealed the breadth of executive misconduct. As reporters and congressional investigators dug further, it became clear that the federal abuse of power dated back decades before Nixon, implicating administrations of both parties, as well as key agencies and officials across the government.

The Committee's investigations revealed not only the extent of these abuses but their systemic nature and found that "intelligence activities have undermined the constitutional rights of

citizens, primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied.”¹⁹

The Church Committee's work led to critical reforms: the creation of permanent Senate and House Intelligence Committees, passage of the Foreign Intelligence Surveillance Act, and establishment of oversight mechanisms for covert action. And as importantly, it represented a reassertion of congressional authority and a demonstration that even the most secretive elements of the executive branch must be brought within the reach of democratic accountability.

Over time, however, these achievements eroded. Intelligence committees grew to be protective of classified programs rather than skeptical in the name of oversight and public accountability. And the executive branch resisted oversight and accountability by reasserting control through doctrines like state secrets and expansive interpretations of inherent presidential authority. In practice, the oversight framework established in the 1970s has proved ill-equipped to handle digital surveillance and covert operations conducted in the name of counterterrorism.

This is precisely why a new Church Committee is needed. It would produce not just findings, but durable reforms. Updated oversight statutes, modernized surveillance law, and renewed accountability structures capable of meeting the threats of the twenty-first century. Most importantly, it would send an unambiguous message that no administration of either party is beyond the reach of democratic accountability.

Conclusion

What has often been consistent when it comes to both surveillance abuses and broader abuses of power by the executive branch is that there is a hesitancy in Congress to restrain presidents of one's own political party. When your political allies hold power, surveillance authorities can seem like reasonable tools for legitimate purposes. For some, it is only when the other party wields these powers that the dangers become clear.

But in reality, the surveillance authorities you grant or tolerate when your party controls the executive branch will be inherited and likely expanded by the next administration. The infrastructure built to monitor individuals or groups you distrust today could very well be turned against causes you support tomorrow. The only sustainable approach is principled oversight that constrains executive power and related surveillance authorities regardless of who holds the office of the presidency. This requires bipartisan commitment to civil liberties and a return to the ideals behind the original Church Committee.

The question before Congress is whether it will continue down its current path or whether we can change course and conduct the kind of comprehensive investigation that the current surveillance state demands. A new Church Committee, tasked with investigating the exercise and abuse of executive power, would represent the first comprehensive review of presidential authority in nearly half a century. As Senator Frank Church himself warned: “The capability at any time could be turned around on the American people, and no American would have any privacy left,

¹⁹ S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755, bk. 2, at 289 (1976).

such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide."²⁰

Thank you for your attention. I welcome your questions.

²⁰ Meet the Press (NBC television broadcast Aug. 17, 1975) (statement of Sen. Frank Church).