STATEMENT OF

Kia Hamadanchy

Senior Policy Counsel

National Political Advocacy Division

American Civil Liberties Union

For a Hearing on

"Declassified MLK Records: What They Reveal and Why They Matter"

Before the

United States House of Representatives

House Committee on Oversight and Government Reform

Task Force on the Declassification of Federal Secrets

January 22, 2026

Chairwoman Luna, Ranking Member Crockett, and members of the Task Force, thank you for the opportunity to testify today on behalf of the American Civil Liberties Union (ACLU) about the release of files related to Dr. Martin Luther King Jr.'s assassination and the broader issues of accountability for government surveillance that this declassification effort brings into sharp focus.

Today's hearing should not just be about illegal surveillance decades ago but should also be about the continuing need for meaningful congressional oversight and accountability over government surveillance. The need for Congress to act against abuse of federal power is at least as great today as it was fifty or sixty years ago. We suggest today that Congress look back fifty years to how a special congressional committee successfully exposed and pushed back against grave abuses of government power to surveil, track, and threaten individuals and communities.

Illegal Surveillance of Dr. Martin Luther King

The surveillance of Dr. Martin Luther King Jr. represented one of the darkest abuses of government power in the history of our country. Under COINTELPRO Dr. King was subjected to extensive, warrantless surveillance that violated both his constitutional rights and the fundamental principles of a free society.

The FBI's campaign against Dr. King had no connection to any legitimate national security concerns or law enforcement purpose. It was about suppressing and disrupting the movement for civil rights and racial equality. The FBI wiretapped Dr. King's phones, bugged his hotel rooms, monitored his associates, and attempted to destroy his reputation. It remains one of the most shameful episodes in FBI history. This surveillance was warrantless. It was illegal. And it was wrong and represented a profound abuse of executive power.

This experience helps show how surveillance powers that the government claimed for ostensibly legitimate purposes could very easily be turned against nonviolent movements and ordinary citizens. No community or political group is safe from this threat. History shows that surveillance authorities can be easily weaponized against whichever groups the government views as threatening at any given moment—whether civil rights activists in the 1960s, anti-war protesters in the 1970s, Muslim Americans after 9/11, or anyone else wrongly targeted by Executive Branch officials.

The Church Committee: A Model for Accountability

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 of the executive branch to infringe on our civil liberties, undermine democratic accountability—and to violate our laws. It remains the gold standard for congressional oversight over 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.

In December 1974, the *New York Times* published a story detailing how the CIA had engaged in a "massive, illegal domestic intelligence operation" against antiwar activists and other American citizens.[1] At this point, it had become abundantly clear that US intelligence and law enforcement agencies had been operating far beyond their statutory and constitutional limits. And in response in January 1975, the Senate voted 82-4 to create the Church Committee, led by Idaho Senator Frank Church. Under his leadership, the Committee launched a sweeping bipartisan inquiry—with a mandate to investigate federal abuse of power for a roughly 30-year period from the 1940s to the 1970s—and over the course of sixteen months, the Committee conducted 126 committee meetings, 40 subcommittee hearings, and 800 witness interviews.[2] It was also entirely a bipartisan effort and all 14 reports issued by the committee were supported on a bipartisan basis.[3]

The investigation uncovered:

- **COINTELPRO**: The FBI's program created under J. Edgar Hoover to infiltrate and disrupt civil rights and antiwar movements. Few members of any of the groups targeted by COINTELPRO were ever charged with a crime. The Church Committee concluded that, "The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power....Groups and individuals have been harassed and disrupted because of their political views and their lifestyles."[4] In 1986, a federal court determined that COINTELPRO was responsible for at least 204 burglaries by FBI agents, the use of 1,300 informants, the theft of 12,600 documents, 20,000 illegal wiretap days, and 12,000 bug days.[5]
- **Operation CHAOS**: The CIA's domestic surveillance of anti-war protestors, political dissidents, and civil rights activists under which it spied on as many as 10,000 Americans.[6]
- **Operation SHAMROCK**: An NSA program that collected the contents of private telegrams and communications without warrant or judicial approval.

---

[1] Levin Ctr. for Oversight & Democracy, *Frank Church and the Church Committee*, https://levin-center.org/frank-church-and-the-church-committee/
[2] Id.
[3] Id.
[4] 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 5 (1976).
[5] Press Release, Am. Civil Liberties Union, "Trust Us, We're the Government": ACLU Looks at Domestic Surveillance and the Need to Watch the Watchers in Times of Crisis (Oct. 10, 2001), https://www.aclu.org/press-releases/trust-us-were-government-aclu-looks-domestic-surveillance-and-need-watch-watchers.
[6] Seymour M. Hersh, Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years, N.Y. TIMES (Dec. 22, 1974), https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html.

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."[7]

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.

For example, we have also seen concerns from across the political spectrum as to the current conduct of the FBI. In recent years, the Heritage Foundation issued a report on reforming the FBI that contained extensive suggestions as to how to rebuild the FBI from the ground up.[8] Similarly, the ACLU and other civil society groups wrote to current FBI Director Kash Patel following his confirmation urging specific reforms to many of the FBI's current practices.[9]

Current Surveillance Abuses

Under the Fourth Amendment, we all have the right to be free from unreasonable searches and seizures by the government. Yet in recent decades—under presidents of both parties--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. And the concerns regarding

---

[7] 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).
[8] Steven G. Bradbury, *How to Fix the FBI*, Heritage Found. Backgrounder No. 3777 (July 10, 2023), https://www.heritage.org/the-constitution/report/how-fix-the-fbi.
[9] *23 Civil Society Groups Including Restore the Fourth Request Meeting with FBI Director Kash Patel on Surveillance Reform, Transparency*, Restore the 4th (Jan. 17, 2025), https://restorethe4th.com/23-civil-society-groups-including-restore-the-fourth-request-meeting-with-fbi-director-kash-patel-on-surveillance-reform-transparency/.

these programs from Congress have been bipartisan, including legislation introduced by the Chairwoman of this Task Force to repeal the PATRIOT Act. Many members of this Task Force--from both sides of the aisle--are among the most consistent and active supporters of Congress asserting its constitutional authority to rein in Executive Branch overreach.

Section 702 of the Foreign Intelligence Surveillance Act

In about three months from now, on April 20, 2026, Section 702 of 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 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.[10] 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.[11] 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.[12]
- Journalists and political activists.[13]
- More than 141 individuals protesting the murder of George Floyd.[14]

---

[10] 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.

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

[12] 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.

[13] 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.

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

- Over 20,000 individuals associated with the events of January 6th.[15]

Executive Order 12333

Beyond the surveillance authorities established by statute, one of the most powerful and least understood surveillance authorities is Executive Order 12333. Signed by President Reagan in 1981 and modified many times since, this executive order is the primary authority relied upon by intelligence agencies, including the NSA, to conduct surveillance of foreigners outside the United States.

Surveillance conducted under EO 12333 is implemented almost entirely by the executive branch, with little review by Congress or the courts. It lacks even the plainly inadequate legislative and judicial checks that exist for other surveillance authorities like Section 702 of FISA. What disclosures that do exist indicate that the government operates a host of large-scale programs under EO 12333, many of which appear to involve the collection of vast quantities of both U.S. and non-U.S. person information.

Programs that have been publicly disclsoed under 12333 in the past have included the NSA's collection of billions of cellphone location records each day[16], its acquisition of hundreds of millions of text messages from around the world daily[17], its recording of every single cellphone call into, out of, and within at least two countries[18], its collection of hundreds of millions of contact lists and address books from personal email and instant messaging accounts[19], and its interception of data from Google and Yahoo user accounts as that information traveled between those companies' data centers located abroad.[20]

The government frequently argues that its sweeping surveillance approach is lawful because it follows certain procedures when searching and sharing the information it gathers. However, if the NSA cannot or will not ensure that it is correctly identifying Americans' communications when it vacuums them up, the public cannot trust that the NSA is properly safeguarding Americans' private information.

---

[15] [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), supra note 97, at 29.
[16] Barton Gellman & Ashkan Soltani, NSA tracking cellphone locations worldwide, Snowden documents show, WASH. POST (Dec. 4, 2013), https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locationsworldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.
[17] James Ball, NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep, THE GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-globalsweep.
[18] Ryan Devereaux, Glenn Greenwald & Laura Poitras, Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas, THE GUARDIAN (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/datapirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.
[19] Barton Gellman & Ashkan Soltani, NSA Collected Millions of E-mail Address Books Globally, WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-booksglobally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html.
[20] Barton Gellman & Ashkan Soltani, NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say, WASH. POST (Oct. 30, 2013) https://www.washingtonpost.com/world/national-security/nsa-infiltrateslinks-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74d89d714ca4dd_story.html.

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 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."[21]

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."[22]

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

- Information from individuals' visits to health clinics[23], as well as reproductive tracking applications installed on people's phones;[24] and
- Information regarding people's race, ethnicity, gender, sexual orientation, income, and political and religious affiliations.[25]

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, 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.[26]

---

[21] Byron Tau, IRS Used Cell Phone Location Data to Try to Find Suspects, WALL ST. J. (Jun. 19, 2020)
[22] Byron Tau, U.S. Spy Agencies Know Your Secrets. They Bought Them., Wall St. J. (Mar. 8, 2024),
[23] Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, Vice (May 3, 2022).
[24] Joseph Cox, Data Marketplace Selling Info About Who Uses Period Tracking Apps, Vice (May 17, 2022).
[25] Joseph Cox, How the U.S. Military Buys Location Data from Ordinary Apps, Vice (Nov. 16, 2020).
[26] *DHS Is Circumventing the Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (May 24, 2022), https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access.

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 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, including from the Chairman and Ranking Member of this Task Force, would have closed this dangerous loophole.

NSPM-7 targeting nonprofits and activists

The Trump Administration recently issued National Security Presidential Memorandum/NSPM-7, titled "Countering Domestic Terrorism and Organized Political Violence," which directs federal departments and law enforcement agencies to focus existing authorities on investigations of civil society groups, including nonprofits, activists, and their donors. Through this memorandum, the administration instructs agencies to investigate and disrupt what it characterizes as networks and organizations engaged in "domestic terrorism" and political violence. While the memorandum and its focus are new, it builds on structures that were built, expanded, and routinely misused for more than twenty years, causing harm to Americans across four administrations, under presidents from both parties.

Specifically, NSPM-7 orders Joint Terrorism Task Forces, which are FBI-operated partnerships between federal law enforcement and intelligence agencies and state and local law enforcement that are intended to conduct counterterrorism investigations, to instead investigate and disrupt groups and individuals based on vaguely defined categories of "ideological agendas." JTTFs already have a documented history of investigations that wrongly target protestors, communities of color, and those engaged in dissent. In major cities, these task forces have monitored Black Lives Matter activists, targeted Muslims, journalists, and environmentalists for investigation, including with intimidating visits to their homes or workplaces.

Although this memorandum does not create any new federal powers or crimes, it uses dangerously stigmatizing rhetorical labels to paint groups and individuals as "domestic terrorists." It asserts the "designation" of groups as domestic terrorism organizations without any citation to authority—and there is no such authority. Unlike for foreign terrorism, there is no domestic terrorism labeling or designation regime, and Congress has passed no law creating one for very good reason: it would inevitably sweep in Americans' First Amendment protected beliefs, associations, and speech.

NSPM-7's strategy to investigate and disrupt networks, entities, and organizations goes right back to many of the abuses uncovered by the Church Committee, including illegal surveillance of Dr. King and other civil rights leaders. The memorandum instructs federal departments to use authorities they already have and focus them on investigations of civil society groups to disrupt and prevent activities the administration characterizes as terrorism and political violence, using categories that are subject to political, ideological, and racial manipulation and bias.

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. 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.[27] 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 certificate, when the app says a person is undocumented.[28] 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.

Automated License Plate Readers

The U.S. Border Patrol, which is part of Customs and Border Protection within DHS, has also secretively 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

---

[27] 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/.
[28] 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/.

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.[29] In August 2025, the Trump administration lifted a previous 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.

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. What is used by ICE for one targeted population will very likely migrate over to other federal law enforcement to target literally anyone in the United States, even those not engaged in any unlawful conduct, and in fact, even those 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.[30]

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.[31] A tool reportedly called ELITE populates

---

[29] Stephanie Kirchgaessner, *Ice Obtains Access to Israeli-Made Spyware that Can Hack Phones and Encrypted Apps*, The Guardian (Sept. 2, 2025), https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware.

[30] 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/.

[31] 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/.

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 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.

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 when it comes to trying 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 presidency. This requires bipartisan commitment to civil liberties and a return to the ideals behind the original Church Committee.

The question before this Task Force and before Congress is whether we 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, such is the capability to

monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide."[32]

Thank you for your attention. I welcome your questions.

[32] *Meet the Press* (NBC television broadcast Aug. 17, 1975) (statement of Sen. Frank Church).