OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

THURSDAY, DECEMBER 11, 2025

Serial No. 119–44

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
62–294 WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
THOMAS P. TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
SCOTT FITZGERALD, Wisconsin
BEN CLINE, Virginia
LANCE GOODEN, Texas
JEFFERSON VAN DREW, New Jersey
TROY E. NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
HARRIET M. HAGEMAN, Wyoming
LAUREL M. LEE, Florida
WESLEY HUNT, Texas
RUSSELL FRY, South Carolina
GLENN GROTHMAN, Wisconsin
BRAD KNOTT, North Carolina
MARK HARRIS, North Carolina
ROBERT F. ONDER, JR., Missouri
DEREK SCHMIDT, Kansas
BRANDON GILL, Texas
MICHAEL BAUMGARTNER, Washington

JAMIE RASKIN, Maryland, *Ranking Member*
JERROLD NADLER, New York
ZOE LOFGREN, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
ERIC SWALWELL, California
TED LIEU, California
PRAMILA JAYAPAL, Washington
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
DEBORAH K. ROSS, North Carolina
BECCA BALINT, Vermont
JESÚS G. "CHUY" GARCÍA, Illinois
SYDNEY KAMLAGER-DOVE, California
JARED MOSKOWITZ, Florida
DANIEL S. GOLDMAN, New York
JASMINE CROCKETT, Texas

CHRISTOPHER HIXON, *Majority Staff Director*
ARTHUR EWENCZYK, *Minority Staff Director*

C O N T E N T S

THURSDAY, DECEMBER 11, 2025

OPENING STATEMENTS

WITNESSES

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

Page

QUESTIONS AND RESPONSES FOR THE RECORD

OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Thursday, December 11, 2025

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

Washington, DC

The Committee met, pursuant to notice, at 9 a.m., in Room 2141, Rayburn House Office Building, the Hon. Jim Jordan [Chair of the Committee] presiding.

Members present: Representatives Jordan, Issa, Biggs, McClintock, Tiffany, Massie, Roy, Fitzgerald, Cline, Gooden, Van Drew, Nehls, Moore, Kiley, Hageman, Lee, Fry, Grothman, Knott, Harris, Onder, Schmidt, Gill, Baumgartner, Raskin, Lofgren, Cohen, Johnson, Jayapal, Scanlon, Neguse, Ross, Balint, Garcia, Moskowitz, and Crockett.

Chair JORDAN. The Committee will come to order. Without objection, the Chair is authorized to declare a recess at any time. We welcome everyone to today's hearing on the Foreign Intelligence Surveillance Act.

The Chair recognizes the gentleman from Texas, Mr. Nehls, to lead us in the Pledge of Allegiance.

ALL. I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation, under God, indivisible, with liberty and justice for all.

Chair JORDAN. I thank the gentleman for leading us and sorry to hear of his recent announcement. He is not going to be running for reelection, but glad to have him with us here today.

We will start with opening statements, and we will get right to witnesses and to today's hearing.

On February 2, 2021, the FBI was given, I believe, it was just then when we were in the Minority, just Minority staff and Members, a briefing on the 702 program and I remember that briefing. I can't remember who asked the question, but one of us asked the question how many agents, how many people at the FBI, have access to the 702 data? The data that is collected in this database, surveilling foreigners, but all kinds of people get swept up, all kinds of Americans, U.S. persons get swept up in this. How many agents, how many people at the FBI can query, which I always point out is a fancy name for search, how many people can search this data? Their answer was 10,000 people. We didn't know what answer to expect, but we didn't quite expect that big of a number. If they had told us three people, I thought well, that seems fairly

small. If they had told us about any number over a 1,000, I would have said that is crazy. They told us 10,000.

We then said how many queries—we found out we had the IG do a study and investigation. How many queries are these 10,000 agents, potentially 10,000 agents doing who have access to this information, how many are they doing on U.S. persons? That answer from the IG was three million, three million in one calendar year, 2021.

The IG also told us that 278,000 of those searches on U.S. persons were most definitely done in an improper way. What that meant by improper is they didn't follow the rules Congress had set. They didn't follow the FBI rules. They didn't follow our rules. They didn't even follow their own rules when they were doing these unbelievable millions of searches, 278,000, definitely done improperly, and the potential of 10,000 people at the FBI to do those very searches.

Who were they searching? Who are some of the people they searched? Well, the IG told us this as well: Journalists, people part of Black Lives Matter, Members of Congress, 19,000 political donors, and ex-girlfriends. It was as obnoxious as you can imagine. Again, we are just talking about the 702. We are not even getting into Title I. With all the problems with Title I, some of the things we learned a few years ago relative to surveilling a Presidential campaign, we all know about that. We are just talking about 702, that all this is coming up, as everyone knows for reauthorization, the 702 program for reauthorization, but we can address the Title I as well. All of that is coming due here in just four months. We felt it was important to have this hearing when we begin to talk about some of the things that still need to be done.

I want to back up a second to say this. Last Congress, I do think the good work of this Committee, some of our Members working closely in a working group with Members of the House Intelligence Committee, I do think we had some good reforms that got put into the bill last Congress. A lot of that is due to the work of our witnesses here and the groups that they represent and we appreciate that. We codified procedures to reduce improper queries. Last year the number was done to 9,000 queries on U.S. persons. Important changes that were made to the 702 program safeguards, protecting Americans' liberties and of course, some changes also made to the Title I section of the FISA law as well.

I know our Ranking Member knows this. I know every Member of this Committee knows this. We are the Judiciary Committee, where we are supposed to be focused on protecting the Constitution, the Bill of Rights, and the liberties that we enjoy as Americans. We think it is important, as we move forward, that we do just that and part of that is if you are going to search this database, and you are going to search using an American's name, phone number, and email address, we believe you should go to a separate and equal branch of government and get a warrant to do so. We think that is fundamental. Everyone knows that last Congress we were close to making that happen, close as you can get without making it there across 212–212. I will never forget that vote. We want to hopefully get that included in the reforms that we put together as we move forward over these next four months.

To start that effort, we have got some great witnesses who we will look forward to hearing, but I want to yield back now and let the Ranking Member have his opening statement and then we will get right to our great panel. With that, I yield to the gentleman from Maryland.

Mr. RASKIN. Thank you very much, Mr. Chair, and thanks to our witnesses for joining us today. Section 702 expires April 19th next year. This gives us four months to put together a bill that prioritizes protecting American fundamental constitutional rights while preserving a program that advances national security. Over the years, FISA has remained a subject of bipartisan collaboration on this Committee, and I really want to thank Chair Jordan and Chair Biggs for working with all of the Members of the Committee to protect American civil liberties.

When Congress reauthorized Section 702 last Congress, we gave the Executive Branch two years to show that it could protect civil liberties without the need for greater judicial oversight. We said that we would rely on the FBI's promise that the modest changes, like requiring approvals for U.S. person queries in the Reforming Intelligence and Securing American Act, or RISAA, would be enough to prevent greater violations of civil liberties, and we promised in turn that we would keep a close eye on how surveillance authorities are used during that time. This two-year experiment is nearly complete now and the results are alarming. We have witnessed an attack on the FBI's internal guardrails against abuse of Section 702 authorities and an unprecedented increase in government surveillance and an alarming coziness between the government and big tech, all which puts Americans' data and civil liberties in jeopardy.

We must strengthen Federal law to protect American privacy and liberty and Congress can start with FISA Section 702. As everyone in the room knows, 702 was never meant to apply to American citizens. Under the law, the government can only collect communications from targets to meet two criteria: (1) They have got to non-U.S. persons; and (2) they have got to be located overseas. Americans and people on U.S. soil are protected by the Fourth Amendment that prohibits unreasonable searches and seizures, guarantees the warrant requirement. If law enforcement wants to look at American citizens' emails, they have got to get a warrant to do it. Despite all these protections, because Section 702 enables the intelligence community to ingest an incredible amount of data, American citizens' communications are often swept up in 702 collections. When that happens, those records end up in the FBI's massive database and under current law, the FBI can search that database for U.S. person identifiers like Americans' names and street addresses or evidence of potential crimes or threats to national security. As the Chair said, "10,000 have access to that."

Administrations of both parties have repeatedly abused this trove of U.S. person data. Recent audits show the FBI has searched the 702 databases for candidates for Federal office, Black Lives Matter, protesters, and Federal contractors, among other Americans, who ought to be protected. Two years since we enacted RISAA. However you might have felt about the modest changes in that bill, the landscape has changed. For years, the leaders of this

Committee have warned of how Executive Branch surveillance powers could be abused by administrations that don't show sufficient care for the protection of civil liberties and who use cutting-edge technology to spy on Americans and who ignore basic principles of due process and constitutional freedom to achieve their own ends.

In 2025, we know that we were right to worry. Here is just one example I have been concerned for years about U.S. Government purchasing and compiling data about our own people. That problem has been compounded in this administration which is actively building profiles on American citizens by combining data traditionally siloed in separate agencies, your tax returns, your health records, and any interactions with police. With information purchased from tech companies, the administration is breaking down the very few guardrails that still exist on protecting our privacy, enabling the Executive Branch to track the movements of dissenters and supporters alike.

We have a lot to be concerned about at this point. I am glad we are proceeding in a bipartisan way for the legislative defense of essential constitutional civil liberties. I look forward to hearing from all our witnesses today and how we can property protect American civil freedom in this perilous era. I yield back to you, Mr. Chair, the balance of my time.

Chair JORDAN. I thank the gentleman for his statement. Without objection, all other opening statements will be included in the record. We will introduce today's witnesses.

Mr. Brett Tolman is the Executive Director of Right on Crime, a nonprofit organization that advocates criminal justice issues. He has testified here many times. He previously served as the U.S. Attorney for the District of Utah and is the Chief Counsel for the Crime and Terrorism for the Senate Judiciary Committee.

Mr. Gene Schaerr is the General Counsel for the Project for Privacy and Surveillance Accountability, a nonprofit organization that advocates greater protections for privacy, civil liberties, and government surveillance programs. He is also the Managing Partner of Schaerr and Jaffe, LLP, where he focuses on civil appellate matters.

Mr. James Czerniawski is the head of Emerging Technology and Policy at the Consumer Choice Center. He previously was a Senior Policy Analyst at Americans For Prosperity. His research focuses on the issues surrounding technology and innovation.

Ms. Elizabeth Goitein is the Senior Director of the Brennan's Center Liberty and National Security Program. She previously served as Senate staffer with the Department and with the Department of Justice. Her work focuses on Presidential emergency powers, government surveillance, and government secrecy.

I know many of you have been here before and we appreciate the work you have done for our country for being with us today. We welcome all of you and we will begin by swearing you in. Would you please stand and raise your right hand?

Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief so help you God?

Let the record reflect that all witnesses answered in the affirmative. Thank you. You can be seated, of course. Please know, you have been through this before, that your written testimony will be entered into the record in its entirety. We ask that you summarize that in five minutes and we will just go right down like you were introduced.

Mr. Tolman, you may begin.

STATEMENT OF BRETT TOLMAN

Mr. TOLMAN. Thank you, Chair Jordan, Ranking Member Raskin, and the distinguished Members of the Committee. Thank you for the opportunity to testify today.

Oversight of the Foreign Intelligence Surveillance Act is a debate that goes to the heart of what it means to be an American: Commitment to the rule of law, the constitutional rights we hold dear, and the principle of limited government. FISA is in desperate need of reforms, or rather our country desperately needs to reform FISA.

For decades and with increasing regularity, it has been the government's permission slip for warrantless spying on Americans. This is despite the Fourth Amendment. To be sure, FISA serves an important national security interest. I would know. I helped write some of the FISA laws when I worked as Chief Counsel over at Crime and Terrorism in the Senate Judiciary Committee. I later prosecuted national security cases as a Federal prosecutor. These credentials, however, don't contradict the harsh truth that the FISA system is flawed. It enables unconstitutional government surveillance and doesn't protect our civil liberties presently.

Nowhere is this more clearer than with Section 702. Section 702 was sold to Congress as a vital tool to target foreign adversaries. We were given high-stake assurances by DOJ and FBI leaders, namely, James Comey and Robert Mueller, that it would not be used improperly against honest Americans. I was in the room when they represented it would not be abused. That was a lie.

FISA abuse is not speculative. There is clear record of systemic failure, constitutional betrayal, and the disregard for the rule of law, confirmed by the FISA Court itself and government watchdogs. For instance, the Crossfire Hurricane investigation used flawed information and deceit to justify FISA's surveillance of Carter Page, proves the vulnerability of the system is to political weaponization.

Arctic Frost investigation, which targeted hundreds of American citizens including sitting Republican lawmakers, highlights how domestic political matters are swept up by FISA. The FBI has carried out warrantless searches of Section 702 database involving American lawmakers, journalists, political donors, and civil rights protesters. One thousand six hundred searches were conducted for Americans who were at a specific airport on a particular day. Two thousand backdoor searches were done on athletes at a sporting event.

NSA analysts searched for communications of prospective tenants and rental properties that they owned personally and for people met through online dating sites. This is not national security intelligence gathering, it is domestic spying.

With FISA set for reauthorization in April, Congress faces an important question. Will we limit the government, or will we license its continued Fourth Amendment violations? Internal policy changes by the offending agencies are not enough. FISA must be rebuilt and reformed.

Section 702, for example, it is necessary that the Congress requires the government to obtain a probable cause warrant if a search is done on a U.S. citizen in a domestic investigation. If this warrant requirement had been in place, the vast domestic surveillance of Americans under Arctic Frost, for example, would have required judicial review and likely would not have occurred.

Section 704, which lets the government surveil Americans abroad believed to be a foreign asset, would benefit from heightened judicial review such as that declassified and released court opinions and the use of third-party experts who can review Section 704 applications.

Section 705(b) can easily bypass the requirement for comprehensive judicial review, allowing the government to move to a more intrusive form of surveillance with less scrutiny than a new probable cause application would require. Reforms should center on the consistent probable cause decisions.

Last, FISA Courts need structural reforms such as penalties for omissions or misrepresentations like those used to target Carter Page. The FISC should also incorporate third-party advocates to balance the weighted government proceeding in declassified FISC rulings.

In conclusion, Congress must not be complicit in facilitating a surveillance State. It must either mandate reforms or allow authorities like Section 702 to expire. I applaud this Committee and its leadership for its thoughtful review and I stand ready to work with you to craft reforms that are conservative in principle, effective in practice, and constitutional in design. Thank you, Mr. Chair.

[The prepared statement of Mr. Tolman follows:]

Right On CRIME

Statement of Brett Tolman, former U.S. Attorney and Executive Director of Right On Crime

U.S. House Judiciary Committee
"Oversight of the Foreign Intelligence Surveillance Act"
Thursday, December 11, 2025

Chairman Jordan, Ranking Member Raskin, and distinguished members of the Committee, thank you for the opportunity to testify today.

Oversight of the Foreign Intelligence Surveillance Act (FISA) is a debate that goes to the heart of what it means to be an American: commitment to the rule of law, the constitutional rights we hold dear, and the principle of limited government.

My name is Brett Tolman, and I have served as a U.S. Attorney for the District of Utah and as a former chief counsel for crime and terrorism for the U.S. Senate Judiciary Committee. I am testifying today as the Executive Director of Right On Crime, a national criminal justice campaign of the Texas Public Policy Foundation and as Chair of the Law and Justice Campaign for the America First Policy Institute.

FISA is in desperate need of reforms—or rather, our country desperately needs to reform FISA. For decades, and with increasing regularity, it has been the government's permission slip for warrantless spying on Americans. This is despite the Fourth Amendment's clear mandate that the government shall not engage in unreasonable searches and seizures, and no warrant shall be issued without probable cause.

To be sure, FISA serves an important national security interest. I would know. I helped write some of the FISA laws when I worked as a chief counsel on the Senate Judiciary Committee. And I prosecuted national security cases as a federal prosecutor. These credentials don't contradict the harsh truth that the FISA system is flawed. It enables unconstitutional government surveillance and doesn't protect our civil liberties.

Nowhere is this clearer than with Section 702 of FISA.

Section 702 of FISA was sold to Congress as a vital tool to target foreign adversaries overseas. We were given high-stake assurances by Department of Justice (DOJ) and Federal Bureau of Investigations (FBI) leadership that it wouldn't be used improperly against honest Americans. In fact, it was James Comey and Robert Mueller who promised this to me and others working on the reauthorization of the PATRIOT Act post-9/11.

That was a lie.

FISA abuse is not speculative. There is a clear record of systemic failure, constitutional betrayal, and a disregard for the rule of law, confirmed by the FISA Court itself, the DOJ Office of the Inspector General, and the Privacy and Civil Liberties Oversight Board (PCLOB).

For instance:

- The Crossfire Hurricane investigation—using flawed information and outright deceit to justify FISA surveillance of American citizen Carter Page—proves how vulnerable this system is to political weaponization.
- The FBI has carried out warrantless searches of the Section 702 database involving American lawmakers, [1] journalists,[2] political donors,[3] and civil rights protestors.[4]
- "[T]ens of thousands" of baseless FBI backdoor searches "related to civil unrest" were conducted over a one-year period.[5]
- Batch backdoor searches were conducted for 1,600 Americans "who had flown through an airport during a particular date range and were either traveling to or returning from a foreign country;"[6]

---

[1] https://thehill.com/homenews/administration/4110850-fbi-improperly-used-702-surveillance-powers-on-us-senator/
[2] https://www.intel.gov/assets/documents/702-documents/declassified/22nd_Joint_Assessment_of_FISA_702_Compliance_CLEARED_REDACTED_FOR_PUBLIC_RELEASE.pdf#page=60
[3] https://www.intelligence.gov/assets/documents/702-documents/declassified/21/2021_FISC_Certification_Opinion.pdf#page=29
[4] https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf?inline=1#page=197
[5] https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf at 151.
[6] *Id.* at 148.

- 2,000 backdoor searches were conducted for "the names and dates of birth of individuals registered as competitors in [an] athletic event;"[7]
- National Security Agency (NSA) analysts searched for communications of a prospective tenant of a rental property they owned[8]; and
- An NSA analyst did a backdoor search for the communications of two individuals the analyst met on an online dating service.[9]

This is not national security intelligence gathering; it is domestic spying.

The entire FISA apparatus – from the expired bulk collection under Section 215 to the continuously abused "backdoor search" loophole in 702 – is structurally compromised. It has evolved from a law intended to surveil foreign spies into a domestic surveillance dragnet.

With FISA set for reauthorization in April, Congress faces an important question: will we limit the government, or will we license its continued Fourth Amendment violations?

The FBI, DOJ, and NSA have all affirmed that prior abuses have been fixed and that they can be prevented in the future.[10] But internal policy changes by the offending agencies aren't enough. FISA must be rebuilt and reformed.

Necessary Reforms:

Section 702:

(1) **A warrant requirement for access to Americans' communications.** The most essential reform is non-negotiable: if the government wants to search Section 702 datasets for a U.S. citizen in a domestic investigation, it must obtain a probable cause warrant. This is not radical; it's simply constitutional.

---

[7] *Id.* at 149.
[8] *Id.* at 137-38.
[9] *Id.* at 138.
[10] *See, generally* testimony from government witnesses before the U.S. Senate Judiciary Committee, "Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities," https://www.judiciary.senate.gov/oversight-of-section-702-of-the-foreign-intelligence-surveillance-act-and-related-surveillance-authorities.

(2) **Close the data-broker loophole.** When intelligence and law enforcement agencies cannot access information due to statutory or constitutional protections, they should not be allowed to purchase that same data from commercial data brokers. This current practice allows the government to buy its way around the law and must end.

(3) **Structural reform of the FISA Court (FISC).** The FISC today operates as a one-sided proceeding where the government controls the information and the narrative. Congress can provide checks, including:

- Penalties for overt omissions or misrepresentations made by agents to obtain FISA warrants.
- Independent advocates who can bring much-needed adversarial balance to a court that currently rubber-stamps government overreach.
- Notice to Americans whose data was accessed, even if no charges were filed.
- Declassification and public release of significant FISC rulings, subject to necessary national security redactions.

Section 704:

Section 704 of FISA authorizes the government to surveil a U.S. person who is reasonably believed to be located outside the U.S. to gather foreign intelligence. But unlike 702, Section 704 uses a probable cause standard. An application to the FISC must demonstrate probable cause to believe that the U.S person is a foreign power or agent.

Nevertheless, reforms could strengthen judicial oversight and minimize the potential for abuse.

(1) Like Section 702, FISC opinions should be declassified and released publicly, subject to necessary national security redactions.

(2) An independent third-party legal expert should be appointed to review applications under Section 704. This could ensure that the FISC hears adversarial arguments, opposed to weighted government-only perspectives.

Section 705:

A related provision, 705(b), poses its own unique threats to due process. This section allows for streamlined judicial approval of an order for physical search and electronic surveillance if a probable cause order has already been issued for the same person under Section 704. This effectively bypasses the requirement for a fresh, comprehensive judicial review, allowing the government to move to a more intrusive form of surveillance with less scrutiny than a new application would require. Reforms should center on consistent probable cause decisions.

(1) The FISC must conduct a *de novo* review of a government's application if the government seeks to use Section 705(b) piggy-back onto an existing Section 704 probable cause order.

(2) Streamlined approvals should be limited to the exact same surveillance method for renewals only, which would prohibit their use for pivoting to more intrusive techniques without specified probable cause.

Section 215:

There are provisions of FISA that have expired – including the controversial business record provision in Section 215. This authority, which largely permitted the bulk collection of telephone metadata, has been limited but it *could* be revived by Congress.[11] I urge this Committee to allow Section 215 to remain unauthorized.

Conclusion:

Congress must not be complicit in facilitating a surveillance state. It must either mandate reforms or allow authorities – like Section 702 – to expire.

I applaud this Committee for its thoughtful review and I stand ready to work with you to craft reforms that are conservative in principle, effective in practice, and constitutional in design.

Thank you, and I look forward to your questions.

[11] Congressional Research Service, "Origins and Impact of the Foreign Intelligence Surveillance Act (FISA) Provisions That Expired on March 15, 2020," available at file:///C:/Users/RachelWright/Downloads/R40138.24.pdf.

Chair JORDAN. Thank you. Mr. Schaerr, you are recognized for five minutes.

STATEMENT OF GENE SCHAERR

Mr. SCHAERR. Thank you, Chair Jordan, Ranking Member Raskin, and the Members of the Committee. Thank you for the opportunity to testify at this hearing which is particularly timely as we prepare to celebrate the Declaration of Independence next year.

In considering the reauthorization of FISA Section 702 which my organization supports, the overriding question faced by this body is the extent to which it will allow the intelligence community to continue engaging in warrantless surveillance of Americans and without, as the Declaration put it, the consent of the government through its representatives in this body or otherwise. As you know, absent consent or truly exigent circumstances, the Fourth Amendment generally condemns warrantless searches.

While last year's reauthorization was in many respects a good first step toward needed reform, at least four important issues remain unresolved.

(1) Section 702 still allows the government to search Americans' communications without a warrant through so-called backdoor searches.

(2) Federal agencies routinely purchase and review our geolocation internet search history and other sensitive personal information from data brokers, all without a warrant and without allowing providers even to inform us of those searches.

(3) A newly expanded definition of electronic communication service provider under last year's reauthorization allows the NSA to force countless small businesses and other organizations to assist in warrantless surveillance. It even includes houses of worship, thus ensuring that even atheists will now have to agree that someone is listening when we pray.

(4) There is still no provision requiring the FISA Court to include amici, experts who represent the privacy interests of all Americans in Title I surveillance proceedings involving the Members of Congress, political campaigns, and other sensitive targets.

How then should Congress approach the upcoming reauthorization?

First, we believe Congress should institute a warrant requirement with appropriate exceptions before the FBI or other agencies can search and review Americans' communications collected under 702. Just last year, as the Chair mentioned, this Committee in a near unanimous bipartisan show of strength, this Committee voted to close that loophole and it should do so again and this time insisting on closing that loophole as a condition of reauthorizing 702.

Second, it is critical for Congress to rein in the Federal Government's ever-growing purchase and warrantless searches of Americans' geolocation and other sensitive personal data purchased from data brokers. I applaud the Committee for its impressive bipartisan work over the last several years to address this issue, but this next reauthorization is the time to insist that this data broker loophole also be closed.

Third, the definition of electronic communication service provider under FISA should be narrowed to exclude houses of worship and

countless small businesses and other organizations that were unfortunately included in last year's reauthorization. There is no justification for secretly coercing these entities to assist the NSA and the FBI in conducting surveillance.

Fourth, Congress should require amicus participation in politically sensitive FISA cases by finally enacting a robust amicus provision of the sort that passed the Senate in 2020 with 77 votes. Nearly a decade after the Trump campaign and transition were illegally surveilled, this key reform which would have prevented many of the abuses that occurred in 2016 is still not in place. I have seen the impact of that outrageous abuse in my separate work representing Carter Page in challenging that abuse in court. Once again, I applaud this Committee for including a robust amicus process in the reform legislation last year, and I urge you to do so again also as a condition of the new 702 reauthorization.

In short, with every passing year, it is harder to square our emerging surveillance State with the consent of the governed articulated in the Declaration of Independence and embodied in your article of the Constitution, Article 1. With bipartisan cooperation that has come to define this Committee's work in this important area, I am confident that you can right the ship.

[The prepared statement of Mr. Schaerr follows:]

Statement of Gene Schaerr
General Counsel, Project for Privacy & Surveillance Accountability
and Managing Partner, Schaerr | Jaffe LLP

Before the House Judiciary Committee
Hearing on "Oversight of the Foreign Intelligence Surveillance Act"
Dec. 11, 2025

Chairman Jordan, Ranking Member Raskin, and members of the committee, thank you for holding this timely and important hearing on oversight of the Foreign Intelligence Surveillance Act (FISA).

As you know, a key FISA authority – Section 702 – is up for reauthorization in April. That authority, enacted by Congress to surveil foreign threats on foreign soil, has become a major means by which the federal government warrantlessly spies on American citizens on American soil. Where that program stands today, and what we know about its development into a major domestic spying tool, I will get to in a moment. But first I want to step back and explore what this development tells us – namely, that surveillance authorities tend to metastasize over time, moving from legitimate purposes to less legitimate ones.

The expansion of surveillance is driven in part by men and women in the Intelligence Community who are passionate about their mission to protect the American people and our homeland. Their patriotism and service deserve our appreciation. But surveillance expansion is also driven by the temptations of power created by increasingly robust technologies that increasingly allow agencies to peer into the lives of Americans.

It is for that reason that the last Section 702 reauthorization in 2024 became a wide-ranging debate over the growth of the surveillance state in America. That debate resulted in the passage of the Reforming Intelligence and Securing America Act (RISAA). RISAA was a great first step toward reform, but more is needed to guard against warrantless intrusions by government agencies into Americans' personal information and lives.

The Scope of the Surveillance State

Congress, appreciating how much is left undone, wisely put a two-year time frame on the 2024 Section 702 reauthorization. You thereby opted for a second opportunity to examine and correct the growing imbalance between government practice and Americans' constitutional rights and privacy interests.

Let us therefore briefly review four current Section 702 surveillance issues that require congressional attention if you, the People's representatives, are to prevent the creation of a full-blown American surveillance state.

- Despite the reforms of RISAA, Section 702 queries of Americans still do not require a warrant. Such queries enable government personnel to conduct "backdoor searches," circumventing the need for court approval before government agents seek out and read Americans' communications.

- Federal agencies, ranging from the FBI to the Department of Homeland Security to the IRS, routinely purchase Americans' sensitive personal digital information from shadowy data brokers. This data can include electronic records, communications metadata, web browsing activity, transaction and purchase records, online search, and many other forms of data that reveal Americans' most intimate beliefs, activities and associations. This data is far more personal than what can be gathered by hand, found in a diary, or pulled from a public website.

- Next is what I call the "make everyone a spy provision" in RISAA. The expanded Electronic Communications Service Provider (ECSP) provision, added in the eleventh hour during the last debate over surveillance in 2024, obligates providers of free Wi-Fi to customers to respond to secret requests by the National Security Agency for private communications. The law allows the government to force providers of office space to, among others, media, law firms, and political campaigns to facilitate warrantless surveillance of people

using their buildings' internet systems. There is nothing to prevent such spying from even being demanded of churches and other houses of worship.

- The addition over the years of amici to proceedings of the FISA Court also provides a much-needed window into civil liberties issues arising from the operations of that secret court. However, amici are still overly restricted in their ability to access critical materials and proceedings. There is also no amicus provision for FISA Title I surveillance, which can also turn a provision originally aimed at foreign threats into an authority for domestic spying.

That was most obviously true in the case of Carter Page, whom I am currently representing on appeal. As you know, he was illegally surveilled by the FBI as a means of spying on a presidential campaign and transition. The four warrants issued by the FISA Court to spy on Mr. Page – none of them examined by an amicus – were, as the Department of Justice Inspector General has established, predicated on a political opposition research document whose most lurid story turned out to be a bar joke. When the Court asked the FBI if Mr. Page had been an asset of the CIA – which he was – an FBI attorney submitted a forged document to the Court saying he was not.

Regardless of party, all members of Congress should be alarmed by this – by an Intelligence Community that asserts the right to interfere in a presidential election in such a dishonest and disingenuous way.

In addressing these four specific needs for FISA 702 reform, Congress should also bear in mind other important developments that are steadily contributing to the development of an American surveillance state.

- For example, when Americans travel through airports or malls, or even walk down a city sidewalk, we are subject to being identified and tracked by their faces. Cell-site simulators in geofenced areas also ping our phones to follow our movements. Our automobiles keep a record of every place we drive – and license plate readers create a database of our movements. Upon our return to U.S. international

airports, our digital devices are subject to having all their contents downloaded and inspected without a warrant.

- All this data generated from myriad sources can then be woven together by the power of artificial intelligence to comprehensively track where we go, who we meet with, what we say or share in private, and what we believe.

- As a result, federal agencies are capable of generating comprehensive political, religious, romantic, health, and personal dossiers on every American from information gathered without a warrant. That is as about as far from James Madison's Fourth Amendment as one can imagine. And it is an additional compelling reason to insist on meaningful Section 702 reforms.

RISAA's Reforms Were Not Enough

As I mentioned earlier, chief among the needed reforms is additional guardrails on warrantless "backdoor searches" of Americans' communications in the Section 702 database. The FBI in 2021 conducted more than 3 million of these searches, an astonishing abuse of a surveillance power that Congress designed for *foreign surveillance*, not warrantless surveillance of Americans.

Further, according to several FISA Court opinions, the FBI frequently has conducted those backdoor searches in politically sensitive cases. For example, in violation of its own rules, the FBI a short time ago illegally searched for communications of 19,000 donors to a congressional campaign, of multiple U.S. government officials, of journalists, of political commentators, of a local political party, of people who came to the FBI to perform repairs, of victims who approached the FBI to report crimes, of business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy," of college students participating in a "Collegiate Academy," of police officer candidates, of colleagues and relatives of FBI agents, and of Black Lives Matter and January 6 protesters.

Defenders of the status quo will claim that passage of RISAA closed the loopholes that allowed such abuses. And no doubt, on the whole, RISAA was an important and valuable step forward. Congress strengthened oversight and codified the rules and procedures the FBI itself had adopted in late 2021 and early 2022. These rules and procedures were meant to prevent the misuse of searches in sensitive cases that involve Americans' most basic civil rights and political expression.

Yet some of the most egregious improper queries *occurred after* the FBI's new rules were implemented. In April 2023, a FISC opinion revealed that the FBI in 2022 dipped into Section 702 data to warrantlessly spy on a United States Senator, a state senator, and a state judge who had the temerity to report suspected civil rights violations by a local police chief.

As these abuses continue, the legal foundation for warrantless searches of Americans is under challenge.

In 2024, a federal district court in New York ruled that the government violated the Fourth Amendment when it failed to obtain a warrant before it conducted such a "backdoor search" in a criminal case using data derived from Section 702.[1] But this is far from settled law. As we have seen repeatedly, a judicial ruling here or there has proven insufficient to deter warrantless searches.

And besides, protecting Americans' privacy is primarily the role of Congress, not the judicial branch. It will take Congressional action – making full use of the coming Section 702 debate – to achieve lasting reforms that protect Americans' privacy and curtail the growing surveillance state.

Section 702: What Remains to be Done

What, specifically, should Congress do now? Remember first that Congress originally intended Section 702 to be limited to the communications of foreigners, an appropriate authority in a time of geopolitical tension. But because Americans are often in communication

[1] *United States v. Agron Hasbajrami*, U.S. District Court for the Eastern District of New York, Dec. 2, 2024.

with people outside the United States, and because of the interconnected nature of global communications systems, surveillance under Section 702 inevitably sweeps up vast amounts of Americans' communications.

Absent Congress's mandating a warrant requirement for searches for Americans' communications in the 702 database, significant abuses will inevitably occur. We should be very concerned about any framework that allows the FBI to routinely search through Americans' communications without a warrant.

That isn't to say the warrant requirement must be absolute or inflexible. The Intelligence Community's own testimony during the last reauthorization offered only a few scenarios in which U.S. person queries – the warrantless searching of Americans' communications in the Section 702 database – had significant value. And the warrant rule proposed by this Committee included reasonable exceptions that would allow the government to act effectively in every exceptional circumstance.

Despite these reasonable compromises, the Intelligence Community is still obfuscating, perhaps in defiance of clear mandates from Congress. The DOJ Inspector General reports that, from December 2023 to November 2024, the number of U.S. person queries conducted by FBI personnel fell to 5,518 – from a high of more than 852,000 in 2019 to 2020.

That sounds like tremendous progress. But on page 49 of the Inspector General's report, the OIG notes that auditors found that the system's "advanced filter functions" may allow for searches of targets' communication without counting them as "queries."[2]

I recommend this as an area for further investigation on your part. As you do, keep in mind that the Intelligence Community cannot have it both ways.

- If the advanced filter function is disguising to a significant degree the actual number of U.S. person queries, then RISAA may not have made as much progress as we had hoped.

[2] https://oig.justice.gov/sites/default/files/reports/26-002_0.pdf

- If, on the other hand, the current reported number is close to the actual number of U.S. person queries, then a requirement for a probable cause warrant for such queries should be a light burden, especially with all the exceptions that were built into this Committee's last 702 reform proposal.

Either way, the facts argue for Congress to impose a clear probable cause warrant requirement for ordinary Section 702 queries of Americans.

Your Achievements

In so doing, you can build on prior successes. In the last Section 702 debate, for example, you demonstrated that it is possible to set guardrails to protect Americans' civil rights against surveillance abuses. You showed that reform is possible while also ensuring that agencies have the ability to track and respond to genuine threats. In fact, on a nearly unanimous, bipartisan basis, this Committee marked up and approved the strongest surveillance reform legislation that we have seen in over a generation—showing your dedication and resolve to protect Americans' civil liberties.

While this Committee's bill was not ultimately adopted by the full Congress, it is still inspiring to consider what the 118th Congress did accomplish on surveillance reform:

- In the 118th Congress, you mandated that the FBI produce quarterly reports on the number of U.S. person queries conducted under Section 702, giving Congress real-time guidance.

- You cracked open the door of the Foreign Intelligence Surveillance Court to your oversight, allowing key Members with oversight responsibility to sit in on hearings – although we understand that provision may need to be strengthened further.

- You shortened the reauthorization of Section 702 from five to two years.

- And on the House floor, you came within a single vote – on a 212-212 tie – of requiring a warrant for the government to search Americans' communications in the Section 702 database.

Finally, last Congress the House also took a significant step in passing a measure to require warrants when federal agents purchase and inspect Americans' most intimate digital data – including their geolocation, internet search history, and online communications – sold to the government by data brokers with no regard for Americans' Fourth Amendment right to privacy.

Although these two warrant requirements did not ultimately become law, the progress made last Congress was a significant achievement, and we applaud this Committee for working to build on last year's strong bipartisan efforts to protect Americans' civil rights.

What You Can Achieve in 2026

Each of these reforms can be passed by this Committee and by Congress in 2026.

- You can take the lead by passing a warrant requirement for Section 702 searches of US persons' communications.

- You can also add a warrant requirement to the federal government's purchase and review of Americans' sensitive personal data.

- You can curb the definition of "electronic communication service provider" under FISA to exclude houses of worship and countless small businesses from being forced by the NSA to assist in spying on congregants and customers.

    - On that point: It has been widely reported in the media – and suggested on the floor of the United States Senate – that the dramatic expansion last year of the definition of "electronic communication service provider" was enacted in order to cover

data centers. We urge you to appropriately tailor the definition to achieve that purpose, but to go no further.

- Beyond that, you can require amici participation in sensitive political FISA cases by including the so-called "Lee-Leahy Amendment" in next year's reauthorization. – which mandates the inclusion of a qualified civil liberties expert holding a high-level clearance to advise the secret FISA courts. This measure, which passed the Senate in 2020 with 77 votes, would go a long way to preventing the types of abuses that occurred in 2016 when the Trump campaign and transition was illegally spied based on improper FISA warrants that issued as a result of the FBI's lies. The measure is popular because it makes so much sense to have at least one advocate for civil liberties in these secret hearings.

As you reform these practices, you can rest assured that the American people are behind you. A YouGov poll from 2023 shows that 76 percent of Americans support a warrant requirement for government inspection of Americans' international communications. Eighty percent believe Congress should pass a law requiring a warrant before the government can purchase and access our digital data. As the debate on the reauthorization of Section 702 begins, you can speak and act with confidence, knowing that your constituents will be strongly on your side.

Expect Intelligence Community Curveballs

In approaching this debate, please also understand just how hard the Intelligence Community will work not just to stop future reforms, but to derail the reforms you've already made.

To cite one example, consider the RISAA reform that allows select Members of Congress and designated staff to attend the secret FISA hearings. This was intended to enhance oversight of the FISA courts and to put a check on judges who have sometimes shown astonishing naiveté in accepting the FBI's assurances at face value.

A recent development in this story, however, shows just tricky it can be to deal with the Intelligence Community. Your Senate counterparts, Chairman Chuck Grassley and Ranking Member Dick Durbin, have publicly challenged Department of Justice rules setting limits on what you can access in FISC proceedings. The new DOJ procedures:

- Prohibit you from sharing information from these hearings with other Members or your cleared staff.
- Restrict you from requesting information or documentation from FISC proceedings.
- Allow DOJ staff to remove you from FISC proceedings for any reason.
- Prohibit you from bringing your designated staff member with you.
- Prohibit note-taking.

These measures mean that, if you attend a secret hearing and learn something that you want to discuss with another Member who had a right to attend the hearing, you will instead be effectively gagged from discussing it with each other or with any of your staff, regardless of security clearance or whether that discussion takes place in a SCIF.

So give them credit – DOJ found a way to turn your oversight and accountability measure into yet another mechanism for silencing you. But I am sure you agree that it is *Congress* that should spell out the rules for your access to oversight, not the very bureaucrats you oversee.

Along similar lines, it has recently come to light that former Special Counsel Jack Smith relied, not on a probable cause warrant, but on a grand jury subpoena, to examine the telephone metadata of eight U.S. Senators and one Member of this House. That is the very definition of a fishing expedition – one in which even Members of Congress are subject to exploratory

spying without the pretense of probable cause. And it should not be allowed.

Expect too to hear whispers that, if you press too hard for reform, you will be setting yourselves up to be responsible for the next 9/11. That is nonsense. As the 9/11 Commission report found, the nation's greatest modern intelligence failure resulted from an inability of siloed intelligence agencies to connect dots that had already been lawfully obtained. The reforms I have discussed today need not result in any such siloing of insights or information. We can protect our constitutional right to privacy while taking great care to make sure the Intelligence Community retains the exceptions and authorities it needs to keep America safe.

Conclusion

In sum: Revulsion at government surveillance runs deep in our DNA as a nation; indeed, it was one of the main factors that led to our revolt against British rule and, later, to our Bill of Rights. Agents of the Crown could break into a warehouse or a home to inspect bills of lading or secret political documents, but they couldn't access anything close to the wealth of private information reflect in our digital lives today.

Month by month, it is harder to square this emerging surveillance state with the "consent of the governed" concept articulated in the Declaration of Independence and embodied in Article I of the Constitution. The Founders believed that American citizens should not be subject to surveillance by their own government without their consent – in the form of a statute duly enacted by their representatives in Congress. They should not be subject to surveillance at the whim of any executive official, none of whom has authority to consent to surveillance on their behalf.

But decades of neglect and dismissal have tarnished that inheritance with intelligence practices that are self-justifying and self-serving. We look forward with hope that you will restore, protect, and burnish these privacy-protecting traditions of a free people.

Chair JORDAN. Thank you, Mr. Schaerr. Mr. Czerniawski, you are recognized.

STATEMENT OF JAMES CZERNIAWSKI

Mr. CZERNIAWSKI. Thank you, Mr. Chair, Ranking Member Raskin, and the Members of the Judiciary Committee for holding this critical hearing on the Foreign Intelligence Surveillance Act. Our Founding Fathers enshrined individual liberty and privacy as bedrock ideals of our Constitution, yet over the years, we have seen a surveillance State that only continues to expand, operating with limited accountability, all under the guise of national security. National security is vital and few would deny the many dangers facing our great Nation today. I would know firsthand growing up in Queens, New York, and experiencing the terrible events and aftermath of 9/11, a tragic day that showed us the cost of being unprepared, but also demonstrated just how quickly extraordinary powers, once granted, can become normalized.

History warns us of the dangers of unchecked government power. Time and time again, we have caught the intelligence community raiding the civil liberties fridge, taking liberties that were supposed to be off limits; apologizing barely when they are caught, if we are lucky; promising to never do it again, and then returning to business as usual. It would be humorous if the consequences to Americans' rights were not so serious. Too often, agencies appear more concerned with managing bad headlines than safeguarding the privacy and rights of the people they were created to serve and protect. This repeated cycle of violations has resulted in an erosion of public trust in the very institutions charged with keeping Americans safe.

In December 2024, *CNN*'s Harry Enten cited Gallup polling showing that support for the FBI, in particular, was at an all-time low with just 41 percent of respondents saying that the agency was doing either an excellent or a great job. That represented an 18 percent drop in just 10 years. That is a damning indictment against the key agency responsible for keeping Americans safe.

An intelligents apparatus that lacks the public trust become less effective, not more. Americans are less likely to cooperate with, have support for, or believe in institutions that they fear and that is precisely why reforms are not optional, they are urgently needed.

Congress has the responsibility to restore the balance and when it comes to addressing the litany of issues under FISA, there are many out there in terms of solutions, but here are four key reforms that Congress should prioritize.

First, close the backdoor search loophole that allows for warrantless searches of Americans' communications.

Second, close the data-broker loophole which lets agencies buy their way out of constitutional constraint.

Third, strengthen third-party oversight at the FISA Court. Improving due process and casting sunlight on decisions too often made in darkness and secrecy.

Fourth, fix the overly expansive definition of an electronic communication service provider, a definition that dangerously brought in the kinds of entities that can be deputized into the surveillance apparatus, a recent issue stemming from FISA's reauthorization

under the Reforming Intelligence and Security America Act, also known as RISA.

These reforms that I highlighted here today will not end surveillance nor will they prevent legitimate national security operations. The country will not go dark, nor will it find itself defenseless against foreign threats, but what they will do is ensure that Americans' rights are not flagrantly disregarded in the process of carrying out those duties. The Constitution is not simply a piece of parchment to be admired. This is a moment to prove that America's strength lies not only in its defenses, but in its devotion to liberty. Let us stand firm so that freedom is not just promised, but practiced.

As the Committee with primary jurisdiction, you have the power to shape policy that balances security, freedom, and by advancing meaningful reforms, you can restore public trust, safeguard rights, and ensure that our intelligence agencies serve the American people, not surveil them. Thank you for the opportunity to share our thoughts with you today. I look forward to the conversation and to answering your questions.

[The prepared statement of Mr. Czerniawski follows:]

CONSUMER CHOICE CENTER

Oversight of The Foreign Intelligence Surveillance Act

JAMES CZERNIAWSKI, Head of Emerging Tech Policy, Consumer Choice Center

Committee on the Judiciary

U.S. House of Representatives

December 11th, 2025

Dear Chair Jordan, Ranking Member Raskin, and Members of the Committee:

On behalf of the Consumer Choice Center, I thank you for the opportunity to provide our view on the increasingly invasive nature of government surveillance of U.S. citizens. In a nation founded on liberty and limited government, the expanding surveillance state is one of the greatest threats to individual freedom. Under the banner of national security, the federal government has exceeded its constitutional limits, empowering and emboldening a national security apparatus that has engaged in warrantless surveillance of Americans with little meaningful accountability. What began as a counterterrorism program has morphed into a surveillance apparatus that erodes privacy, chills free speech, and undermines faith in the very institutions of government charged with protecting Americans.

Years of numerous documented abuses, coupled with a lack of accountability, have deepened the erosion of trust between citizens and their government. At the Consumer Choice Center, we believe national security and constitutionally protected rights are not mutually exclusive. Protecting the nation must never come at the expense of personal liberties. Encouragingly, Congress is approaching this issue in a bipartisan manner, correctly recognizing that the government's overreaches on surveillance affects all Americans, regardless of their political affiliation. We hope this hearing serves as a launchpad, leveraging the opportunity to work on bipartisan legislative solutions that properly balance national security interests while safeguarding civil liberties.

CONSUMER CHOICE CENTER

I. Foreign Intelligence Surveillance Act (FISA) and the Need for Reform

Congress originally passed the Foreign Intelligence Surveillance Act (FISA) in 1978 in response to findings of the select committee to investigate federal intelligence operations, led by Senator Frank Church, which uncovered rampant abuses by the FBI, CIA, NSA, and IRS, including surveillance of civil rights leaders, journalists, and political activists.[1] The Committee's investigations revealed how agencies had operated with little oversight, often violating constitutional rights under the guise of national security. To address these abuses, FISA established a statutory framework for electronic surveillance and created the Foreign Intelligence Surveillance Court to review government applications targeting foreign powers or agents inside the United States.

Over time, Congress amended FISA to expand the government's surveillance toolkit. For example, in the 1990s, new provisions authorized physical searches and electronic surveillance. Additionally, after the terrible attacks on September 11th, 2001, the USA PATRIOT Act further broadened FISA authorities, including "roving" wiretaps and access to "any tangible thing", significantly lowering the threshold required for government collection in the process.[2] These expansions reflected the government's growing reliance on electronic surveillance but also raised concerns surrounding the erosion of privacy and the adequacy of judicial oversight.

In recognition of these concerns, Congress established the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency responsible for ensuring that counterterrorism programs respect the constitutional rights of Americans. The PCLOB has played a critical role in reviewing surveillance authorities, including Section 702, and has issued reports that highlight both the national security value of these programs and the risks they pose to Americans' privacy. The very creation of PCLOB was a reminder that liberty must always be a coequal partner to security.

Passed in 2008, Section 702 of the Foreign Surveillance Act expanded the government's authority to conduct warrantless surveillance of suspected

---

[1] United States Senate. "Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities." U.S. Senate: Powers and Procedures - Investigations, https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm

[2] Liu, Edward C. "Congressional Oversight of Intelligence: Current Structrure and Alternatives." Congressional Research Service, April 11, 2016. https://www.congress.gov/crs_external_products/R/PDF/R40138/R40138.23.pdf

foreign terrorists. While this may appear to be a reasonable national security measure, its implementation has repeatedly blurred the line between foreign and domestic surveillance. In practice, Section 702 has become a go-to resource for the government to access Americans' communications without the proper protections of a warrant. For instance, in 2022 alone, the Federal Bureau of Investigation (FBI) conducted 200,000 warrantless searches of the communications of American citizens using the Section 702 data.[3]

The FISA Court revealed troubling examples of misuse: improper queries targeting individuals present at the Capitol on January 6th, 2021; surveillance of Black Lives Matter protestors in the summer of 2020[4]; the collection of information on 19,000 donors to a congressional campaign[5]; and even the targeting of elected officials, including a sitting U.S. Senator.[6] These actions fall far outside Section 702's intended purpose of monitoring foreigners abroad and strike at the core of the Fourth Amendment and our fundamental natural rights.

Rather than instituting meaningful guardrails to ensure compliance, intelligence agencies have failed to prioritize privacy in their reforms. In 2023, instead of addressing substantive concerns, agencies issued a report describing changes to their methodology designed to reduce the reported number of queries.[7] In effect, they appear more focused on managing headlines than on protecting Americans' privacy and constitutional rights against government overreach and tyranny.

A. The Conversation of Reform

Some proponents of surveillance reform would argue that Congress should let Section 702 authorities expire; however, we believe that would be a grave mistake. In 2020, Congress permitted Section 215 of the PATRIOT Act to sunset after failing to reach consensus on necessary reforms. Yet this did not halt intelligence agencies from conducting similar surveillance.

---

[3] Office of the Director of National Intelligence. Annual, having failed Statistical Transparency Report Regarding the Use of National Security Authorities: Calendar Year 2022. 2023, https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.

[4] Sterling, Toby. FBI Misused Intelligence Database in 278,000 Searches, Court Says. Reuters, 19 May 2023, https://www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/.

[5] Foreign Intelligence Surveillance Court. 2021 FISC Certification Opinion. 2021, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opi nion.pdf.

[6] Carney, Jordain. "FBI Analyst Improperly Searched Surveillance Data for U.S. Senator's Name - Politico." Politico, 21 July 2023, www.politico.com/news/2023/07/21/fbi-surveillance-dat,a-senators-name-00107621.

[7] https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf

Instead, they continued such activities under other surveillance authorities, such as Executive Order 12333, a worse outcome, as it lacks the statutory transparency and congressional oversight that Section 215 provided.

During the most recent debate surrounding Section 702, Congress first granted a short-term extension in December 2023 by attaching it to the must-pass National Defense Authorization Act[8]. Ultimately, lawmakers reauthorized the authority under H.R. 7888, the Reforming Intelligence and Securing America Act (RISAA).[9] Supporters of this "solution" claimed the bill contained meaningful reforms, but in reality, it offered little substantive change while dangerously expanding surveillance powers by broadening the definition of an electronic communications service provider (ECSP).[10]

Those so-called reforms largely codified internal guidelines from the FBI. Yet analysis from the Center for Democracy and Technology revealed that the FBI conducted an estimated 4,000 queries in violation of those very guidelines, underscoring how inadequate that standard is.[11]

One of the most controversial components of RISAA was the expanded definition of an ECSP. The change poses a significant risk by sweeping in companies and organizations far beyond traditional telecommunications carriers or internet service providers. Under prior law, the ECSP definition was relatively narrow, applying to entities directly involved in transmitting or storing communications. RISAA's reauthorization, however, expanded that definition to cover a wider range of service providers, including companies that merely provide access to communications infrastructure or related services.[12]

In practice, this could mean that cloud service providers, data centers, or even businesses tangentially connected to communications networks could be compelled to assist in surveillance activities. By expanding the universe of entities captured under Section 702, RISAA created a far larger surveillance

---

[8] Foran, Clair, Fox, Lauren, Grayer, Annie and Haley Talbot. "Defense Policy bill includes short-term extension of controversial government surveillance program". CNN. December 7, 2023. https://www.cnn.com/2023/12/07/politics/ndaa-fisa-extension/index.html

[9] U.S. Congress. (2024). H.R. 7888 – Reforming Intelligence and Securing America Act. 118th Congress. Retrieved from https://www.congress.gov/bill/118th-congress/house-bill/7888/text

[10] Id.

[11] Laperruque, Jake. "Requiring a Warrant for U.S. Person Queries Is Critical for FISA 702 Legislation." Center for Democracy & Technology. 25 Mar. 2024, https://cdt.org/insights/requiring-a-warrant-for-u-s-person-queries-is-critical-for-fisa-702-legislation/.

[12] Miller, John. "Expansion of FISA Electronic Communications Service Provider Definition Must Be Removed." Information Technology Industry Council, 2024. https://www.itic.org/news-events/techwonk-blog/expansion-of-fisa-electronic-communications-service-provider-definition-must-be-removed

dragnet, one that touches companies never before considered part of the intelligence collection process.[13]

The danger this creates is two-fold. First, it increases the number of potential entry points through which the government can access Americans' communications, raising the likelihood of overcollection and misuse. Second, it erodes transparency and accountability, given that many of these newly covered entities lack the statutory oversight mechanisms traditionally applied to telecommunications carriers. One could argue that the definitional expansion would effectively deputize a wide swath of private industry into the surveillance apparatus without adequate safeguards to protect civil liberties and constitutional protections.

Although Senator Mark Warner pledged to work with colleagues to narrow the ECSP definition[14], the most recent attempt to do so in the Intelligence Authorization Act was ultimately stripped out.[15]

This debate is not occurring in a vacuum.

Even as Congress wrestles with how to rein in warrantless surveillance under Section 702, some voices have urged the intelligence community to "modernize" by leveraging new technology and open-source data more aggressively.[16] Modernization in itself is not objectionable. In fact, modernization driven by technological innovation can strengthen national security when paired with accountability. However, without sufficient guardrails, those efforts of modernization become a vehicle for expanding surveillance of Americans in ways that directly undermine the Fourth Amendment.

Commercially available information, whether location data, internet records, or even genetic data, is no less sensitive simply because it's sold by private actors. Treating this data as "fair game" for government collection without a warrant would amount to a massive expansion of surveillance powers, deputizing technology as a tool for constitutional violations under the guise of improvements to agency operations.

---

[13] Restore the Fourth. "Scope of FISA Sec. 702 ECSP Provision Narrowed but Remains Classified." Restore the Fourth, 2024. https://restorethe4th.com/scope-of-fisa-sec-702-ecsp-provision-narrowed-but-remains-classified/

[14] https://www.congress.gov/118/crec/2024/04/18/170/68/CREC-2024-04-18-pt1-PgS2837.pdf

[15] Matishak, Martin. "No FISA fix in annual intelligence policy bill approved by House panel". The Record. June 12th, 2024. https://therecord.media/house-intel-committee-politicalapproves-bill

[16] Steube, Greg . ""U.S. intelligence is sitting Idly by - it's time for an intervention." The Washington Times, September 9, 2025. https://www.washingtontimes.com/news/2025/sep/9/us-intelligence-sitting-idly/

The problem isn't that the intelligence community lacks access to information; the problem is that it has repeatedly abused the authorities it already possesses with near impunity to access sensitive databases for information on Americans.

Calls to modernize by leveraging open-source intelligence or commercially available information in datasets must be scrutinized. Agencies should be encouraged to adapt and innovate; however, Congress must ensure that modernization is accompanied by strong safeguards that respect the rights of American citizens. Otherwise, "modernization" becomes a euphemism for unchecked expansion of surveillance, compounding the very abuses that have eroded public trust. That very erosion of trust is precisely why this committee is convened today, to confront the failures of Section 702 and to chart a path towards reforms that restore both accountability and confidence in our intelligence agencies.

We believe that Congress made meaningful progress in recognizing the need for reforms to surveillance authorities, and that this momentum positions lawmakers to secure serious, lasting reforms during the upcoming FISA reauthorization in 2026. While there are many potential avenues for reform, here are several key priorities that deserve particular focus:

Closing the backdoor search loophole

The backdoor search loophole allows intelligence agencies such as the CIA, FBI, and NSA to access Section 702 databases, intended solely for targeting non-U.S. persons located overseas, to review Americans' phone calls, text messages, and emails. Such practices directly undermine the Fourth Amendment rights of U.S. citizens. These searches have already been abused to monitor individuals across the political spectrum. According to polling by Demand Progress and FreedomWorks, 76% of Americans believe that government agencies should "obtain warrants before intentionally searching international communications obtained without a warrant for conversations involving people in the US."[17]

During the last reauthorization debate, amendments were introduced to strike a balance between legitimate security needs and civil liberties. These proposals included exceptions for exigent circumstances, certain cybersecurity-related queries, and consent-based queries performed to identify or assist potential victims. Importantly, warrant requirements

[17] https://demandprogresseducationfund.org/new-polling-as-mass-surveillance-debate-reaches-final-stages-in-congress-americans-demonstrate-overwhelming-support-for-increased-privacy-protections/.

would not apply to metadata searches, preserving the FBI's ability to determine whether U.S. persons are in contact with foreign targets.

Closing the Data Broker Loophole

Congress should also prevent the government from bypassing constitutional protections by purchasing Americans' personal data from private actors without a warrant. Such practices allow law enforcement to exploit sensitive information tied to constitutionally protected activities, subjecting individuals to further surveillance through other technologies. Coupled with the backdoor search loophole, these end-runs around the Fourth Amendment chill free speech by making millions of Americans fear unwarranted government monitoring.

Public opinion strongly supports reforms in this area. The same polling found that 80% of Americans agree that government agencies should "obtain warrants before purchasing location information, internet records, and other sensitive data about people in the U.S. from data brokers."[18] The Fourth Amendment is Not for Sale Act, which passed the House in the last Congress, offers a concrete solution to this precise problem.

Strengthening third-party oversight at the FISA Court

Congress should expand the role of neutral, third-party attorneys – or amici – within the FISA Court proceedings whenever Americans' rights are at stake. FISA Court judges should be required to appoint amicus curiae to cases involving "sensitive investigative matters," unless doing so would jeopardize an ongoing investigation or reveal sensitive methods.

Furthermore, an amicus should be able to raise issues with the FISA Court at any time and give both the court and the amicus access to documents and information related to the surveillance application.

These reforms would significantly improve due process and strengthen civil liberties protections for Americans in the courts by ensuring surveillance decisions are not made entirely in secret without counterarguments or checks. Congress has considered this issue before: the Senate overwhelmingly adopted the Lee-Leahy amendment to the USA Freedom Act by a strong bipartisan vote of 77-

[18] Id.

19. More recently, the Government Surveillance Reform Act included a section based on that very amendment.

These reforms would not eliminate surveillance authorities or prevent their use in protecting national security. Instead, they would ensure that the rights of American citizens are safeguarded, preventing constitutional protections from being trampled on in the process.

II. Government's Use of Technology for Surveillance

The government has long relied on technology to support its mission of public safety. In the hands of law enforcement, technology can be a powerful tool for crime prevention, investigation, and response. Yet without the proper guardrails, these tools are vulnerable to abuse, undermining public trust and working against the very mission of safety they are meant to serve.

Facial recognition technology illustrates this tension clearly. While it can provide benefits in commercial settings, its use by the government raises serious concerns.

Though the technology dates back to the 1960s, when Woodrow Bledsoe developed a semi-automated system to analyze facial features[19], advances in the years since have made it far more powerful. Still, it remains imperfect and can place innocent people in the crosshairs of law enforcement.

A federal study in 2019 showed that Asian and African American individuals were up to 100 times more likely to be misidentified than white men, depending on the algorithm and what type of search was conducted. According to that same study, Native Americans had the highest false positive rate of all ethnicities.[20]

The case of Robert Williams in Detroit demonstrates the human costs of such errors. In January of 2020, police used facial recognition technology on low-quality video from security cameras in the store, which produced Mr. Williams' name. Police admitted that their use of facial recognition technology was what prompted them to arrest Williams. Ultimately, the charges against Williams were dropped, but not before he had spent 30

[19] Jeremy Norman. "Woodrow Bledsoe Originates of Automated Facial Recognition." Jeremy Norman's History of Information. December 30, 2020. http://www.historyofinformation.com/detail.php?entryid=2495.

[20] Drew Harwell. "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use." Washington Post. December 19, 2019. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

hours in jail and had to make bail for a crime he didn't commit.[21] Congress should continue to work to explore ways to implement common-sense restrictions around the use of such technologies by law enforcement while still allowing the technology to develop so that it can be an effective tool to advance public safety in the future.

While Artificial Intelligence is a relatively new topic of discussion in Congress, its use cases in this space aren't exactly new. The intelligence community has leveraged artificial intelligence in its surveillance practices to help analysts sift through the vast amounts of intercepted communications.[22]

Predictive Policing, which uses machine learning algorithms to forecast where and when crimes may occur, has proven especially controversial. In Florida, one such program came under fire after investigative reporting revealed how the program being utilized there led to months of harassment under the guise of a "prolific offender check".[23] Investigative reporting revealed the repeated constitutional violations, prompting a lawsuit by the Institute for Justice. The county ultimately settled, admitting the program's repeated constitutional violations.[24]

Congress should ensure strong guardrails around law enforcement's use of AI and predictive policing, and work with state lawmakers to promote similar protections at the local level.

Lastly, recent revelations around the bankruptcy announcement for 23andMe present interesting questions about biometric privacy.[25] The announcement sent shockwaves through the ecosystem, driving a surge in website traffic as customers rushed to the website looking for details around deleting data and closing their accounts.[26] The company has roughly 15

---

[21] Bobby Allyn. "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest of Black Man." NPR. June 24, 2020. https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

[22] Christopher R Moran, Joe Burton, George Christou, The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying, Journal of Global Security Studies, Volume 8, Issue 2, June 2023, ogad005, https://doi.org/10.1093/jogss/ogad005

[23] McGrory, Kathleen, et al. "A Futuristic Data Policing Program Is Harassing Pasco County Families." Pasco's Sheriff Created a Futuristic Program to Stop Crime before It Happens. It Monitors and Harasses Families. | Investigations | Tampa Bay Times. https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/

[24] Institute for Justice. Case Closed: Pasco Sheriff Admits Predictive Policing Program Violated Constitution. 22 Feb. 2023, https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution/.

[25] 23andMe. Questions Related to 23andMe's Chapter 11 Filing. March 26, 2025. https://customercare.23andme.com/hc/en-us/articles/30805135934615-Questions-related-to-23andMe-s-Chapter-11-Filing.

million customers around the globe.[27]

FTC Chair Andrew Ferguson understands some of the privacy concerns presented here, issuing a letter stating that the promises made by 23andMe must be kept by whoever ultimately purchases that information.[28] However, there is a risk that the sensitive type of data held by 23andMe could potentially get funneled to the government via the data broker loophole, allowing for a massive expansion of genetic surveillance to empower governments to go on what amounts to a genetic fishing expedition. At a minimum, it's definitely a topic that the committee should potentially explore.

III. Conclusion

Keeping Americans safe is a goal we deeply support. We live in a dangerous world, and there are adversaries who seek to do harm against the United States. We deeply respect and appreciate the dedicated men and women in our intelligence agencies who work tirelessly to protect us from those threats. Yet public safety must never come at the expense of the very freedoms it is meant to defend. Protecting constitutional rights and safeguarding national security are not opposing missions. They are inseparable obligations.

We appreciate the work of the Judiciary Committee and the subcommittee earlier this year to pursue the critical and needed reforms to curb the unchecked surveillance of U.S. citizens. Last year's strong bipartisan efforts set a powerful precedent, reflecting the overwhelming demand from both lawmakers and the American people for strong privacy protections against government overreach. That momentum MUST continue.

The task before us is clear: to work together and ensure that liberty and national security advance together, rather than being at odds. We stand ready to work with you and your colleagues to secure reforms that honor both our safety and our rights. As this Congress takes up the challenge, we look forward to answering your questions and joining you in the effort to ensure that America remains both secure and free.

---

[26] Williams, Kevin. "23andMe bankruptcy: With America's DNA put on sale, market panic gets a new twist." CNBC.com. March 30, 2025. https://www.cnbc.com/2025/03/30/23andme-bankruptcy-selling-deleting-dna-genetic-testing.html

[27] Id.

[28] Ferguson, Andrew. "Re: In re 23andMe Holding Co., et al., Case No. 25-40976, United States Bankruptcy Court for the Eastern District of Missouri (Eastern Division)." Federal Trade Commission. March 31, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/23andme-letter-ferguson.pdf

Chair JORDAN. Thank you, Mr. Czerniawski. Ms. Goitein, you are recognized for five minutes.

STATEMENT OF ELIZABETH GOITEIN

Ms. GOITEIN. Chair Jordan, Ranking Member Raskin, and the Members of the Committee, thank you for this opportunity to testify. Congress conceived and enacted Section 702 as a foreign terrorist surveillance program. Over the last 17 years, it has become something very different. Today, Section 702 is a rich source of warrantless access to Americans' communications. It is long past time for Congress to put an end to this betrayal of Americans' trust.

Section 702 authorizes the government to target any foreigner overseas for foreign intelligence purposes and to collect all their communications without an individualized court order. This surveillance inevitably sweeps in Americans' communications in large amounts because Americans communicate with foreigners and because those foreigners need not be suspected of any wrongdoing, these communications can and do include purely innocent conversations between Americans and their friends, family members, and colleagues overseas, a point that was emphasized by the Privacy and Civil Liberties Oversight Board in its 2023 report.

Now, if the government's intent were to spy on those Americans, it would have to get a probable cause order, a warrant in a criminal investigation, or a FISA Title I order in a foreign intelligence investigation. The government gets around this requirement by certifying to the FISA Court that it is not using Section 702 as a way to access the communications of particular known Americans. Yet, once the data is in their hands, all of the agencies that receive Section 702 data routinely run warrantless electronic searches for the communications of particular known Americans. This is a bait and switch that drives a massive hole through the Fourth Amendment and FISA.

In 2023, the year for which we have complete data, the FBI conducted more than 57,000 of these backdoor searches. Congress and the FISA Court have attempted to put some limits on this practice, but the FBI has engaged in persistent and widespread violations of those limits according to the FISA Court. Those violations have included searches for the communications of Members of Congress and congressional staffers, protesters from across the political spectrum, multiple U.S. Government officials, journalists and political commentators, and more than 19,000 donors to a congressional campaign.

In April of last year, Congress passed the Reforming Intelligence and Security America Act which sought to rein in the FBI's backdoor searches largely by bolstering internal oversight and reporting mechanisms. We don't know what the impact of these reforms has been, however, because the FBI failed to track all its queries as required by law. Specifically, last August, the Justice Department discovered that the FBI was using a tool to search for the communications of specific individuals, including U.S. persons from among a particular target's communication. The FBI did not count these as queries. It didn't follow any of the procedures required by law

such as obtaining attorney approval or providing a written justification for U.S. person queries.

The government told the FISA Court that it lacks the information to determine whether there was a sufficient legal basis for these queries. As a result, we have no idea how many queries the FBI conducted in 2024. The number that appears in the annual statistical report is 5,518. That is the number of known queries, the queries that the FBI actually counted. The total number of queries remains unknown as does the FBI's compliance rate. This is important information and Congress should have it before it reauthorizes Section 702. Let me be clear, even if the FBI conducted only 5,000 warrantless searches for Americans' emails, text messages, and phone calls last year, that would be 5,000 too many. Warrantless access to Americans' private communications is an invitation to government over reach and abuse under any administration.

All the internal oversight in the world cannot substitute for the balance that the Framers struck in the Fourth Amendment. As Justice Roberts said in a 2014 case about the privacy of our cell phones, "The Founders did not fight a Revolution to gain the right to government agency protocol." Congress must do now what it should have done years ago, require the government to get a warrant or a FISA Title 1 order before accessing Americans' communications obtained under Section 702. Thank you, and I look forward to your questions.

[The prepared statement of Ms. Goitein follows:]

TESTIMONY OF

ELIZABETH GOITEIN
SENIOR DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY

HEARING ON

OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

DECEMBER 11, 2025

Introduction

Section 702 of the Foreign Intelligence Surveillance Act ("FISA") allows the government to target foreigners abroad and obtain their communications and other personal information without obtaining an individualized court order. Congress passed the law in 2008 to give our government more powerful tools to address international terrorism and other foreign threats. Consistent with this purpose, the law has been used (according to the government) to obtain information about terrorist plots and the intentions of hostile foreign powers, and — more recently — to gain insight into international drug trafficking activities and investigate foreign threats to cybersecurity.

Needless to say, these activities are not why Section 702 has become so deeply controversial, leading many lawmakers to demand either sunset or reform. If the government were using Section 702 solely to spy on hostile foreign actors, there would be little to debate in next year's reauthorization. The fundamental problem with Section 702 is that the government is also using it as a rich source of warrantless access to *Americans*' communications. According to the Office of the Director of National Intelligence ("ODNI"), the government conducted more than thirteen thousand *known* searches of Section 702 data in 2024 for the purpose of finding Americans' communications and other personal information — though the FBI's failure to track all of its searches means that the actual number may be much higher. This outcome is contrary not only to the original intent of Section 702 and to basic Fourth Amendment principles, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms.

Recent changes to Section 702 have heightened the program's impact on Americans' privacy. The Reforming Intelligence and Securing America Act ("RISAA"), enacted in April 2024, authorized the government to compel surveillance assistance from a dizzying range of U.S. companies and organizations, vastly expanding the potential reach of Section 702 surveillance. The Foreign Intelligence Surveillance Court ("FISA Court") also recently approved the government's request to collect data related to international narcotics trafficking — collection that the Court acknowledged is likely to result in acquisition of a larger volume of Americans' communications. Additionally, RISAA authorized entirely suspicionless searches of Section 702 data for the purpose of vetting individuals seeking to travel to the United States, increasing the number of overall searches that in turn risk retrieving Americans' data for review.

Moreover, since the inception of the program, the rules designed to protect Americans' privacy have been honored in the breach. Agencies have repeatedly, and in some cases systemically, violated statutory or court-ordered limitations on collection, retention, querying, and dissemination. Some of these violations have rendered the operation of the program unconstitutional. Breaches in recent years have involved baseless searches for the communications of protesters, journalists, campaign contributors, and members of Congress. Between 2018 and 2024, Section 702 required the FBI to obtain a warrant before accessing Section 702 data about Americans in a subset of criminal investigations; over the six years this requirement was in place, the FBI *never* complied with it.

Since RISAA was passed, FISA Court opinions and a Department of Justice Office of Inspector General ("OIG") report suggest that the rate of violations by the FBI has decreased.

However, OIG cautions that it is much too soon to conclude that the pattern of violations is in the past. More fundamentally, there is an enormous caveat to these bodies' findings. For one of the methods it was using to search Section 702 data, the FBI failed to follow the procedural requirements mandated by law, including the requirements to obtain attorney approval and record the factual basis for searches that target U.S. persons. Because the government did not track or audit these queries, the number of U.S. person searches and the rate of violations that took place when FBI agents used this method remain unknown.

Congress should not reauthorize Section 702 without sweeping reforms to ensure that it cannot be used as a domestic spying tool. At a minimum, that means closing the backdoor search loophole that enables government officials to access Americans' phone calls, text messages, and emails without a warrant. It also means walking back RISAA's radical expansion of the types of U.S. entities that may be obligated to assist in the government's Section 702 surveillance; ending suspicionless travel-vetting queries; strengthening Section 702's reverse-targeting and minimization requirements; and right-sizing the scope of Section 702 surveillance targets.

Addressing the problems with Section 702 will also necessitate reforms to FISA more generally, starting with its judicial review provisions. Despite changes that Congress made in 2015, the FISA Court still hears only from the government in too many cases. RISAA compounded the problem by limiting the issues *amici curiae* are permitted to address and weighting *amici* selection towards former government personnel. Congress must strengthen *amici* participation at the FISA Court — and other mechanisms for judicial review — to ensure that there is meaningful oversight of the government's surveillance.

Finally, it is critical to recognize Section 702 as one authority within an ecosystem of often-overlapping surveillance authorities, many of which contain gaps and loopholes that are increasingly allowing warrantless access to Americans' most sensitive information. Reform of any single statute, on its own, is unlikely to make a serious dent in the broader problem: the government could evade any new restrictions by using other, more permissive authorities — or, in some cases, by simply purchasing the information from data brokers. Moreover, Section 702 is one of the few surveillance authorities that includes a sunset. Congress should thus view the expiration of Section 702 next year as a rare and vital opportunity to reverse the broader drift, in the law and in practice, toward warrantless surveillance.

I. History and Design of Section 702

Congress passed FISA in 1978 following revelations that the government had engaged in extensive surveillance abuses, including spying on civil rights activists, anti-war protesters, and political opponents, throughout the early decades of the Cold War.[1] The purpose of the law was to ensure that Americans' rights were protected when the government conducts foreign intelligence surveillance.

---

[1] *See* Lee Lacy, "Curtailment of the National Security State: The Church Senate Committee of 1975 – 1976," Boise State, *Frank Church Institute*, May 13, 2019, https://www.boisestate.edu/sps-frankchurchinstitute/2019/05/13/curtailment-of-the-national-security-state-the-church-senate-committee-of-1975-1976/.

Under Title I of FISA, the government was required to obtain an order from a special court (the FISA Court) to conduct "electronic surveillance." To obtain the order, the government had to show probable cause that the target of surveillance — whether that target was a foreigner or a "U.S. person" (an American citizen or legal permanent resident) — was a foreign power or an agent of a foreign power.[2] For non-U.S. persons, the terms "foreign power" and "agent of a foreign" power are defined quite broadly,[3] but for U.S. persons, "agent of a foreign power" is defined to require potential involvement in certain criminal activities, including espionage, sabotage, and terrorism.[4] This requirement remains in place today for electronic surveillance that is not targeted at foreigners abroad.

The term "electronic surveillance" is defined in a complex manner keyed to the communications technologies and government surveillance programs that existed at the time.[5] In practice, the definition means that most surveillance activities conducted inside the United States are covered by FISA, whereas most surveillance activities conducted outside the United States — other than those intentionally targeting U.S. persons — are not covered by FISA and are not subject to any of the law's privacy protections for people in the United States. Overseas collection of communications between foreign targets and Americans, for instance, takes place without any statutory authority or FISA Court involvement.

After 9/11, Congress raced to loosen restrictions on surveillance, including some contained in FISA. The 9/11 Commission later determined that U.S. intelligence agencies had ample intelligence about the planned attacks; they simply failed to share and act on that intelligence.[6] But in the attacks' immediate aftermath, lawmakers assumed otherwise. Congress passed the USA PATRIOT Act ("Patriot Act"), a 341-page bill that made extensive changes to over a dozen federal statutes, only one day after introduction — before many members had even had time to read it.[7]

The law's sweeping new surveillance powers did not satisfy the government, however. President George W. Bush authorized a set of secret programs, code-named Stellar Wind, to collect communications and other personal data without congressional authorization.[8] One of these programs involved the domestic warrantless collection of the content of communications

---

[2] 50 U.S.C. § 1805.
[3] 50 U.S.C. § 1801(a), (b)(1).
[4] 50 U.S.C. § 1801(b)(2).
[5] 50 U.S.C. § 1801(f).
[6] National Commission on Terrorist Attacks Upon the U. S., *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* 254-77, 339-60, July 22, 2004.
[7] *See* Electronic Privacy Information Center, "PATRIOT Act," Electronic Privacy Information Center, accessed June 11, 2023, https://epic.org/issues/surveillance-oversight/patriot-act/; Kate Tummarello, "Debunking the Patriot Act as It Turns 15," Electronic Frontier Foundation, October 26, 2016, https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15.
[8] *See* Offices of Inspectors General, Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and Office of the Director of National Intelligence, *Report on the President's Surveillance Program*, July 10, 2009, https://int.nyt.com/data/documenttools/savage-foia-stellarwind-ig-report/fd1368590db24fe1/full.pdf; Jake Laperruque, "Secrets, Surveillance, and Scandals: The War on Terror's Unending Impact on Americans' Private Lives," Project on Government Oversight, September 7, 2021, https://www.pogo.org/analysis/2021/09/secrets-surveillance-and-scandals-the-war-on-terrors-unending-impact-on-americans-private-lives.

between suspected foreign terrorists and Americans in the United States. This was a clear violation of FISA: although the Patriot Act expanded the purposes for which the government could seek a Title I order, it did not eliminate the requirement to obtain one.

After investigative journalists exposed the program,[9] the government attempted to obtain legal cover by securing the FISA Court's approval. When the court balked,[10] the government turned to Congress. Officials observed that changes in communications technology had altered which communications qualified as "electronic surveillance." As a result, the government was being required to obtain a FISA Title I order to collect foreigners' communications handled by U.S. service providers. Officials argued that this was impeding counterterrorism efforts, and they asked Congress to "modernize" FISA by loosening its restrictions.[11]

Congress responded by enacting the Protect America Act in 2007,[12] soon to be replaced by the FISA Amendments Act — which created Section 702 of FISA — in 2008.[13] Section 702 allows the government to target any foreigner abroad for foreign intelligence collection. Under this authority, the government may collect all of the target's communications, including those with Americans, without obtaining any individualized court order. The only substantive restriction is that a significant purpose of the collection must be the acquisition of foreign intelligence information, defined extremely broadly to include information "related to . . . the conduct of the foreign affairs of the United States."[14]

The Attorney General and the Director of National Intelligence make annual certifications, which historically have included broad categories of foreign intelligence information the government seeks to acquire, and submit general procedures for the surveillance to the FISA Court.[15] The Court approves the certifications and procedures but has no role in approving individual targets.[16] Currently, the government may obtain foreign intelligence information under four certifications covering the following topics: foreign governments and related entities; counterterrorism; combating the proliferation of weapons of mass destruction; and protecting against certain types of international drug activity.[17]

---

[9] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," New York Times, December 16, 2005, https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.
[10] *See* Charlie Savage, "Documents Shed New Light on Legal Wrangling Over Spying in U.S.," New York Times, December 12, 2014, https://www.nytimes.com/2014/12/13/us/politics/documents-shed-new-light-on-legal-wrangling-over-spying-in-us-.html.
[11] *Modernizing the Foreign Intelligence Surveillance Act, Hearing Before the S. Select Comm. on Intelligence*, 110th Cong., May 1, 2007 (statement for the record of J. Michael McConnell, Director of National Intelligence), https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-hearings-110399.pdf.
[12] Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (2007), https://uscode.house.gov/statutes/pl/110/140.pdf.
[13] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008), https://uscode.house.gov/statutes/pl/110/261.pdf.
[14] 50 U.S.C. § 1801(e)(2).
[15] 50 U.S.C. § 1881a(h); Office of the Director of National Intelligence, "ODNI Releases February 2025 FISC Certification D Opinion and April 2025 FISC Amended Certification D Opinion and Agency Procedures," August 19, 2025, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2025/4099-pr-23-25.
[16] 50 U.S.C. § 1881a.
[17] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certifications 2025-A, 2025-B, 2025-C, and Predecessor Certifications*, Nos. 702(j)-25-01, 702(j)-25-02, 702(j)-25-03, and predecessor dockets (FISA Ct. March 18, 2025),

The government uses Section 702 to engage in two types of surveillance. The first is "upstream collection," whereby communications flowing into and out of the United States on the Internet backbone are scanned for selectors associated with foreign targets. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired.[18] The second type of Section 702 surveillance is "downstream collection," also known as "PRISM," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communication service providers, who must turn over any communications to or from the selector.[19]

Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011 — the last year for which such information is publicly available.[20] Because agencies generally store Section 702 data for at least five years, a yearly intake of 250 million Internet communications would result in at least 1.25 billion such communications residing in government databases at any given time. Given the growth in the program — from 89,138 targets in 2013[21] to 291,824 targets in 2024[22] — the number of communications collected today is likely closer to one billion annually, with several billion sitting in storage.

II. The Impact on Americans' Privacy

Although Section 702 may only be targeted at foreigners overseas, it inevitably sweeps in Americans' communications, for the simple reason that Americans communicate with foreigners. The government does not deny that Section 702 results in the collection of Americans'

---

https://www.intelligence.gov/assets/documents/702-documents/declassified/2025/FISC_Opinion_Cert_ABC_03182025_Redacted.pdf; Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (FISA Ct. April 9, 2025), https://www.intel.gov/assets/documents/702-documents/declassified/2025/FISC_Opinion_2_Apr_2025_2024_Cert_D_Redacted_8-19-25_final.pdf; Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2023* at 16, April 2024, https://www.intelligence.gov/assets/documents/702-documents/statistical-transparency-report/2024_ASTR_for_CY2023.pdf [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2023].

[18] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 174–78, 2023, https://documents.pclob.gov/prod/Documents/OversightReport/d21d1c6b-6dc3-4bc4-b018-6c9151a0497d/2023%20PCLOB%20702%20Report,%20508%20Completed,%20Dec%203,%202024.pdf [hereinafter 2023 PCLOB 702 Report].

[19] *Id.* at 64–65.

[20] Memorandum Opinion and Order, [Redacted], No. [Redacted], 2011 WL 10945618, at *29 (FISA Ct. October 3, 2011). In addition, the Privacy and Civil Liberties Oversight Board reported that, "as of 2021, NSA acquired approximately 85.3 million internet transactions per year in upstream collection, which constitutes a small percentage of NSA's Section 702 collection." 2023 PCLOB 702 Report, *supra* note 18, at 178.

[21] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities: Annual Statistics for Calendar Year 2013*, June 2014, https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

[22] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2024* at 22, May 2025, https://www.intelligence.gov/assets/documents/702-documents/statistical-transparency-report/ASTR_CY24.pdf, [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2024].

communications in large numbers, although it has rebuffed lawmakers' requests[23] to provide a rough estimate of how many Americans' communications are collected.[24] Given the prevalence of international communication, however, it is safe to assume that the billions of communications acquired under Section 702 include millions of communications involving Americans.

The government refers to the collection of Americans' communications as "incidental," to signify that Americans are not the intended targets of the surveillance.[25] Indeed, if the government's purpose were to spy on those Americans, the program would be unlawful. Such surveillance would require either a warrant (in a criminal investigation) or a FISA Title I order (in a foreign intelligence investigation). To prevent the government from using Section 702 as an end-run around these constitutional and statutory requirements, Congress included two key provisions in the law. First, it required the government to "minimize" the collection, retention, and sharing of U.S. person information.[26] Second, it required the government to certify to the FISA Court, on an annual basis, that it is not engaged in "reverse targeting" — i.e., using Section 702 to gain access to the communications of "particular, known" Americans.[27]

---

[23] *See* Senators Ron Wyden and Mark Udall to I. Charles McCullough III (Inspector General of the Intelligence Community, Office of the Director of National Intelligence), and Dr. George Ellard (Inspector General, National Security Agency), May 4, 2011, https://www.wyden.senate.gov/download/?id=CE360936-DFF9-4273-8777-09BF29565086&download=1; Ron Wyden, "Senators Seek Answers from DNI on How Many of Americans' Communications Have Been Monitored," July 12, 2012, https://www.wyden.senate.gov/news/press-releases/senators-seek-answers-from-dni-on-how-many-of-americans-communications-have-been-monitored; Rep. John Conyers, Jr., et al., to James Clapper (Director Of National Intelligence), April 22, 2016, https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf; Reps. Bob Goodlatte and John Conyers to Daniel Coats (Director of National Intelligence), April 7, 2017, https://drive.google.com/file/d/1uaCE_5atwxhh0opdXdtekdHaZ7FqPI4V/view.

[24] Initially, the government claimed that providing such an estimate would itself violate Americans' privacy. *See* I. Charles McCullough, III (Inspector General of the Intelligence Community, Office of the Director of National Intelligence), to Sens. Ron Wyden and Mark Udall, June 15, 2012, https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1. After privacy experts and advocates refuted that claim, *see* Brennan Center for Justice, et al., to James Clapper (Director of National Intelligence), October 29, 2015, https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf, the Obama administration agreed to provide an estimate in early 2017. *See* U.S. House Comm. on the Judiciary Democrats, "Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance," December 16, 2016, https://democrats-judiciary.house.gov/media-center/press-releases/bipartisan-house-coalition-presses-clapper-for-information-on-phone-email-surveillance. The Trump administration then reneged on that promise, *see* Dustin Volz, "NSA Backtracks On Sharing Number of Americans Caught in Warrant-less Spying," Reuters, June 12, 2017, http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B, and the Biden administration took a similar approach.

[25] In this statement, I use quotation marks for the terms "target," "incidental," and "minimize," to underscore that they are terms of art with particular legal meanings. Legal and policy defenses of Section 702 rely heavily on these terms and concepts. The impact on Americans' privacy, however, does not. If the government is collecting tens of millions of Americans' communications and keeping them for years in databases where they are vulnerable to abuse, inadvertent mishandling, or theft, it matters little — from a practical perspective — that their initial acquisition was "incidental," or that the procedures allowing them to be kept and stored include "minimization" in their title. And if FBI agents are searching this data for Americans' communications, reading and listening to them, and using them against Americans in legal proceedings, those Americans will not be particularly comforted (indeed, they may well be baffled) to hear that they are not "targets."

[26] 50 U.S.C. § 1881a(e).

[27] 50 U.S.C. § 1881a(b)(2), (h)(2)(A)(iii).

Over the past 17 years, it has become abundantly clear that these protections have failed. Rather than actually "minimize" the retention and use of Americans' communications, as Congress directed, the government retains such data for years on end and routinely runs electronic searches designed to locate and retrieve the communications of particular Americans. The resulting privacy intrusion is exacerbated by recent changes in the law that further expanded the scope of surveillance authorized by Section 702 and the purposes for which Section 702 data may be searched.

A. Minimization and Its Loopholes

While the concept behind minimization is fairly simple, the statutory language is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[28] The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[29]

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data from its downstream collection under three of the four current certifications with the FBI, the CIA, and the National Counterterrorism Center ("NCTC").[30] All four agencies generally may keep unreviewed raw data — including

---

[28] 50 U.S.C. § 1801(h)(1).

[29] 50 U.S.C. § 1801(h)(3).

[30] *See* Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 9, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/NSA_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 NSA 702 Minimization Procedures] (minimization procedures for three of the four current certifications, i.e., Certifications A, B, and C). The minimization procedures for Certification D, adopted in April 2025, allow the NSA to share raw data with the CIA but not the FBI or the NCTC. Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Concerning the International Production, Distribution, or Financing of Certain Illicit Drugs Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 9, December 11, 2024, https://www.intel.gov/assets/documents/702-documents/declassified/2025/NSA_MPs_2024_Cert_D_12-16-24_Redacted_8-19-25_final.pdf [hereinafter 2025 NSA 702 Cert D Minimization Procedures]. Because the procedures for this new certification differ from those for prior certifications, this Part's discussion is limited to the minimization procedures for Certifications A, B, and C. Certification D is discussed in more detail *infra* in Part II.C.1.

data about U.S. persons — for five years after the certification expires;[31] they also can seek extensions from a high-level official,[32] and the NSA and FBI expressly exempt encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) from the 5-year limit.[33] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[34]

If the NSA discovers U.S. person information that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.[35] The NSA, however, maintains that data with no apparent foreign intelligence value "may have foreign intelligence value in the future or for another concurrent investigation." [36] Accordingly, "communications are rarely purged before their designated age-off date."[37]

The FBI, CIA, and NCTC have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements.[38] Moreover, if the FBI reviews U.S. person information and *does not identify it* as foreign intelligence information or evidence

---

[31] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 4(c)(1)–(2) ; Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § III.D.4.b, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/FBI_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 FBI 702 Minimization Procedures]; Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 2.a, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/CIA_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 CIA 702 Minimization Procedures]; Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the National Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § B.2.a, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/NCTC_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 NCTC 702 Minimization Procedures].

[32] 2023 PCLOB 702 Report, *supra* note 18, at 78; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at § B.2.a.; 2025 FBI 702 Minimization Procedures, *supra* note 31, at §III.I.1; 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 7(1); 2025 CIA 702 Minimization Procedures, *supra* note 31, at § 2.a.

[33] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 7(1)a; 2025 FBI 702 Minimization Procedures, *supra* note 31, at § III.I.4. The CIA has also historically permitted communications to be retained indefinitely if they are "enciphered or contain[] secret meaning." *See* Lisa O. Monaco, Deputy Attorney General, U.S. Department of Justice, *Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 3.c, October 14, 2021, https://www.intelligence.gov/assets/documents/702-documents/declassified/2024/2024_Cert_CIA_MPs_for_Public_Redacted_3-13-23.pdf [hereinafter 2024 CIA 702 Minimization Procedures].

[34] 2025 NSA 702 Minimization Procedures, *supra* note 30, at §§ 6(2), 7(3); 2025 FBI 702 Minimization Procedures, *supra* note 31, at §§ III.A.3, III.C.1.b; 2025 CIA 702 Minimization Procedures *supra* note 31, at §§ 2.a, 3, 8; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at §§ B.2.a, B.3, B.4, C.4.

[35] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 4(b)(1).

[36] 2023 PCLOB 702 Report, *supra* note 18, at 78.

[37] *Id.*

[38] *Id.* at 78–80.

of a crime, the 5-year limit evaporates, and the FBI may keep the data for 15 years.[39] A similar rule applies to the NCTC.[40]

If any of the four agencies — all of which have access to raw data — disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person's identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.[41]

In short, the NSA routinely shares raw Section 702 data with the FBI, CIA, and NCTC; and the agencies' minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are "minimized" under any commonsense understanding of the term.

B. Backdoor Searches

Perhaps the most glaring failure of the protections Congress put in place for Americans' privacy is the practice of "backdoor searches." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans (which would constitute "reverse targeting"). Immediately upon obtaining the data, however, all four agencies have procedures in place that allow them to sort through the data looking for the communications of particular, known Americans — the very people who the government just certified were not intended targets.[42] This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the requirements of the Fourth Amendment and Title I of FISA.

According to the Privacy and Civil Liberties Oversight Board ("PCLOB"), the FBI routinely conducts these searches at the "pre-assessment" and "assessment" phases of its investigations[43] — i.e., before agents have a factual basis to suspect a national security threat or criminal activity, let alone probable cause and a warrant.[44] For years, the FBI resisted calls to disclose how many backdoor searches it performs each year. But after Congress and the FISA Court forced the FBI to track those queries, the government lost its excuse to withhold the number. In 2022, the ODNI's annual statistical transparency report revealed that, in 2021 alone,

---

[39] 2025 FBI 702 Minimization Procedures, *supra* note 31, at § III.D.4.c.
[40] 2025 NCTC 702 Minimization Procedures, *supra* note 31, § B.2.b.
[41] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 8(2), (9); 2025 FBI 702 Minimization Procedures, *supra* note 31, at § IV.A.1–2, B; 2025 CIA 702 Minimization Procedures, *supra* note 31, at §§ 5.a, 7.d; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at § D.1–2. In addition, the FBI may disseminate unminimized Section 702 data to the NSA, CIA, and in some cases the NCTC. 2025 FBI 702 Minimization Procedures, *supra* note 31, at § IV.E.
[42] 2025 NSA 702 Minimization Procedures, *supra* note 30, § 4(b)(4); 2025 FBI 702 Minimization Procedures, *supra* note 31, at § III.D.3; 2025 CIA 702 Minimization Procedures, *supra* note 31, at § 4; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at § C.1.
[43] 2023 PCLOB 702 Report, *supra* note 18, at 11.
[44] *Id.* at 38–39.

the FBI conducted up to *3.4 million* U.S. person queries of federated data systems that included Section 702 data.[45]

In 2022, after the FBI made changes to its data systems that required FBI agents to "opt in" to receiving Section 702 data in response to queries rather than having to "opt out," the number of U.S. person queries reportedly conducted by the FBI dropped to around 200,000;[46] following additional changes to internal querying procedures, the number dropped further in 2023 to 57,094.[47] While that represents a sizeable decrease, it is still an enormous number by any standard, comprising more than 150 warrantless searches for Americans' communications each day.

The number of backdoor searches conducted by the FBI in 2024 is unknown. In September 2024, the Department of Justice's National Security Division ("NSD") notified the FISA Court that it was evaluating the FBI's use of a particular tool known as an "advanced filter function."[48] When using this tool to retrieve the communications of particular targets, FBI agents could select from a list of "participants" who were in contact with those targets and review those participants' communications. Although this functionality enabled FBI to search for U.S. persons' communications, the FBI did not consider these searches to be queries and therefore did not track them or, presumably, follow required querying procedures (such as obtaining attorney approval and providing a written justification for U.S. person queries). After the NSD determined that these searches constituted queries, it informed the FISA Court that it "'does not presently have access to historical data' . . . and is coordinating with FBI to assess what records of the use of this functionality may have been generated and maintained."[49] Without such records, data on the number of U.S. person queries in 2024 — and perhaps other years — is incomplete.

This failure to track an entire category of queries could help to explain an otherwise perplexing drop in the number of *reported* queries to 5,518 in 2024.[50] Both the FISA Court and the OIG attribute this drop in part to reforms made by RISAA. Yet, as OIG acknowledges

---

[45] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2021* at 21, April 2022, https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf, [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2021].

[46] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2022* at 24, April 2023, https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2022]. The government has provided a "de-duplicated" number of 119,383, which represents the number of unique identifiers used to perform queries. *Id.* That is likely a more accurate proxy for the number of Americans affected, but it fails to capture situations in which the FBI performs repeated searches of the same account to find additional information. Each of those searches is a distinct privacy intrusion. Accordingly, the number of total searches (204,090) is a better indicator of the cumulative privacy impact of this practice.

[47] ODNI, Annual Statistical Transparency Report: Calendar Year 2023, supra note 17, at 25.

[48] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certifications 2025-A, 2025-B, 2025-C*, Nos. 702(j)-25-01, 702(j)-25-02, 702(j)-25-03, supra note 17, at 40.

[49] *Id.*

[50] ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 6.

elsewhere in the report,[51] most of those reforms — including several of those highlighted by OIG as being the most significant — simply codified changes the FBI had already implemented well before RISAA's enactment.[52] The few additional changes made by RISAA might explain some portion of the subsequent drop in reported queries, but it is highly implausible that they alone caused a decline of more than 90%.

Even if the number of U.S. person queries reported by the FBI in 2024 could be taken at face value, 5,518 warrantless searches of private communications would still represent a gross intrusion on U.S. persons' privacy and civil liberties. The government is able to present that number as a success story only because the FBI conducted *3.4 million* U.S. person queries in 2021. But a burglar should not escape condemnation for robbing a house — let alone be applauded for his restraint — simply because he robbed an entire neighborhood three years ago. The shockingly low bar the government set in 2021 cannot be used as the measure of Americans' rights. Moreover, there was a significant *increase* in the number of U.S. person queries conducted by the CIA, NSA, and NCTC during this period — from 4,684 in 2022 to 7,845 in 2024.[53] In total, the U.S. government conducted 13,363 known warrantless searches of Americans' emails, text messages, and phone calls in 2024.

Government officials have defended backdoor searches, claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose.[54] This argument ignores Congress's command to agencies to "minimize" information about U.S. persons. The very meaning of "minimization" is that agencies may *not* use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: As one FISA Court judge has observed, "[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[55] Whatever merit the government's

---

[51] *See* Oversight and Review Division, Office of the Inspector General, Department of Justice, *A Review of the Federal Bureau of Investigation's Querying Practices Under Section 702 of the Foreign Intelligence Surveillance Act* 13–14, October 2025, https://oig.justice.gov/sites/default/files/reports/26-002_0.pdf [hereinafter 2025 OIG Report].

[52] *Compare* Reforming Intelligence and Securing America Act, Pub. L 118-49, § 2(b), (d), 138 Stat. 862, 862–65 (2024), https://www.congress.gov/118/plaws/publ49/PLAW-118publ49.pdf [hereinafter RISAA], *with Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities, Hearing Before the S. Comm. on the Judiciary*, 118th Cong., June 13, 2023 (joint statement for the record of Chris Fonzone, General Counsel, Office of the Director of National Intelligence, et al.), https://www.judiciary.senate.gov/imo/media/doc/2023-06-13%20-%20Joint%20statement%20-%20ODNI,%20NSA,%20CIA,%20FBI,%20DOJ%20(1).pdf, *and* ODNI, Annual Statistical Transparency Report: Calendar Year 2022, *supra* at note 46, at 22.

[53] ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 25.

[54] *See, e.g.*, *The FISA Amendments Act: Reauthorizing American's Vital National Security Authority and Protecting Privacy and Civil Liberties Reauthorization, Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (June 27, 2017), C-SPAN, 44:02, (testimony of Stuart J. Evans, Deputy Assistant Attorney General for Intelligence, National Security Division, Department of Justice), https://www.c-span.org/program/senate-committee/fisa-reauthorization/481407; *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities, Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 14, 27 (June 13, 2023) (testimony of Matthew G. Olsen, Assistant Attorney General for National Security, Department of Justice), https://www.congress.gov/118/chrg/CHRG-118shrg58969/CHRG-118.

[55] [Redacted], 2011 WL 10945618, *supra* note 20, at *27.

defense might or might not have in other contexts,[56] it is contrary to the constitutional and statutory grounding of the Section 702 program.

Despite these principles, the FISA Court has held that backdoor searches are lawful. But among the handful of regular federal courts outside the FISA Court that have had the opportunity to weigh in on this question, a divide has emerged, with several judges — including a unanimous panel of the Second Circuit Court of Appeals, the only federal appellate court to rule on this question — raising constitutional concerns.[57] In December 2024, a district court judge held that the Fourth Amendment applies to backdoor searches and that the searches at issue in the case were unconstitutional.[58] Outside of the courts, constitutional scholars have assessed that

---

[56] In fact, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant. *See, e.g.*, United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016); United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010) ("[O]fficers and others involved in searches of digital media [must] exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."). The fact that the data was lawfully obtained does not give the government permission to conduct a fishing expedition that goes beyond the authorized purpose for the seizure. In an analogous 2014 ruling, the Supreme Court held that police officers must obtain a warrant to search the contents of a cell phone even after they lawfully seized that cell phone without a warrant during a search incident to arrest. *See* Riley v. California, 573 U.S. 373 (2014); *see also* Walter v. United States, 447 U.S. 649, 654 (1980) ("The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents."); United States v. Odoni, 782 F.3d 1226, 1237–38 (11th Cir. 2015) ("We . . . must analyze the search and the seizure separately, keeping in mind that the fact that police have lawfully come into possession of an item does not necessarily mean they are entitled to search that item without a warrant.").

[57] *See* United States v. Hasbajrami, 945 F.3d 641, 669–73 (2d Cir. 2019). The Second Circuit remanded to the district court for further factual development about the search that occurred in that case. Judge Carlos Lucero of the U.S. Court of Appeals for the Tenth Circuit, in a dissenting opinion, similarly expressed constitutional concerns about backdoor searches, opining that such searches must be analyzed as separate Fourth Amendment events from the original collection; the majority did not reach the issue, as they held that the record did not establish that a backdoor search occurred. *See* United States v. Muhtorov, 20 F.4th 558, 678–80 (10th Cir. 2021).

The judges on the other side of this divide have relied heavily on a misrepresentation that the Department of Justice made in litigation, i.e., that government officials need to review Americans' communications anyway as part of the minimization process. *See* United States v. Mohamud, 2014 WL 2866749, at *26 (D. Oregon 2014); United States v. Hasbajrami, 2016 WL 1029500, at *12 n.20 (E.D.N.Y. 2016); United States v. Al-Jayab, No. 16 CR 181, at 55–56 (N.D. Ill. June 28, 2018), *available at* https://storage.courtlistener.com/recap/gov.uscourts.ilnd.324196/gov.uscourts.ilnd.324196.115.0.pdf; *see also* Elizabeth Goitein, "Americans' Privacy at Stake as Second Circuit Hears Hasbajrami FISA Case," *Just Security*, August 24, 2018, https://www.justsecurity.org/60439/americans-privacy-stake-circuit-hears-hasbajrami-fisa-case/ (explaining the misrepresentation on which the court relied). In fact, none of the agencies' minimization procedures require them to review communications to determine whether they must be minimized. *See generally* 2025 NSA 702 Minimization Procedures, *supra* note 30; 2025 FBI 702 Minimization Procedures, *supra* note 31; 2025 CIA 702 Minimization Procedures, *supra* note 31; 2025 NCTC 702 Minimization Procedures, *supra* note 31. Indeed, such a review would be literally impossible, given that the government collects close to a billion communications per year under Section 702. *See* Part I, *supra.*

[58] United States v. Hasbajrami, No. 1:11-CR-623 (LDH), 2025 WL 447498, at *5–9, *16 (E.D.N.Y. February 10, 2025)

backdoor searches must be treated as a Fourth Amendment event that is separate from the underlying collection,[59] thus generally triggering the warrant requirement.[60]

C. Recent Expansions of Section 702 Surveillance

Recent changes to the collection of communications under Section 702 have heightened the program's impact on Americans' privacy, underscoring the need for reform. RISAA dramatically (and unnecessarily) expanded the types of entities that can be compelled to assist the government in Section 702 surveillance. It also amended the definition of "foreign intelligence" to include information relating to international narcotics trafficking, and it authorized suspicionless queries of Section 702 for the purpose of vetting individuals seeking to travel to the United States. The first change creates massive potential for abuse, while all three changes increase the volume of Americans' communications that may be collected "incidentally" and/or retrieved through warrantless searches.

1. Expanded Definition of "Electronic Communication Service Provider"

The government conducts Section 702 surveillance with the compelled assistance of "electronic communication service providers" ("ECSPs"),[61] generally by requiring them to turn over the communications of targets identified by the government.[62] In 2023, the FISA Court ruled that FISA's definition of "electronic communication service provider" did not cover a specific type of provider[63] — reportedly, a data center for cloud computing.[64] The Biden

---

[59] *See* Barry Friedman and Danielle Keats Citron, "Indiscriminate Data Surveillance," *Virginia Law Review* 110, no. 6 (2024): 1403–04, 1410 n.258; *see also* Orin Kerr, "The Fourth Amendment and Querying the 702 Database for Evidence of Crimes," Washington Post, October 20, 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/20/the-fourth-amendment-and-querying-the-702-database-for-evidence-of-crimes/.

[60] The Supreme Court has held that warrantless searches are *per se* unreasonable unless they fall within an established exception to the warrant requirement. City of Los Angeles v. Patel, 576 U.S. 409, 419–420 (2015). A few circuit courts have held than there is a narrow "foreign intelligence" exception to the warrant requirement in at least some cases; the Fourth Circuit, for instance, recognized such an exception in cases where the surveillance is for the primary purpose of obtaining foreign intelligence and the target is a foreign power or agent of a foreign power. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980). In addition, the district court that ruled certain backdoor searches unconstitutional recognized a much broader version of this exception. *See Hasbajrami,* 2025 WL 447498, *supra* note 58, at *13–16; *see also* Hannah James, "The Dangerous Foreign Intelligence Exception Loophole in the Hasbajrami Decision," *Just Security*, April 7, 2025, https://www.justsecurity.org/109879/foreign-intelligence-exception-hasbajrami/. The Supreme Court has not recognized any such exception, however. Accordingly, it would be a stretch to say that there is an established foreign intelligence exception to the Fourth Amendment's warrant requirement, let alone one that is broad enough to support the government's current practice with regard to U.S. person queries. *See* Elizabeth Goitein and Faiza Patel, *What Went Wrong with the FISA Court* 11-12, Brennan Center for Justice, March 14, 2015, https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court (discussing case law on foreign intelligence exception).

[61] 50 U.S.C. § 1881a(i).

[62] *See* 2023 PCLOB 702 Report, *supra* note 18, at 34, 54.

[63] *See* Opinion and Order, *In re: Petition to Set Aside or Modify Directive Issued to [Redacted]*, Nos. [Redacted], (FISA Ct. Rev. 2023), https://www.intel.gov/assets/documents/702-documents/declassified/2023_FISC-R_ECSP_Opinion.pdf.

[64] *See* Charlie Savage, "Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program," New York Times, April 16, 2024, https://www.nytimes.com/2024/04/16/us/fisa-surveillance-bill-program.html.

administration solicited an amendment to RISAA that would expand the ECSP definition. Because the type of provider was (and remains) classified, however, the amendment was deliberately drafted using vague and broad language to conceal the type of provider at issue. It was unveiled three days before the House voted on it, leaving members with little time to investigate assurances that the amendment was a narrow fix to address a specific FISA Court decision.[65] In reality, while the issue the amendment sought to address was a narrow one, the amendment itself, enacted in RISAA, is a truly breathtaking expansion of surveillance authority.

The provision expands the ECSP definition to include not only providers of communication services, like Verizon and Gmail, but providers of *any service* (with certain narrow exceptions), as long as they have access to equipment on which communications are transmitted or stored.[66] This change vastly inflates the universe of entities that can be compelled to assist the government in Section 702 collection. Almost every public-facing business or organization, large or small, provides some type of "service," and they all have access to communications equipment (e.g., phones and computers). The new definition sweeps in grocery stores, barber shops, fitness centers, places of worship, and a host of other establishments frequented by the American public. It also encompasses the commercial landlords that lease office space where tens of millions of Americans go to work every day.[67]

Although the government is still limited to collecting the communications of foreign targets, this sea change in the law has direct consequences for, and poses alarming risks to, Americans' privacy. For one thing, expanding the range of entities from which the government may compel assistance increases the volume of communications it can collect, which in turn increases the number of Americans' communications that may "incidentally" be obtained. Moreover, unlike Verizon or Gmail, many of the businesses covered by the expanded definition lack the ability to isolate and turn over particular communications. Their only option may be to give NSA personnel access to the relevant equipment. That, in turn, would give the NSA access to *all* the communications transmitted through or stored on the equipment, including purely domestic communications between and among Americans. NSA would be on the "honor system" to pull out and retain only the communications of valid foreign targets.

Put simply, this provision potentially gives the NSA the authority to directly access the communications equipment of nearly every business and organization in the United States. The potential for abuse in a system that provides such broad access is difficult to overstate. It is for this reason that Senator Ron Wyden described the amended ECSP definition as "one of the most

---

[65] *See* Rebecca Beitsch, "Intelligence Community Largely Won House FISA Fight. Now Comes the Senate," The Hill, April 16, 2024, https://thehill.com/homenews/house/4596017-intelligence-community-largely-won-house-fisa-fight-now-comes-the-senate/; 170 Cong. Rec. H2354 (daily ed., April 12, 2024) (statement of Rep. Mike Turner).

[66] *See* RISAA, supra note 52, at § 25(a)(3). In response to criticism of an earlier version of the amendment, *see, e.g.*, Marc Zwillinger and Steve Lane, "House Intelligence Committee FISA 'Reform' Bill Would Greatly Expand the Class of Businesses and Other Entities Required to Assist in FISA 702 Surveillance," *ZwillGenBlog,* December 8, 2023, https://www.zwillgen.com/law-enforcement/fisa-reform-bill-702-surveillance/, its drafters excluded hotels, residential buildings, food service establishments, and community facilities (such as libraries and hospitals) in the final version. *See* 50 U.S.C. § 1881(b)(4)(E).

[67] *See* Elizabeth Goitein, "The FISA Expansion Turning Cable Installers Into Spies Cannot Stand," The Hill, April 17, 2024, https://thehill.com/opinion/technology/4599695-the-fisa-expansion-turning-cable-installers-into-spies-cannot-stand/.

dramatic and terrifying expansions of government surveillance authority in history."[68] Tacitly conceding the danger of the expanded definition, the Biden administration made a public commitment to apply it only to the specific type of provider at issue in the FISC opinion and to notify Congress when requiring such providers' assistance.[69] However, that commitment is not binding on the current administration nor on future ones.

2. International Narcotics Trafficking

RISAA also amended the definition of "foreign intelligence information" to include "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned."[70] Pursuant to this change, the government in April 2025 obtained FISA Court approval of a new certification authorizing acquisition of foreign intelligence information "concerning the international production, distribution, or financing of illicit opioids [redacted] or cocaine."[71]

Both the collection and the querying authorized under this certification have significant implications for Americans' privacy. As the FISA Court observed, the threat sought to be addressed under this certification "encompasses a domestic component . . . [i]ndeed, the domestic impact . . . is what makes the threat posed by international trafficking so significant."[72] This domestic nexus increases the likelihood that Americans' communications will be "incidentally" collected. Moreover, because information at the collection stage "need only bear on, or have some relation to" the ability of the United States to protect against the threat of drug trafficking,[73] the FISA Court expressed "concern[] that the NSA and CIA might acquire a larger number of communications of or concerning U.S. persons, including those engaged in purely legitimate business" under this certification.[74]

This certification also poses unique concerns regarding the use of Section 702 data for ordinary crime control. As the FISA Court recognized, there is "inherent overlap" between what constitutes foreign intelligence information as defined in the certification and evidence of ordinary drug crime.[75] As a result, the government is more likely both to acquire evidence of ordinary crime under this certification and to retrieve such evidence through its foreign-

---

[68] Ron Wyden, "Wyden: 'I Will Do Everything In My Power' to Stop Bill Expanding Government Surveillance Under FISA 702," April 12, 2024, https://www.wyden.senate.gov/news/press-releases/wyden-i-will-do-everything-in-my-power-to-stop-bill-expanding-government-surveillance-under-fisa-702.
[69] Carlos Felipe Uriarte (Assistant Attorney General, U.S. Department of Justice) to Sen. Mark Warner, (Chairman, Senate Select Comm. on Intelligence), April 17, 2024, https://www.justice.gov/opa/media/1348621/dl?inline.
[70] 50 U.S.C. § 1801(e)(1)(D).
[71] *See In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (April 9, 2025), *supra* note 17, at 2.
[72] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04, at 49–50 (FISA Ct. February 20, 2025), https://www.intelligence.gov/assets/documents/702-documents/declassified/2025/FISC_Opinion_1_Feb_2025_2024_Cert_D_Redacted_8-19-25_final.pdf.
[73] *Id.* at 25.
[74] *In re DNI/AG 702(h) Certification 2024-D*, No. 702(j)-24-04 (April 9, 2025), *supra* note 17, at 6.
[75] *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (February 20, 2025), *supra* note 72, at 7.

intelligence queries.[76] The statute then permits the government to disseminate that information for law enforcement purposes.[77]

In short, the certification facilitates scenarios in which "evidence of drug-related crime will have been collected without a warrant, identified through a subsequent query using a U.S. person identifier . . . and then used for a non-foreign intelligence law-enforcement purpose."[78] Such scenarios stray far from the intent of Section 702 and from the constitutional safeguards ordinarily present in domestic criminal investigations.

3. Suspicionless Queries for Travel Vetting

The primary substantive restriction on queries of Section 702 data is that they must be reasonably likely to retrieve foreign intelligence information. RISAA created an exception to that restriction in a provision that requires agencies' querying procedures to "enable the vetting of all non-United States persons who are being processed for travel to the United States using terms that do not qualify as United States person query terms."[79] The provision permits entirely suspicionless searches of individuals seeking to travel to the United States — whether on student or work visas or as tourists and business travelers — even when the multiple other vetting mechanisms used by the government have not revealed any basis for believing that the individual poses a threat to the United States.

The provision has an obvious and significant impact on non-U.S. persons, whose private communications can now be searched simply because they apply to travel to the United States. The provision impacts Americans' privacy, too. Any query of Section 702 information runs the risk of returning communications that involve Americans. Because querying for the purposes of travel vetting increases the number of queries run — presumably by a significant amount, considering the United States issued more than 11 million visas in 2024[80] — it increases the chance that Americans' private communications will be accessed as a result of those queries.[81] Moreover, given the suspicionless nature of the queries, any U.S. person communications that are retrieved are highly likely to contain innocuous private conversations rather than foreign intelligence.

III. Violations of Statutory and Court-Ordered Privacy Protections

Section 702 has been marked since its inception by repeated, often systemic violations of the rules Congress and the FISA Court have put in place to protect Americans' privacy. The extent of this non-compliance is alarming in its own right. Any unauthorized collection, search,

---

[76] *Id.* at 7, 60.
[77] 50 U.S.C. § 1801(h)(3).
[78] *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (April 9, 2025), *supra* note 17, at 60.
[79] *See* RISAA, *supra* note 52, at § 24.
[80] *See* U.S. Department of State, *Summary of Visas Issued by Issuing Office Fiscal Year 2024* at 6, 2025, https://travel.state.gov/content/dam/visas/Statistics/AnnualReports/FY2024AnnualReport/Table%20IV.pdf.
[81] Visa applicants are unlikely to be Section 702 targets themselves, so any communications retrieved by travel vetting queries are likely to be communications between the applicants and targets, both of whom must be non-U.S. persons. However, such communications could involve U.S. persons as additional participants (e.g., in group emails or text chats).

or dissemination can result in Americans being investigated without proper legal basis or sensitive information falling into the hands of people who could misuse it. But violations in recent years raise even more acute concerns: the use of foreign intelligence surveillance powers against Americans based on their race, ethnicity, politics, or journalistic activity. The government has been quick to celebrate improved rates of compliance since 2023, glossing over the potentially significant gaps in compliance information and the serious compliance incidents that have occurred.

A. FBI Violations of Limitations on U.S. Person Queries

Congress and the FISA Court have attempted to place some modest limits on the FBI's use of backdoor searches. The FBI, however, has routinely violated those limits.

In 2018, Congress required the FBI to obtain a probable-cause order from the FISA Court before reviewing the results of U.S. person queries not designed to extract foreign intelligence information in a very small subset of cases, i.e., predicated criminal investigations unrelated to national security.[82] This provision was rarely triggered, both because "related to national security" is a subjective and malleable criterion and because the FBI, according to the PCLOB, routinely performs U.S. person queries at the "pre-assessment" and "assessment" stages — i.e., before the FBI has sufficient information to open a predicated investigation.[83] Nonetheless, according to the ODNI's statistical transparency reports, the requirement was triggered on at least 100 occasions over six years.[84] Incredibly, the FBI did not obtain a FISA Court order in a *single one* of those cases.[85]

---

[82] FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118, § 101(a)(1)(B), 132 Stat. 3, 4 (2017), https://www.govinfo.gov/content/pkg/PLAW-115publ118/pdf/PLAW-115publ118.pdf.

[83] 2023 PCLOB 702 Report, *supra* note 18, at 11.

[84] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2020* at 21, April 2021, https://www.dni.gov/files/CLPT/documents/2021_ASTR_for_CY2020_FINAL.pdf [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2020]; ODNI, Annual Statistical Transparency Report: Calendar Year 2021, *supra* note 45, at 22; ODNI, Annual Statistical Transparency Report: Calendar Year 2022, *supra* note 46, at 26; ODNI, Annual Statistical Transparency Report: Calendar Year 2023, *supra* note 17, at 27. Before 2021, rather than reporting the number of times the court-order requirement (which appears in Section 702(f)(2)) was triggered, the government reported a slightly broader number, i.e., how many times the government reported to the FISA Court that FBI agents had accessed Section 702 data in response to queries not designed to return foreign intelligence. (Congress had required this reporting in 2018.) However, in its 2020 report, the government noted that "a Section 702(f)(2) order should have been obtained . . . in nearly all of [these] queries." ODNI, Annual Statistical Transparency Report: Calendar Year 2020, *supra* note 84, at 20. The government also stated that, "in some instances, a single report to the Court involved multiple queries on the same day by the same user that returned and displayed Section 702 content." *Id.* at 21. Accordingly, the total number of cases in which the government should have obtained a court order before accessing queries is almost certainly higher than 100.

[85] *See* ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 27; ODNI, Annual Statistical Transparency Report: Calendar Year 2020, *supra* note 84, at 21. Addressing this issue in its December 2019 opinion, the FISA Court noted that "*[s]ome* violations resulted *in part* from the manner in which FBI systems displayed information in response to queries." Memorandum Opinion and Order, [Redacted], No. [Redacted], at 69–70 (FISA Ct. December 6, 2019), https://www.intelligence.gov/assets/documents/702-documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf (emphasis added). Specifically, systems would display query results in a summary field that showed 100 characters of text around the query term within the records identified as responsive to the query. According to the FISA Court, however, "FBI personnel are known to

In 2024, Congress replaced the court order requirement with an outright prohibition on queries "solely designed to find and extract evidence of criminal activity."[86] There are two exceptions to the prohibition: (1) queries to retrieve information that could assist in mitigating a threat to life or serious bodily harm; and (2) queries to identify information that must be produced or preserved in connection with litigation, including criminal matters. Though touted as a significant reform,[87] this prohibition in fact impacts a very small number of queries — of the more than 57,000 U.S. person queries conducted in 2023, this provision would have prohibited the FBI from accessing Section 702 data in only four cases.[88] Moreover, because the FBI did not track all of its queries in 2024 (as discussed further below), there is no way to determine whether the FBI has fully complied with the prohibition. What official statistics *do* show is a conspicuous six-fold increase in the querying and accessing of Section 702 data for the ostensible purpose of meeting litigation obligations[89] — one of the two circumstances under which the FBI may still perform evidence-of-a-crime only queries.

For the vast majority of U.S. person queries (those that are not solely designed to find and extract evidence of criminal activity), the only substantive restriction on queries is the standard set forth in the FBI's querying procedures. Under that standard, "[e]ach query of FBI systems [containing raw Section 702 data] . . . must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, unless otherwise specifically excepted in these procedures."[90] This is a fairly low bar, to be sure. Even so, government reports and FISA Court opinions show that the FBI has engaged in a pattern of "widespread violations" of this rule.[91]

In 2018, the FISA Court expressed "serious concern" about "the large number of [FBI] queries evidencing a misunderstanding of the querying standard — or indifference to it."[92] The Court posited that the reported violations were likely the tip of the iceberg. It noted that Department of Justice overseers, at that time, "review[ed] only a small portion of the queries conducted," making it "entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the Court."[93] The Court ultimately found that the FBI's querying and minimization procedures,

---

have taken further steps in response to such displays (e.g., opening 'products' containing contents returned by a query), thereby accessing Section 702-acquired contents beyond what was initially displayed to them." *Id.* at 70. In any event, this feature did not account for all of the violations.

[86] 50 U.S.C. § 1881a(f)(2)(A).

[87] *See, e.g.*, 170 Cong. Rec. H2329 (daily ed. April 12, 2024) (statement of Rep. Jim Himes).

[88] *See* ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 27, 31.

[89] *See* ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 31.

[90] *See* Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Querying Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § IV.A., January 17, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/FBI_QPs_2025_Cert_ABC_01172025_Redacted.pdf.

[91] Memorandum Opinion and Order, [Redacted], No. [Redacted], at 44 (FISA Ct. November 18, 2020), https://www.intel.gov/assets/documents/702-documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf.

[92] Memorandum Opinion and Order, [Redacted], No. [Redacted], 402 F. Supp. 3d 45, 72 (FISA Ct. October 18, 2018).

[93] *Id.* at 74.

as implemented, were inconsistent with both the requirements of FISA and the Fourth Amendment.[94]

The FBI responded by implementing several measures designed to improve compliance through enhanced training, oversight and approval requirements, and changes to data systems access. Many of these measures were later codified in RISAA. Nonetheless, over the next four years, the FISA Court continued to observe "widespread violations of the querying standard by the FBI."[95] The "[l]arge-scale, suspicionless queries of Section 702 information [that] contributed to a finding of deficiency in the FBI's querying and minimization procedures . . . remained a concern . . . in April 2022."[96] Indeed, in March 2022, the government submitted a notice to the FISA Court in which it reported more than 278,000 non-compliant FBI queries of raw FISA-acquired information.[97]

The violations that took place during this period are memorialized in FISA Court opinions, compliance reports, and the PCLOB's report on Section 702. In 2020, for instance, FBI agents conducted 141 backdoor searches for the communications of people who had protested the police killing of George Floyd, despite having "no information connecting the individuals or the conduct to information that would be contained in FBI's Section 702-acquired information."[98] The following year, agents ran thousands of searches relating to the January 6 attack on the U.S. Capitol, also on a baseless hunt for evidence of foreign ties.[99] In total, between November 2020 and December 2021, "non-compliant queries related to civil unrest numbered in the tens of thousands."[100] Agents ran additional searches for information about members of Congress;[101] a congressional candidate;[102] a congressional chief of staff;[103] a local political

---

[94] *Id.* at 133–34.
[95] [Redacted], No. [Redacted] (FISA Ct. December 6, 2019), *supra* note 85, at 65.
[96] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, and predecessor dockets, at 87 (FISA Ct. April 11, 2023), https://www.intelligence.gov/assets/documents/702-documents/declassified/2023/FISC_2023_FISA_702_Certifications_Opinion_April11_2023.pdf.
[97] *See* Memorandum Opinion and Order, [Redacted], No. [Redacted], at 31 (FISA Ct. April 21, 2022), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.
[98] 2023 PCLOB 702 Report, *supra* note 18, at 150–51.
[99] [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 28–29.
[100] 2023 PCLOB 702 Report, *supra* note 18, at 151.
[101] *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-FISA-702-Compliance.pdf [hereinafter DOJ & ODNI, Semiannual Assessment December 2021]; 2023 PCLOB 702 Report, *supra* note 18, at 155.
[102] *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* 48 n.89, March 2023, https://www.intel.gov/assets/documents/702-documents/declassified/27th_Joint%20Assessment_for%20PUBLIC_1.15.25.pdf [hereinafter DOJ & ODNI, Semiannual Assessment March 2023].
[103] *Id.*

party;[104] multiple U.S. government officials, journalists, and political commentators;[105] 19,000 donors to a political campaign;[106] and two "Middle Eastern" men who were reported by a witness because they were loading boxes labeled "Drano" into a vehicle.[107]

These incidents carry echoes of the politically and racially motivated surveillance abuses that occurred under the reign of J. Edgar Hoover. That is alarming, but it should not be surprising. When government officials are not required to show probable cause of criminal activity to a court, it greatly increases the risk that searches will be driven by improper considerations — including officials' conscious or subconscious prejudices or political leanings.

Other reported violations are disturbing simply because they violated the privacy of ordinary Americans who should never have come under law enforcement scrutiny. They include searches for the communications of:

- people who came to the FBI to perform repairs;[108]
- victims who approached the FBI to report crimes;[109]
- business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy";[110]
- college students participating in a "Collegiate Academy";[111]
- police officer candidates;[112]
- colleagues and relatives of the FBI agent performing the search;[113]
- people traveling through an airport during a particular date range who were either traveling to or returning from a foreign country;[114]
- registered competitors in an athletic event;[115]
- visitors to a government facility;[116]
- potential FBI sources;[117] and

---

[104] DOJ & ODNI, Semiannual Assessment December 2021, *supra* note 101, at 58.
[105] 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.
[106] [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 29.
[107] DOJ & ODNI, Semiannual Assessment December 2021, *supra* note 101, at 61.
[108] [Redacted], No. [Redacted] (FISA Ct. November 18, 2020), *supra* note 91, at 40.
[109] *Id.*
[110] *Id.* at 39.
[111] [Redacted], No. [Redacted] (FISA Ct. December 6, 2019), *supra* note 85, at 66.
[112] *Id.*
[113] [Redacted], 402 F. Supp. 3d 45, *supra* note 92, at 78.
[114] 2023 PCLOB 702 Report, *supra* note 18, at 148.
[115] *Id.* at 149.
[116] *Id.*; [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 32.
[117] 2023 PCLOB 702 Report, *supra* note 18, at 149–50; [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 27–28.

- an individual who invited the agent that conducted the search to speak at their company.[118]

The government has heralded "significant improvement" in FBI compliance in the past two years,[119] but the reality is much more nuanced. For one thing, even after the FBI implemented many of the reforms that were ultimately codified in RISAA and compliance rates began to increase, serious abuses continued. For instance, the FISA Court's April 2023 opinion revealed that FBI agents had conducted improper queries for the communications of a U.S. Senator, a state senator, and a state court judge who contacted the FBI to report civil rights violations by a local police chief.[120] In light of the FBI's poor compliance history, OIG stated in its October 2025 report that it was "not able to conclude . . . that FBI's querying compliance issues are entirely in the past."[121]

More fundamentally, FBI has not produced complete data on its queries. As discussed above, the FBI in 2024 (and possibly before then) employed at least one querying tool that agents wrongly treated as exempt from the statutory and court-ordered requirements applicable to queries. At a minimum, as OIG found, the queries conducted using this tool "likely did not comply with the pre-approval, written justification, and recordkeeping requirements for U.S. person queries" because the system did not prompt users to take these steps.[122] Nor did NSD conduct the statutorily required audit of these queries. These failures alone constitute significant and possibly extensive violations of RISAA.

Moreover, because the system "had not been configured to record each use of the participants filter, NSD did not have historical data that would enable NSD to determine whether each use of the function complied with the query standard."[123] It is possible, as OIG acknowledged, that "these queries may have included sensitive queries or queries designed solely to retrieve evidence of a crime," as well as "an unspecified number of [other] compliance incidents."[124] Indeed, given that FBI agents were not following the pre-approval, written justification, and recordkeeping requirements — requirements that the government itself credits for improved compliance rates — one would expect to see a higher rate of violations among

---

[118] See Department of Justice and Office of the Director of National Intelligence, *28th 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* 54, February 2024, https://www.intel.gov/assets/documents/702-documents/declassified/28th_Joint_Assessment_for_PUBLIC_1.15.25.pdf.

[119] *See, e.g.*, Federal Bureau of Investigation, "Release of 2023 Foreign Intelligence Surveillance Court Opinion Highlights FBI's Improved Section 702 Query Compliance," July 21, 2023, https://www.fbi.gov/news/press-releases/release-of-2023-foreign-intelligence-surveillance-court-opinion-highlights-fbis-improved-section-702-query-compliance.

[120] *In re DNI/AG 702(h) Certification 2023-A*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, *supra* note 96, at 86.

[121] 2025 OIG Report, *supra* note 51, at 51.

[122] *Id.* at 49.

[123] *Id.*

[124] *Id.* at 48, 49.

these queries.[125] And the fact that all of these queries have escaped review means that significant abuses could well have gone undetected.

Without complete data on how many queries were conducted in 2024 or whether these queries complied with applicable standards, Congress cannot evaluate the FBI's querying record post-RISAA. As of the March 2025 FISA Court opinion, NSA was "coordinating with FBI to assess what records of the use of this functionality may have been generated and maintained."[126] Congress should exercise active oversight to ensure that the FBI is providing any and all information in its possession about the use of this querying tool, and it should not reauthorize Section 702 until it is has a more complete picture of the FBI's querying practices since RISAA's enactment.

B. Other Violations

The FBI's querying violations in recent years are merely one subset of the compliance problems that have attended the government's implementation of Section 702. The program's seventeen-year history has been marked by repeated, significant, and sometimes systemic failures to comply with statutory requirements or court orders. These failures have taken place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, access, dissemination, and retention.

My written testimony before this Committee in July 2023 highlighted several of the most notable compliance failures that occurred between 2008-2023. These include the NSA's systemic violations of querying restrictions over a period of nearly a decade; the FBI's over-retention of Section 702 data in violation of minimization requirements; the NSA's "institutional lack of candor" (as described by the FISA Court); and the FBI's widespread non-compliance with procedures designed to ensure the accuracy of its FISA Court submissions.[127] Since that testimony, serious compliance incidents have only continued to emerge.

One such incident involved repeated misapplication of the NSA's tasking standards (the rules governing when the NSA can target someone and collect their communications).[128] A review by the NSA Office of the General Counsel and NSD identified at least 571 tasking errors

---

[125] U.S. person queries conducted using this tool run against a pool of communications obtained through an initial query that retrieves communications associated with a particular case file or target. The government asserts that *if* that initial query was compliant, "most, but not necessarily all, queries conducted through the [participants filter] likely would have satisfied the applicable query standard" because the second query is "narrower" than the first. 2025 OIG Report, *supra* note 51, at 49. This reasoning makes little sense. While the retrieval of *all* of a foreign target's communications (through the initial query) might reasonably be expected to yield some foreign intelligence, it does not follow that communications with specific U.S. person participants can be assumed to contain foreign intelligence.

[126] *In re DNI/AG 702(h) Certifications 2025-A, 2025-B, 2025-C*, Nos. 702(j)-25-01, 702(j)-25-02, 702(j)-25-03, *supra* note 17, at 40.

[127] *See Fixing FISA, Part II, Hearing Before the H. Comm. on the Judiciary, Subcomm. On Crime and Federal Government Surveillance*, 118th Cong. 17–22, July 14, 2023 (testimony of Elizabeth Goitein, Senior Director, Liberty and National Security Program, Brennan Center for Justice), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/goitein-testimony.pdf..

[128] *In re DNI/AG 702(h) Certification 2023-A*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, *supra* note 96, at 94–95.

in a single office, errors that the NSA attributed to a "misunderstanding" of tasking guidance provided in 2016 and 2018.[129] The review concluded that "many targeting decisions had been improper because the target was not reasonably expected to possess or receive, and was not likely to communicate, foreign intelligence information related to [redacted]."[130]

The implementation of newly approved travel-vetting procedures has also been accompanied by several compliance incidents, including improper U.S. person queries. The FISA Court recounted one incident involving an undisclosed number of violations of the rules limiting queries related to certain visa applications from individuals "expected to be located in the United States and with United States home addresses."[131] In another incident, the NSA conducted multiple non-compliant queries related to applications submitted by legal permanent residents, who are U.S. persons under the law.[132]

In 2024, the CIA disclosed a significant compliance issue with its main FISA repository. The CIA is required by statute to include a technical procedure to record each U.S. person query term used,[133] and CIA querying procedures require personnel to document the justification for U.S. person queries.[134] For an undisclosed period of time (but at least three years), users were able to conduct certain free-text queries of the CIA's main FISA repository without being prompted to specify whether the query used a U.S.-person term or to enter a justification for any U.S. person queries.[135] The CIA's review of such free-text queries conducted between 2021 and April 2024 identified over 10,000 queries that CIA assessed could have included U.S. person query terms conducted without these prompts.[136]

Perhaps most concerning, the FISA Court's September 2024 opinion, issued five months after RISAA's passage, includes six pages of entirely redacted material under the heading: "Reported Intentional Violations at [Redacted]."[137] Due to the redactions, it is impossible to ascertain the agency at which the violations were reported or which aspect of Section 702 implementation they involved. The FISA Court cautioned that "[t]he underlying facts are still

---

[129] *Id.*
[130] *Id.*
[131] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C, and Predecessor Certifications*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, and predecessor dockets, at 94 (FISA Ct. September 17, 2024), https://www.intelligence.gov/assets/documents/702-documents/declassified/2024/2024_Sep_702_Cert_FISC_Opinion_9-17-24_Redacted.pdf.
[132] *In re DNI/AG 702(h) Certification 2023-A*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, *supra* note 96, at 51, n.36; *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, *supra* note 131, at 69.
[133] 50 U.S.C. § 1881a(f)(1)(B).
[134] *See* Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Querying Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § IV.B., July 18, 2024, https://www.intel.gov/assets/documents/702-documents/declassified/2024/2024_Sep_702_Cert_Amended_CIA_Querying_Procedures_Redacted.pdf.
[135] *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, *supra* note 131, at 102.
[136] *Id.* The FISA Court assessed that "the probable number of actual U.S. person queries was substantially lower." *Id.* at 103 n.75. However, the court's basis for its conclusion is redacted.
[137] *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, *supra* note 131, at 96–102.

being investigated" and so the misconduct described in the opinion "should be understood as alleged, not established."[138] Nonetheless, such an extensive recounting of reported *intentional* misconduct is cause for significant concern.

The long, unbroken string of violations detailed here and in my 2023 testimony paints a vivid and unmistakable picture of foreign intelligence surveillance operating outside the constraints of the law. It is unclear whether the violations are occurring because agencies are not putting sufficient sustained effort into compliance, because they lack the technical capability to ensure compliance, or for some other reason. It may be the case that collection programs have become so massive in scope, and the systems for retaining and processing the data so technically complex, that it is simply impossible to achieve consistent compliance with the rules governing their use. Whatever the explanation, the widespread and continuing failures to honor privacy protections should give lawmakers pause as the government once again asks Congress to entrust the government with immense quantities of Americans' private data.

IV. Needed Reforms

The above discussion makes clear that Congress should not reauthorize Section 702 without far-reaching reforms. Section 702 itself should be amended to close the backdoor search loophole, narrow the definition of "electronic communication service provider," and end suspicionless queries for travel-vetting, among other changes. For these reforms to be effective, however, Congress must go beyond Section 702. It also must address broader problems in FISA by strengthening the role of *amici curiae* in FISA Court proceedings and otherwise bolstering judicial oversight. Finally, Congress should address statutory gaps and outdated laws that could allow warrantless surveillance of Americans to migrate from backdoor searches of Section 702 data to other methods, such as the purchase of Americans' sensitive information from data brokers.

A. Protecting Americans' Privacy Under Section 702

1. Close the Backdoor Search Loophole

The starting point for any reauthorization of Section 702 must be an end to warrantless searches of Americans' "incidentally" obtained communications. Specifically, Congress should require all government agencies to obtain a probable-cause order — i.e., either a warrant or a Title I FISA Court order — before running queries designed to extract communications content or other Fourth Amendment-protected information (such as geolocation data) of or concerning U.S. persons. What makes warrantless surveillance under Section 702 lawful in the first instance is the government's certification that it is targeting *only* foreigners. That representation becomes a semantic sleight of hand when the government simultaneously adopts procedures allowing it to search the data for particular Americans' communications.

Section 702 surveillance also can result in the "incidental" collection of other types of sensitive data that do not receive full Fourth Amendment protection but that Congress has chosen to protect by statute. Depending on the information in question, the government ordinarily may

[138] *Id.* at 96.

be required to obtain a court order (e.g., under 18 U.S.C. § 2703(d) or Section 215 of the USA Patriot Act[139]) or a subpoena (e.g., under § 2703(c)(2) or with a National Security Letter) to obtain it. Before performing a U.S. person query of such data, agencies should be required to follow the legal process that would apply if the agencies were collecting the data in the first instance.

During the last Section 702 reauthorization, Congress considered an amendment that would have required agency officials to obtain a warrant or a FISA Title I order before accessing the content of U.S. persons' communications, with exceptions for consent, exigent circumstances, and certain cybersecurity-related queries. (The amendment failed by the narrowest possible margin: a tied vote of 212-212.[140]) Those who opposed this reform claimed it would harm national security.[141] They will no doubt make the same claim during the debate over next year's reauthorization. But the program's seventeen-year track record shows otherwise.

The government has provided multiple examples in which *surveillance of foreign targets* provided key information about cyberattacks, espionage, and fentanyl trafficking. By contrast, after a thorough review of all of the relevant classified and unclassified information, the PCLOB found in its 2023 report that "there was little justification provided to the Board on the relative value of the close to 5 million searches [U.S. person queries] conducted by the FBI from 2019 to 2022."[142] The government cited only a handful of instances in which backdoor searches for Americans' communications had been useful. In each of those cases, it appeared that the government could have obtained a warrant, gotten the consent of the subject of the search (for instance, where the search was conducted for the purpose of identifying and protecting potential

---

[139] Although Section 215 expired in 2020, it is still available for investigations commenced before the provision expired, as well as investigations into actions that took place before the expiration. *See* USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. 109-177, § 102(b)(2), 120 Stat. 192, 195 (2006), https://www.govinfo.gov/content/pkg/PLAW-109publ177/pdf/PLAW-109publ177.pdf (as amended by Pub. L. 116-69, § 1703(a), 133 Stat. 1134, 1143 (2019), https://www.congress.gov/116/plaws/publ69/PLAW-116publ69.pdf).

[140] H. Amdt. 876, H.R. 7888, 118th Cong. (2024), https://www.congress.gov/amendment/118th-congress/house-amendment/876.

[141] In the same vein, FBI officials have occasionally suggested that requiring a warrant or FISA Title I order for U.S. person queries would be tantamount to re-building "the wall." *See* Christopher Wray Director, Federal Bureau of Investigation, "*Defending the Values of FISA Section 702*," October 13, 2017, https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702; Privacy and Civil Liberties Oversight Bd., *PCLOB Public Forum on FISA Section 702*, YouTube, January 12, 2023, at 1:57:28 (comments of Mike Herrington, Senior Operations Advisor, FBI), https://www.youtube.com/watch?v=AZvaimMTqio&t=357s. This notion is utterly baseless. "The wall" refers to a set of pre-9/11 procedures that — in practice, if not on paper — restricted intelligence officials' ability to share identified threat information with criminal prosecutors. *See* Barbara A. Grewe, Senior Counsel for Special Projects, Commission on Terrorist Attacks Upon the United States, *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations*, August 20, 2004, https://irp.fas.org/eprint/wall.pdf.

The information in question was obtained under Title I of FISA, which means the government had *already* secured a probable-cause order at the point in the case where "the wall" kicked in. *See id.* at 29. Moreover, requiring a warrant for U.S. person queries would in no way inhibit the sharing of threat information — including information about Americans — that officials encountered in the course of querying and reviewing *foreigners'* communications. Any such discovery would be analogous to the "plain view" exception to the Fourth Amendment's warrant requirement. *See generally* Coolidge v. New Hampshire, 403 U.S. 443 (1971) (discussing "plain view" exception); Horton v. California, 496 U.S. 128 (1990) (same). What the Fourth Amendment cannot tolerate is the government collecting information without a warrant or Title I order with the intent of mining it for use against Americans.

[142] 2023 PCLOB 702 Report, *supra* note 18, at 190.

victims of malicious foreign activity[143]), or invoked the emergency exception — a point confirmed by the Chair of the PCLOB.[144]

Some defenders of warrantless queries may argue that RISAA already closed the backdoor search loophole by prohibiting FBI queries for the sole purpose of retrieving evidence of a crime. As noted above, however, that prohibition applies only to a tiny fraction of U.S. person queries. Indeed, the worst abuses we have seen under Section 702 thus far have been couched as efforts to obtain foreign intelligence, not evidence of a crime — including queries of more than 100 U.S. persons involved in the protests against the police killing of George Floyd;[145] the FBI's batch query for the communications of more than 19,000 donors to a single congressional campaign;[146] the FBI's query using the name of then-U.S. Congressman Darrin LaHood;[147] and the thousands of queries aimed at people or groups suspected of involvement in the January 6, 2021 attack on the U.S. Capitol.[148]

Opponents of reform may claim that RISAA has reduced the FBI's number of U.S. person queries and its rate of non-compliance to acceptable levels. Any such claim would rest on a flawed premise. As noted above, the FBI failed to track all of its queries — itself a major compliance issue. As a result, the number of U.S. person queries and the overall compliance rate for 2024 remain unknown.

But even if the FBI had conducted only a handful of U.S. person queries and committed no violations of its querying procedures last year, that would not obviate the need for a warrant. An agency's internal determination that a search of Fourth Amendment-protected data is reasonably likely to yield foreign intelligence is not the same as, and cannot substitute for, a showing of probable cause before a neutral magistrate. As the Supreme Court stated in a Fourth Amendment case where the government had argued that its protocols for searching cell phones were sufficient to protect Americans' privacy: "The founders did not fight a revolution to gain the right to government agency protocols."[149]

---

[143] In opposing the proposed warrant requirement, the government relied heavily on its use of U.S. person queries for "defensive" purposes — i.e., to protect potential victims. But the need to protect victims is hardly unique to the Section 702 context. Domestic law enforcement agencies are routinely faced with this task. They manage to keep the American public safe using investigative techniques that comport with the Fourth Amendment — including obtaining the consent and cooperation of potential victims themselves, or invoking the "exigent circumstances" exception to the warrant requirement in cases where victims are in imminent danger. There is no "victim" exception to the Fourth Amendment, however, nor does the Constitution draw any distinction between "offensive" or "defensive" searches or seizures.

[144] 2023 PCLOB 702 Report, *supra* note 18, at A6–A7.

[145] The FBI maintained (wrongly) that there was a "reasonable basis to believe the queries would return foreign intelligence." [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 27.

[146] This batch query was based on an allegation that the campaign was a target of "foreign influence." *Id.* at 29.

[147] The query was reportedly based on concerns that "a foreign government had targeted him as part of an espionage or covert influence intelligence operation." Charlie Savage, "FBI Feared Lawmaker Was Target of Foreign Intelligence Operation," New York Times, April 13, 2023, https://www.nytimes.com/2023/04/13/us/politics/fbi-darin-lahood.html.

[148] The FBI ran these queries seeking evidence of "foreign influence." [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 29.

[149] Riley v. California, 573 U.S. 373, 398 (2014).

In fact, if the FBI indeed conducted "only" 5,518 warrantless searches for Americans' private communications in 2024, that would actually bolster the case for a warrant requirement. When the number of annual U.S. person queries stood at more than 200,000, the government argued that a warrant requirement would be unworkable and overwhelm the courts. That argument was unpersuasive, given that most legislative warrant requirement proposals would allow the FBI to determine whether the U.S. person was in communication with a target *before* obtaining the warrant. By the government's own statistics, this step would reduce the number of required warrant applications by 98%.[150] The government's "unworkability" argument is even less persuasive if the actual number of U.S. person queries today is closer to 5,000, thus requiring the FBI to obtain warrants in roughly 110 cases. The number of FISA Title I order applications submitted by the government each year routinely fluctuates by more than this amount.[151]

A warrant requirement would also solve a potential problem identified by the government during OIG's review. FBI employees interviewed by OIG expressed "concern" that "the extensive oversight" put in place in recent years "has caused 'audit fatigue' that has reduced the willingness of some FBI personnel to query Section 702-acquired information altogether."[152] In addition to the "administrative burden" of obtaining attorney approval and keeping records of U.S. person queries, agents are reportedly "concerned that they may be subject to disciplinary actions for running noncompliant queries" and may therefore refrain from conducting queries that would in fact be justified.[153]

The simplest way to address this purported issue[154] without a resurgence of querying violations is by placing the burden of gatekeeping these searches where it belongs: with a court. This would reduce the need for the multiple layers of internal oversight that have been established in a futile effort to replicate the function of judicial approval. It would also take away any motive for excessive caution; the only penalty if an agent submitted an application that turned out to lack sufficient basis would be the court's denial of the application. Agents would be free to do their jobs — i.e., to vigorously pursue their investigations consistent with the law and their professional obligations — while the courts would perform *their* job of determining whether the government has a lawful basis for searching Americans' private communications.

2. Fix the Definition of "Electronic Communication Service Provider"

In addition to closing the backdoor search loophole, Congress should walk back its radical expansion of the definition of "electronic communication service provider." As discussed above, the impetus for expanding the definition was a ruling by the FISA Court that the provision did not cover a particular type of provider.[155] The administration deliberately pressed for an overbroad solution in order to obscure the type of provider at issue. Alarmed at the

---

[150] 2023 PCLOB 702 Report, *supra* note 18, at 168, B-16.
[151] *See, e.g.*, ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 17.
[152] 2025 OIG Report, *supra* note 51, at 34.
[153] *Id.* at 48.
[154] The extent of this problem is unclear. The witnesses interviewed by OIG were relaying their perceptions of other agents' concerns; none of the witnesses acknowledged limiting their own searches as a result of the new oversight measures. *Id.* at 47.
[155] *See In re: Petition to Set Aside or Modify Directive Issued to [Redacted]*, Nos. [Redacted], *supra* note 63.

change, which the House had hastily adopted, several senators threatened to scuttle the reauthorization of Section 702. With the sunset fast approaching, the then-chair of the Senate Intelligence Committee, Senator Warner, conceded that the provision "could have been drafted better,"[156] but urged his colleagues to vote for reauthorization and promised to work to "improve the definition . . . before the next sunset."[157] No such improvement has passed to date, and the dangerously broad definition remains law.

The optimal solution would be for the administration to declassify the type of provider at issue, which would remove any concerns about Congress limiting the new definition to that type of provider. Declassifying the information would cause no harm to national security because it is already squarely in the public domain. The *New York Times* revealed in April 2024 that the relevant FISA Court decisions involved a data center for cloud computing.[158] That information has been confirmed by authoritative sources: During the Senate debate over this provision, multiple senators with access to classified FISA Court opinions, including Senator Warner himself, [159] either stated or implied that the provision was intended to address data centers.

Even if the administration fails to declassify this information, however, Congress can simply pass legislation stating that the new definition may be applied only to data centers for cloud computing. If the legislation does not expressly tie this change to the FISA Court opinions, it would not directly be revealing classified information. And while people might infer from the change that the FISA Court opinions in question addressed data centers, that inference can already be drawn from other sources, including the public statements of members of Congress.

Alternatively, Congress could adopt language proposed by Senator Warner that would limit the new definition to providers of "the type of service at issue in the covered opinions"—with "covered opinions" defined to include the two specific FISA Court opinions holding that a specific type of provider was not covered.[160] This solution is far from ideal, as incorporating classified opinions by reference creates a type of "secret law."[161] Among other concerns, companies that receive directives from the government requiring them to assist with Section 702 surveillance would face serious limitations in their ability to identify and challenge unlawful directives.[162] It would nonetheless be preferable to the status quo, under which NSA personnel may compel surveillance assistance from nearly every business and organization in the country.

3. End Suspicionless Queries for Travel Vetting

Congress should repeal the provision of RISAA authorizing suspicionless searches of Section 702 data for the communications of anyone seeking to travel to the United States. This invasive measure is wholly unnecessary given the multiple vetting mechanisms already in place

---

[156] 170 Cong. Rec. S2836 (daily ed. April 18, 2024) (statement of Sen. Warner).
[157] 170 Cong. Rec. S2837 (daily ed. April 18, 2024) (statement of Sen. Warner).
[158] *See* Charlie Savage, "Secret Rift," supra note 64.
[159] *See generally* 170 Cong. Rec. S2833–37 (daily ed. April 18, 2024).
[160] S. 4443, 118th Cong. § 1202 (2024).
[161] *See* Elizabeth Goitein, "Secret Law is not the Solution to an Overbroad Surveillance Authority," Brennan Center for Justice, June 11, 2024, https://www.brennancenter.org/our-work/analysis-opinion/secret-law-not-solution-overbroad-surveillance-authority.
[162] *See id.*

to ensure that visitors to this country do not threaten our national security. People should be able to vacation, work, or study in the U.S. without automatically exposing their private communications to U.S. government scrutiny. Allowing suspicionless queries for visa applicants' private communications unnecessarily intrudes on the privacy of such applicants, as well as the privacy of U.S. persons whose communications may be retrieved in response to such queries. Moreover, as noted above, the travel vetting program already has suffered from compliance problems leading to multiple improper U.S. person queries.

B. Bolstering Judicial Review by Restoring and Strengthening the Role of *Amici Curiae*

The FISA Court reviews applications to conduct electronic surveillance under Title I of FISA and to engage in other types of collection of Americans' information. The Court also approves Section 702 certifications and procedures and conducts general oversight of that program.

FISA Court proceedings are non-public and conducted *ex parte*, meaning the government is the only party.[163] The secrecy and one-sided nature of such proceedings are inherently problematic. When judges hear only from one party and their decisions in favor of that party are never subject to appeal, there is a higher risk of skewed and erroneous decisions — as evidenced by the FISA Court's approval of the NSA's program to collect Americans' phone records in bulk, which three regular federal courts subsequently ruled unlawful.[164]

Congress attempted to address this problem in the 2015 USA FREEDOM Act by creating a panel of security-cleared *amici curiae* who could provide a perspective other than the government's in significant cases. This was an important step, but various factors have limited its effectiveness. *Amici* are still left out of too many important cases. In those cases in which they do participate, they lack sufficient access to the underlying materials. And they have no means of securing an appeal if the Court decides in favor of the government.

RISAA partially addressed one of these problems by creating a presumption of *amicus* participation in Section 702 certification approvals. However, two other changes made by RISAA significantly undermined the effectiveness of *amici*. First, *amici* are now "limited to addressing the specific issues identified by the court."[165] The value of *amici* derives in significant part from their ability to raise issues and arguments the court has not considered. This provision places a handicap on *amici* that defeats the very purpose of their participation.

Second, the Court must "to the maximum extent practicable appoint an individual who possesses expertise in both privacy and civil liberties *and intelligence collection*" (emphasis added).[166] The practical consequence of this provision is that *amici* selection is heavily weighted

---

[163] *See* U.S. Foreign Intelligence Surveillance Court, "About the Foreign Intelligence Surveillance Court," accessed December 4, 2025, https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.
[164] United States v. Moalin, 973 F.3d 977 (9th Cir. 2020); American Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).
[165] 50 U.S.C. § 1803(i)(4)(A).
[166] 50 U.S.C. § 1803(i)(2)(B).

towards former government personnel, who may well come into the proceedings with institutional bias. The views of the government are more than adequately represented in FISA Court proceedings. Indeed, the need for perspectives *other* than the government's is what prompted the creation of the *amici* program in the first place.

Congress should repeal these provisions and strengthen *amici* participation by enacting the reforms to FISA Court proceedings set forth in the "Lee-Welch" amendment (previously known as the "Lee-Leahy" amendment).[167] Senators Mike Lee and Patrick Leahy initially offered this amendment to the USA FREEDOM Reauthorization Act of 2020.[168] Although Congress failed to pass the reauthorization bill, the amendment passed by an overwhelming bipartisan vote of 77-19.[169]

The amendment seeks to ensure that *amici* can weigh in on the most significant cases (in addition to Section 702 certification approvals), including those that involve public officials, political candidates, religious or political organizations, or the media; that *amici* have access to the materials they need to do their job, including exculpatory materials in the government's possession; that *amici* can petition the FISA Court to certify questions for appeal; and that the government has in place FISA Court-approved procedures to ensure the accuracy of its submissions. There is no legitimate argument against such basic accountability-enhancing measures, which is why the amendment received such a strong showing of support in 2020.

C. Closing the Data Broker Loophole to Prevent Warrantless Surveillance of Americans

It is critical that Congress not consider Section 702, or even FISA itself, in isolation. The authorities provided by FISA are part of a large and complex ecosystem of often-overlapping surveillance authorities. In many cases, the government may obtain the same or equivalent information using different techniques (for example, the government may place a wiretap or it may compel production of communications from a service provider) and can choose among them on the basis of convenience. If one avenue of surveillance is closed off or restricted, it is often possible for the government to simply turn to another — or to exploit gaps in the network of surveillance laws to acquire the information without any statutory authorization whatsoever.

One such gap exists within FISA's "exclusivity" provision, which provides that FISA, along with various criminal law provisions authorizing electronic surveillance, "shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted."[170] FISA's highly technical definition of "electronic surveillance"[171] does not cover the collection of many types of records containing communications metadata and other sensitive non-contents information, such as geolocation data. The government can thus claim that certain provisions of FISA — including Section 702

[167] S. Amdt. 1840, H.R. 7888, 118th Cong. (2024), https://www.congress.gov/amendment/118th-congress/senate-amendment/1840/text.
[168] S. Amdt. 1584, H.R. 6172, 116th Cong. (2020), https://www.congress.gov/amendment/116th-congress/senate-amendment/1584/text.
[169] *Id.* (as agreed to in Senate, May 13, 2020).
[170] 50 U.S.C. § 1812.
[171] 50 U.S.C. § 1801(f).

itself, to the extent it authorizes collection activities that do not qualify as "electronic surveillance," as well as the provisions governing physical searches and the collection of some third-party records — are *not* the exclusive means by which such activities may be conducted, and that the government may ignore the restrictions and procedures contained in such provisions.

There is ample reason to believe that's happening now. In 2020, Congress was debating whether to reauthorize Section 215, the so-called "business records" provision of FISA that the NSA relied on to collect Americans' phone records in bulk. Senator Richard Burr — who then chaired the Senate Select Committee on Intelligence — warned that if Section 215 expired, "the president under [Executive Order] 12333 authority can do all of this without Congress's permission, with no guardrails."[172] The authority indeed expired (although pending investigations were grandfathered), and the conspicuous absence of any serious government efforts to reinstate it strongly suggests that the government is obtaining the same information through other means.

The information that the government may obtain outside of FISA can be extremely sensitive. Take the phone records that were the subject of the NSA's bulk collection program. After Edward Snowden's disclosure of the program, experts explained how communications "metadata" — a term many Americans had never encountered — could be crunched to reveal people's associations, activities, and even beliefs.[173] This understanding led lawmakers to end the bulk collection program and ultimately Section 215 itself. In 2020, the Senate voted overwhelmingly in favor of a bipartisan amendment to impose a warrant requirement for internet search and browsing records, noting that they, too, reveal Americans' private thoughts and preferences.[174] Geolocation information can similarly reveal the most intimate aspects of people's private lives. Indeed, for that very reason, the Supreme Court in *Carpenter v. United States* (2018) held that police need a warrant to obtain a week's worth of geolocation information from a cell phone company.[175]

If the government wanted to obtain such information without adhering to FISA, one workaround would be to purchase it from data brokers. Such purchases have become an increasingly common practice in the federal government.[176] Multiple agencies have reportedly purchased access to Americans' cell phone location information and other sensitive data,

---

[172] *See* Richard Burr, "Sen. Burr Claims EO 12333 Permits Mass Surveillance 'Without Congress's Permission,'" U.S. Senate, streamed live on March 12, 2020, C-SPAN, 00:15, https://www.c-span.org/clip/us-senate/user-clip-sen-burr-claims-eo-12333-permits-all-of-this-without-congresss-permission/4860931.
[173] Declaration of Professor Edward W. Felten at 16, American Civil Liberties Union v. Clapper, 785 F. Supp. 2d 724 (S.D.N.Y. 2013), *available at* https://s3.documentcloud.org/documents/781486/declaration-felten.pdf.
[174] Niels Lesniewski, "Senate Amends Surveillance Bill to Add New Oversight," Roll Call, May 13, 2020, https://rollcall.com/2020/05/13/senate-may-have-the-votes-to-limit-surveillance-of-browser-history/.
[175] Carpenter v. United States, 585 U.S. 296 (2018).
[176] *See* Emile Ayoub and Elizabeth Goitein, "Closing the Data Broker Loophole," Brennan Center for Justice, February 13, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

including the Federal Bureau of Investigation,[177] the Drug Enforcement Administration,[178] the National Security Agency,[179] multiple components of the Department of Homeland Security[180] (including Immigration and Customs Enforcement[181] and Customs and Border Protection[182]), the Secret Service,[183] and the Department of Defense.[184] Even the Internal Revenue Service, according to the Wall Street Journal, "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."[185] In one particularly disturbing example, Vice News reported that "[m]ultiple branches of the U.S. military have bought access to a powerful internet monitoring tool that claims to cover over 90 percent of the world's internet traffic, and which in some cases provides access to people's email data, browsing history, and other information such as their sensitive internet cookies."[186]

---

[177] *See* Sara Morrison, "A Surprising Number of Government Agencies Buy Cellphone Location Data. Lawmakers Want to Know Why," *Vox*, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; Ashley Belanger, "FBI Finally Admits to Buying Location Data on Americans, Horrifying Experts," *Ars Technica*, March 9, 2023, https://arstechnica.com/tech-policy/2023/03/fbi-finally-admits-to-buying-location-data-on-americans-horrifying-experts/; Byron Tau, "FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do," Wall Street Journal, March 10, 2023, https://www.wsj.com/articles/fbi-once-bought-mobile-phone-data-for-warrantless-tracking-other-agencies-still-do-ad65ebe9.

[178] *See* Morrison, "A Surprising Number," *supra* note 177.

[179] Charlie Savage, "N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says," New York Times, January 25, 2024, https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html. The agency admitted that it purchased Americans' communications metadata from data brokers. Much like geolocation data, this information, when accumulated, can reveal intimate information like associations, habits, and beliefs. *See* American Civil Liberties Union v. Clapper, 785 F. Supp. 2d 724 (S.D.N.Y. 2013).

[180] Joseph Cox, "Airlines Don't Want You to Know They Sold Your Flight Data to DHS," *404 Media*, June 10, 2025, https://www.404media.co/airlines-dont-want-you-to-know-they-sold-your-flight-data-to-dhs/.

[181] *See* Joseph Cox, "ICE to Buy Tool that Tracks Locations of Hundreds of Millions of Phones Every Day," *404 Media*, September 30, 2025, https://www.404media.co/ice-to-buy-tool-that-tracks-locations-of-hundreds-of-millions-of-phones-every-day/; Paul Blest, "ICE Is Using Location Data From Games and Apps to Track and Arrest Immigrants, Report Says," *Vice*, February 7, 2020, https://www.vice.com/en/article/v7479m/ice-is-using-location-data-from-games-and-apps-to-track-and-arrest-immigrants-report-says.

[182] *See* Joseph Cox, "ICE to Buy Tool," *supra* note 181; Paul Blest, "ICE Is Using Location Data," *supra* note 181.

[183] *See* Joseph Cox, "Secret Service Bought Phone Location Data from Apps, Contract Confirms," *Vice*, August 17, 2020, https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.

[184] *See* Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," New York Times, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

[185] Byron Tau, "IRS Used Cellphone Location Data to Try to Find Suspects," Wall Street Journal, June 19, 2020, https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815. Although more is known about the practice at the federal level, state and local law enforcement also have been caught buying Americans' personal information from data vendors. *See* Kristina Cooke, "U.S. Police Used Facebook, Twitter Data to track Protestors - ACLU," Reuters, October 11, 2016, https://www.reuters.com/article/us-social-media-data-idUSKCN12B2L7; Bennett Cyphers, "How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale," Electronic Frontier Foundation, August 31, 2022, https://www.eff.org/deeplinks/2022/08/how-law-enforcement-around-country-buys-cell-phone-location-data-wholesale.

[186] Joseph Cox, "Revealed: U.S. Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data," *Vice*, September 21, 2021, https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data. The Federal Trade Commission later brought enforcement actions against one of those data brokers, Outlogic (formerly X-mode), for selling location data collected from popular prayer apps. Federal Trade Commission [hereinafter FTC], "FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data," January 9, 2024, https://www.ftc.gov/news-events/news/press-

A declassified report to ODNI released in June 2023 confirmed the extent of this practice, finding that intelligence agencies have been acquiring vast amounts of Americans' personal information from commercial entities.[187] The report explained that this commercially available information "includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection."[188] It also warned that intelligence agencies have failed to keep track of the information they are acquiring and how they are using it.[189] Exacerbating these concerns, ODNI earlier this year reportedly proposed consolidating all of this commercially acquired information into a single "data consortium" accessible to intelligence agencies and potentially other agencies.[190]

The warrantless collection of Americans' cell phone location information — potentially in massive amounts — would seem to violate the Supreme Court's holding in *Carpenter*. But agency lawyers have found a way around the case law. They have construed *Carpenter* to apply only when the government *compels* companies to disclose location information.[191] When the government merely *incentivizes* such disclosure — by writing a big check — the warrant requirement simply disappears. At that point, the argument goes, the government may obtain this Fourth Amendment-protected information in unlimited quantities without any individualized suspicion of wrongdoing, let alone probable cause and a warrant.

Agencies maintain that warrants are unnecessary even when a data broker obtains location information from mobile applications without the users' awareness.[192] In some instances, agencies have made disingenuous claims that consumers consent to the selling of their data by accepting applications' often-opaque terms of service. In emails obtained by 404 Media, for example, officials argued that the Secret Service could broadly collect location data without a

---

releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data. The FTC followed with enforcement actions against data brokers Gravy Analytics, Venntel, and Mobilewall — all of whom reportedly sold location data to government agencies. *See* FTC, "FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers; FTC, "FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data.

[187] Panel on Commercially Available Information, Office of the Director of National Intelligence Senior Advisory Group, *Report to the Director of National Intelligence*, January 27, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [hereinafter ODNI, *Report to ODNI*].

[188] *Id.* at 2–3, 14.

[189] *Id.* at 2, 21, 36 (finding that the intelligence community "does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements" and "cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI").

[190] Sam Biddle, "U.S. Spy Agencies are Getting a One-Stop Shop to Buy Your Most Sensitive Personal Data," *The Intercept*, May 22, 2025, https://theintercept.com/2025/05/22/intel-agencies-buying-data-portal-privacy/.

[191] *See* Savage, "Intelligence Analysts," *supra* note 184; Hamed Aleaziz and Caroline Haskins, "DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People," *BuzzFeed News*, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[192] *See* Savage, "Intelligence Analysts," *supra* note 184; Aleaziz and Haskins, "DHS Authorities," *supra* note 191.

warrant based on a theory of user consent, even while acknowledging that terms of service often do not indicate that user data may be sold to the federal government.[193]

The government's attempts to bypass *Carpenter* and to infer consent in the absence of meaningful disclosure to customers are legal sophistry, but it could take years for the courts to resolve these issues. In the meantime, the government has effectively sidelined the Fourth Amendment when it comes to data purchases.

Another apparent barrier to these purchases — the Electronic Communications Privacy Act (ECPA) — has also proven inadequate. ECPA prohibits phone and Internet companies from disclosing customer records to government agencies unless the government produces a warrant, court order, or subpoena.[194] But the law is woefully outdated. It does not cover digital data brokers or many app developers, for the simple reason that they largely did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections.[195] Companies that are prohibited from selling their data to the government can simply sell it to a data broker — a disturbingly common practice[196] — and the data broker can resell the same information to the government, at a handsome profit. The information is effectively laundered through a middleman.

Current agency guidelines are an inadequate replacement for the constitutional and statutory protections that are being sidestepped. For example, ODNI released a framework in May 2024 establishing uniform baseline standards for how intelligence agencies should categorize, acquire, and handle commercially available information ("CAI").[197] Although the framework articulates laudable general principles — e.g., "The protection of privacy and civil liberties, and compliance with procedures governing the conduct of intelligence activities, shall be integral considerations . . . in an IC element's access to and collection and processing of CAI"[198] — its subjective, discretionary, and exception-riddled standards risk making it a box-

---

[193] Joseph Cox, "'FYI. A Warrant Isn't Needed': Secret Service Says You Agreed To Be Tracked With Location Data," *404 Media*, November 12, 2024, https://www.404media.co/fyi-a-warrant-isnt-needed-secret-service-says-you-agreed-to-be-tracked-with-location-data/.

[194] 18 U.S.C. § 2702. The law, however, includes broad exemptions for foreign intelligence surveillance. *See* 18 U.S.C. § 2511(2)(a)(ii), (e), (f).

[195] *See* Ayoub and Goitein, "Closing the Data Broker Loophole," *supra* note 176.

[196] In 2020, for example, Federal Communications Commission Chairman Ajit Pai proposed fines totaling $208 million after major mobile phone carriers like T-Mobile, Verizon, and Sprint were caught selling their consumers' real-time location data to data brokers without their knowledge or consent. *See* Jon Brodkin, "Senate Bill Would Ban Data Brokers from Selling Location and Health Data," *Ars Technica*, June 15, 2022, https://arstechnica.com/tech-policy/2022/06/senate-bill-would-ban-data-brokers-from-selling-location-and-health-data/.

[197] Office of the Director of National Intelligence, "ODNI Releases IC Policy Framework for Commercially Available Information," May 8, 2024, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3815-odni-releases-ic-policy-framework-for-commercially-available-information; *see also* James A. Smith, Assistant Director for Policy and Strategy, Office of the Director of National Intelligence, *Intelligence Community Policy 504 (01)*, February 6, 2025, https://www.odni.gov/files/documents/ICPM/ICPM-2024-504-01-IC-Policy-Framework-for-Commerically-Available-Information-Tech-Amendment-Feb2025.pdf [hereinafter Intelligence Community Policy 504].

[198] Intelligence Community Policy 504, *supra* note 197, at 4.

checking exercise for agencies.[199] It also fails to prohibit intelligence agencies from purchasing information that would otherwise be subject to statutory or constitutional requirements to obtain a warrant, court order, or subpoena.[200]

For foreign intelligence investigations, there's a simple way to fix the problem: amend FISA's exclusivity rule to encompass all of FISA's provisions. Specifically, Congress could provide that the provisions of FISA, insofar as they authorize the collection of Americans' information or searches of Americans' property, constitute the exclusive means by which such collection or searches may occur for foreign intelligence purposes. Without this modest step, many of the protections Congress wrote into FISA will become largely optional.

But Congress should go further and use the opportunity presented by the Section 702 sunset to close the data broker loophole completely — i.e., not just for foreign intelligence investigations. Congress should make clear that the government may not purchase Americans' personal information if compelled disclosure of that information would require a warrant, court order, or subpoena. In the last Congress, the House passed the bipartisan Fourth Amendment Is Not For Sale Act,[201] a bill that would go a long way toward closing the data broker loophole for certain sensitive types of data.[202] Congress should include that legislation—or similar reforms, such as those contained in the bipartisan Government Surveillance Reform Act[203]—as part of any Section 702 reauthorization.

D. Other Reforms

My testimony before this Committee in July 2023 describes several other concerns stemming from Section 702 and other warrantless surveillance practices, and identifies reforms that would address them. Because there have been relatively few developments in these areas since 2023, they are only briefly summarized here, with footnotes citing the relevant pages of my earlier testimony.

1. Protecting Americans' Privacy Under Section 702

Strengthen the reverse-targeting prohibition.[204] In its current form, the prohibition on reverse targeting applies only if "the purpose" of collection is to target a U.S. person. This language allows the government to target someone under Section 702 even when the *primary*

---

[199] *See* Emile Ayoub, "The Intelligence Community's Policy on Commercially Available Data Falls Short," Brennan Center for Justice, September 12, 2024, https://www.brennancenter.org/our-work/analysis-opinion/intelligence-communitys-policy-commercially-available-data-falls-short.
[200] *See id.*
[201] Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/4639; Fourth Amendment Is Not For Sale Act, S. 2576, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/2576/text.
[202] *See* Ayoub and Goitein, "Closing the Data Broker Loophole," *supra* note 176; Elizabeth Goitein, "The Government Can't Seize Your Digital Data. Except by Buying It.," Washington Post, April 26, 2021, https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.
[203] Government Surveillance Reform Act of 2023, S. 3234, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/3234/text; H.R. 6262, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/6262.
[204] *See* Goitein, *Fixing FISA, Part II*, *supra* note 127, at 27.

purpose of the collection is to spy on a U.S. person with whom the target is communicating, as long as the government has any interest whatsoever in the foreign target. Congress should close this giant loophole by prohibiting the government from targeting someone if "a significant purpose" is to target a U.S. person.

Specify minimization requirements.[205] In the absence of objective statutory criteria, there has been a predictable steady slide toward wider sharing of raw data, greater access to the data by agency personnel, and more exceptions to retention limits. Congress should specify that all information not subject to a litigation hold must be destroyed within three years unless it has been reviewed and determined to be foreign intelligence or evidence of a crime.

Narrow the scope of surveillance.[206] Section 702 authorizes surveillance of almost any non-U.S. person outside the United States, regardless of whether that person poses any threat to U.S. security or interests. The sprawling scope of permissible targets creates an enormous pool of Americans' communications that can be "incidentally" caught up in surveillance. It is also causing significant legal and economic problems for U.S. businesses, as European courts have twice blocked the transfer of data between EU and U.S. companies on the ground that U.S. companies cannot protect EU citizens' data against unjustified surveillance.[207] Congress should narrow the scope of permissible Section 702 targets in a way that preserves the government's ability to address foreign threats to the nation while reducing the impact on Americans' privacy and on U.S. businesses. It can do so by requiring the targets to be foreign powers or agents of a foreign power; by amending the definition of "foreign intelligence" information to remove overbroad catch-all language; by codifying certain limitations included in an executive order issued by President Biden; or through some combination of all three approaches.

---

[205] *Id.*

[206] *Id.* at 11–12, 28–29.

[207] *See* Case C-311/18, Data Protection Commissioner v. Schrems, ECLI:EU:C:2020:559 (July 16, 2020), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4231279; Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (October 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en. President Biden issued an executive order to pave the way for a new data-transfer agreement, which took effect in July 2023. *See* Data Privacy Framework Program, "Data Privacy Framework (DPF) Program Overview," accessed November 18, 2025, https://www.dataprivacyframework.gov/Program-Overview. The General Court of the EU recently upheld the new agreement, *see* Case T-553/23, Latombe v. Commission, ECLI:EU:T:2025:831, (September 3, 2025), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=303827&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=15593637, but its decision has been appealed to the CJEU, *see* Case C-703/25 P, Latombe v. Commission, *available at* https://curia.europa.eu/juris/liste.jsf?num=C-703/25&language=en, and observers doubt that the agreement includes sufficient constraints on surveillance to satisfy the higher court. *See* Iain Nash, "The European Commission's Rejection of Latombe," *Lawfare*, November 3, 2025, https://www.lawfaremedia.org/article/the-european-commission-s-rejection-of-latombe; Rachael Annear et al., "EU-US Data Privacy Framework Survives Its First Judicial Challenge – But More Are Expected," September 11, 2025, https://technologyquotient.freshfields.com/post/102l4m1/eu-us-data-privacy-framework-survives-its-first-judicial-challenge-but-more-are; "EU-US Data Transfers: First Reaction on 'Latombe' Case," *Noyb*, September 3, 2025, https://noyb.eu/en/eu-us-data-transfers-first-reaction-latombe-case.

2. Bolstering Judicial Review

Congress provided two mechanisms by which courts other than the FISA Court may review electronic surveillance conducted under FISA. First, Congress required the government to disclose any use of FISA-derived information in criminal prosecutions or other legal proceedings, thus enabling challenges by the non-government party. Second, Congress expressly provided for civil lawsuits to challenge unlawful surveillance under FISA. Neither mechanism is working as Congress intended, and reforms are needed to shore them up.

End the practice of parallel construction.[208] The government has a statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. But there is reason to believe that the government is avoiding its notification requirements by engaging in "parallel construction" — i.e., recreating the Section 702 evidence using less controversial means. Congress should clarify that evidence is "derived" from Section 702 surveillance if the government would not otherwise have possessed this evidence, regardless of any claim that the evidence is attenuated from the surveillance, would inevitably have been discovered, or was subsequently reobtained through other means.

Clarify application of standing and state secrets doctrines.[209] Congress expressly authorized civil suits against the government for FISA violations, and it included a provision carefully directing courts how to handle sensitive information in such cases. Yet civil lawsuits have consistently been derailed — either by stingy judicial interpretations of standing, or by courts allowing the government to evade FISA's rules for handling sensitive information through assertions of the "state secrets" privilege. Congress should remove these artificial barriers to civil litigation by (1) specifying that a person has standing to bring a civil lawsuit if they have a reasonable basis to believe their information has been (or will be) acquired, and if they have expended (or will expend) time or resources in an attempt to avoid acquisition; and (2) by clarifying that the statutory procedures for handling sensitive information in FISA cases govern how courts should resolve any claims of the state secrets privilege.

3. Closing Gaps in the Law to Prevent Warrantless Surveillance of Americans

Complete the modernization of FISA by eliminating obsolete geographical distinctions in the protection of Americans' communications. As a general matter, FISA applies when the government collects foreign intelligence inside the United States or from U.S.-based companies. When the government collects foreign intelligence abroad, it usually relies on claims of inherent presidential authority, as regulated by Executive Order ("EO") 12333 and related executive branch policies. The distinction has critical consequences, as there are exceedingly few legislative protections for Americans' privacy when the government conducts surveillance under EO 12333, and such surveillance is not subject to any judicial oversight whatsoever.

A geographic limitation on FISA's reach might have made some sense in 1978, when FISA was enacted. At the time, surveillance inside the United States generally meant

---

[208] *See* Goitein, *Fixing FISA, Part II*, supra note 127, at 31–32.
[209] *Id.* at 32–33.

surveillance of Americans and surveillance overseas generally meant surveillance of foreigners. By contrast, communications today are routinely routed and stored all over the world, in places far removed from the points of origin and receipt. Indeed, the fact that purely foreign communications were being handled by internet service providers inside the United States — which, under FISA as originally enacted, would have triggered the requirement to obtain a probable-cause order — is one of the main reasons the government sought to "modernize" FISA in 2008 through the enactment of Section 702.

But Section 702 failed to address the other half of this problem: the fact that purely domestic communications and other personal data are routinely routed and stored abroad, which can in some cases remove them from FISA's protections and expose them to EO 12333 surveillance. In particular, purely domestic communications may be obtained under EO 12333 when the government conducts bulk surveillance. Moreover, even when EO 12333 surveillance is targeted at specific foreigners, it results in the "incidental" collection of Americans' communications, just as Section 702 does. Yet protections for Americans' data obtained under EO 12333 are left entirely to executive branch policies, with no judicial review to ensure that these policies comport with the Constitution — or that agencies' practices comport with the policies.

There is no justification for giving lesser protections to Americans' constitutional rights based simply on the accident of where our digital data happens to travel. If anything, the privacy implications of EO 12333 for Americans are likely even greater than those of Section 702. The government has acknowledged that the majority of its foreign intelligence surveillance activities take place under EO 12333. Accordingly, it reasonable to expect that there is more "incidental" collection of Americans' information under EO 12333 than under Section 702, even when such surveillance is targeted. And, of course, bulk collection has the potential to sweep in Americans' data in amounts that far exceed what normally occurs during targeted surveillance.

To complete the modernization of FISA that began with Section 702, Congress should extend basic protections to Americans' communications and other Fourth Amendment-protected information, regardless of where they are obtained. Among other measures, Congress should prohibit the targeting of Americans under EO 12333; require the government to minimize the retention, sharing, and use of Americans' information that is "incidentally" acquired under EO 12333; close the EO 12333 backdoor search loophole by requiring the government to obtain a warrant or FISA Title I order before conducing U.S. person queries of the data; and require the government to inform criminal defendants when using evidence obtained or derived from EO 12333 surveillance.

Update the law to reflect the Supreme Court's decision in Carpenter v. United States.[210] For decades, the "third party doctrine" held that that people have no reasonable expectation of privacy — and therefore no Fourth Amendment protection — in any information that they voluntarily disclose to third parties. Whatever merit this doctrine might have had in the 1970s, when it was established, today it is virtually impossible to go 24 hours without disclosing highly

[210] *Id.* at 40–42.

sensitive information to the multitude of third parties (cell phone companies, internet service providers, mobile applications, etc.) that manage life in the digital world.[211]

In 2018, the Supreme Court began the long process of bringing the third-party doctrine in line with the realities of our modern era. In *Carpenter v. United States*,[212] the Court held that police officers need a warrant to compel cell phone companies to turn over historical cell-site information for a seven-day period, even though customers "share" such information with the companies. The Court reasoned that comprehensive geolocation information can reveal the most intimate details of a person's associations and activities — what the Court referred to as "the privacies of life."[213] In addition, disclosure of one's location though the use of a cell phone cannot fairly be described as "voluntary," given that the only alternative is to forego cell phone use and — along with it — participation in modern life.

Unfortunately, the holding in *Carpenter* is limited to the facts of that case. The Court expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party. But Americans' Fourth Amendment rights should not hang in the balance for years or longer while each use-case scenario wends its way through the courts. Congress should take action now, using the principles set forth in *Carpenter* to identify additional categories of highly sensitive information that merit the protection of a warrant regardless of whether they are held by third parties. At a minimum, in addition to communications content and geolocation data, those categories should include communications metadata; internet search and web browsing records; biometric information; and health information.

Conclusion

Notwithstanding the government's terminology, Section 702's impact on Americans is anything but "incidental." Intelligence agencies have leveraged this authority on a systemic basis to gain warrantless access to Americans' communications and other personal information in ways that circumvent FISA, the Constitution, and orders of the FISA Court. At the same time, gaps in the law are rendering Americans' personal information vulnerable to warrantless surveillance outside of any statutory framework and without judicial oversight. With the scheduled expiration of Section 702 next year, Congress has the opportunity — and the responsibility — to better align the law with Americans' constitutional rights and legitimate privacy expectations.

---

[211] *See generally Digital Dragnets: Examining the Government's Access to Your Personal Data, Hearing Before the H. Comm. on the Judiciary*, 117th Cong. 17–22, July 19, 2022 (testimony of Elizabeth Goitein, Senior Director, Liberty and National Security Program, Brennan Center for Justice), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-GoiteinE-20220719.pdf.
[212] Carpenter v. United States, 585 U.S. 296 (2018).
[213] *Id.* at 311 (quoting Riley v. California, 573 U.S. 373, 403 (2014) (internal quotation marks omitted)).

Chair JORDAN. Thank you, Ms. Goitein. All of you, well done. Without objection, the following documents will be included in the record: A letter from the Reform Government Surveillance about the need to reform the Foreign Intelligence Surveillance Act; a letter from a coalition of 25 organizations about the need to reform Foreign Intelligence Surveillance Act; and a statement for the record on the topic of today's hearing from the Electronic Frontier Foundation.

We will start with the gentlelady from Florida, who was part of our working group last year on this issue, the gentlelady, Ms. Lee, is recognized from Florida.

Ms. LEE. Thank you, Mr. Chair, for holding this hearing, and to our witnesses for appearing with us here this morning.

Last Congress, I was proud to sponsor the Reforming Intelligence and Securing America Act, or RISAA, which was signed into law. RISAA included sweeping reforms designed to bring meaningful changes to surveillance operations and prevent the past abuses of FISA from occurring again.

As Section 702 is now up for reauthorization, I'm committed to work with this Committee to pass a bill that equips our intelligence community with the tools that they need to protect our national security against threats, while continuing to protect the civil liberties of Americans.

There are two facts that should be evident from today's hearing.

First, serious failures occurred under prior FISA and Section 702 authorities, particularly in the FBI's queries of U.S. person data.

Second, Congress acted; reforms were imposed, and those reforms are now demonstrably working.

The Department of Justice Inspector General has now completed the statutorily required post-reform review under RISAA. That report confirms that the FBI did for years run noncompliant U.S. persons queries; that the Foreign Intelligence Surveillance Court found those practices inconsistent with both statutory law and the Constitution, and that this problem persisted well into the 2020s. Those facts are gravely serious, demanded correction, and did not resolve themselves.

The IG also found that reforms from RISAA have been implemented, including mandatory preapproval by supervisors or attorneys for U.S. person queries, mandatory DOJ audits of every one of those queries, written factual justifications, escalating discipline for negligent, reckless, intentional violations, and many others.

Most importantly, the data now shows a dramatic reduction in noncompliant queries. The IG found that widespread noncompliant querying no longer appears to be occurring, and that the remaining errors are overwhelmingly administrative/typographically as opposed to structural or abusive.

None of this means that oversight is finished. The IG explicitly noted that its postreform review covers only one year and that continued monitoring is essential.

Today, we must continue to assess what further action is needed, while recognizing the purpose of FISA, the FISC, and 702. Holding the FBI accountable does not mean stripping the FBI of targeted vital tools that are needed to protect the American people. We did not respond to the past failures by abandoning national security.

We responded by tightening the law, raising the standards, hardwiring accountability, making violations visible, and punishable. That is what we must do again.

Mr. Schaerr, as you know, RISAA now requires the FBI to obtain supervisory or legal approval before conducting a U.S. person query of Section 702-acquired information, except when there's a reasonable belief that the query could help mitigate or prevent threat to life or serious bodily harm.

Why was that additional layer of oversight important?

Mr. SCHAERR. It was a good change, and it certainly reduces the number of abusive incidences of surveillance and examining 702 data that we saw in the past. As we've all discussed, there are several other things that need to be done, but that was a very good and wise change in my view.

Ms. LEE. To what extent has the increased auditing and mandatory reporting, in your perspective, changed personnel behavior? Are there measurable improvements with this compliance? Tell us specifically what additional requirements you believe we need to impose.

Mr. SCHAERR. Well, there do appear to be improvements. However, as Ms. Goitein mentioned, because the FBI has apparently changed what it considers to be a query, it's not entirely clear the extent to which the number of queries has actually been reduced.

In terms of additional reforms, I would just reiterate the four that I mentioned in my, in my testimony:

Closing the data broker loophole entirely. Especially if the number of queries is relatively small, there's no longer any argument that it would be a huge administrative burden to get a warrant before the database is searched on Americans, right?

That's something the prosecutors do all the time. They have well-established mechanisms whereby they go to a magistrate. In this case, it would be the FISC. They send them an email. They outline why they think a warrant is warranted, and they typically get a warrant very quickly in response.

It's not a huge burden of the sort that would be suggested if you looked at the Carter Page warrant applications, for example. The Carter Page warrant applications were very extensive, but they are not typical of warrant applications in general. Typically, getting a warrant is a very simple and quick process when a prosecutor has a good reason for getting it.

Ms. LEE. Thank you. Mr. Chair, I yield back.

Chair JORDAN. The gentlelady yields back. The gentleman from Maryland is recognized.

Mr. RASKIN. Thank you, Mr. Chair. Thanks to all the witnesses for your testimony.

Ms. Goitein, let me start with you. Lord Acton famously said that: "Power corrupts; absolute power corrupts absolutely."

There was a Supreme Court decision called *Smith* v. *Maryland* 50 years ago about the pen register, where Marshall and Brennan said that unregulated government monitoring of people's private communications is most fearful for people who have nothing to hide—people who have not done anything illicit.

I wonder if you would maybe reflect for a moment on those two thoughts in the policy choice that confronts us today.

Ms. GOITEIN. Yes, absolutely. I think that's true. There is a sense, and we hear it sometimes from those who actually oppose getting a warrant requirement, that if people haven't done anything wrong, then they shouldn't have any need for the protection of a warrant. From this view, warrants protect the guilty, not the innocent. That makes no sense. Right?

Warrants are there to make sure that people who are, in fact, innocent are not subject to these searches, and that the government has to have probable cause that someone has engaged in wrongdoing to access their private communications.

There are all kinds of ways that access to private communications can be used against a person even if they show no evidence of crime. We see this in countries that don't have Fourth Amendment protections or the constitutional protections we have in this country.

One of the primary features of authoritarian regimes is that people are tracked and that their communications are monitored, and this is used to keep them in line and prevent political dissent. That is not America; that should not be America, and the Fourth Amendment is an absolutely critical safeguard against that kind of overreach.

Mr. RASKIN. I'm troubled by the government's contracts with Palantir to create software that allows the government to assemble and combine previously siloed information; in particular, departments with data purchased from data brokers. Could you explain to the Committee how purchased data can be used to compile comprehensive profiles of American citizens?

Ms. GOITEIN. Sure. The word silo sounds very negative, but, in fact, there's a good reason why data that is collected for certain purposes isn't necessarily widely shared. Often, if there's a major privacy intrusion involved in collecting the data, what justifies that privacy intrusion is the specific use to which the data is being put.

That same balance of factors doesn't apply in every situation. It doesn't make sense to distribute the data more widely, where the privacy intrusion is greater and the justification might be lesser.

You have different parts of the government that are obtaining very sensitive data, sometimes from data—often, from data brokers. This is often data that is so sensitive that it would need a warrant or a subpoena or a court order to acquire, if the government wasn't able to purchase it from a data broker.

This sensitive information may be used initially for very specific purposes. If all these pieces of data, are shared across the government and put together, it is possible, it could be possible, to build dossiers on Americans that would give a startlingly complete picture of their private lives—their associations, their habits, and their beliefs. This is information that our government in a free society should not have access to, unless there is a specific justification for a specific purpose.

Mr. RASKIN. That is what the warrant requirement is all about.

Ms. GOITEIN. Exactly.

Mr. RASKIN. Like a lot of Members of this Committee on both sides of the aisle, I'm a former prosecutor.

Perhaps, Mr. Tolman, you could address this because you were the U.S. Attorney in Utah, as I understand it. When I first heard

about this stuff, I confess that my reaction was, well, prosecutors oftentimes come into possession of information without a search warrant.

For example, the Chimel search, a search incident, an arrest will produce evidence of another crime; the Belton search with automobile stops. In some sense, that becomes the bread and butter of what a lot of prosecutors do.

I thought to myself, well, if this information just accidently and inadvertently comes into the possession of the government, then what's the big deal of letting the government use it? I wonder why, as a former prosecutor, you would say this really is a completely different matter and that's comparing apples and oranges.

Mr. TOLMAN. Yes, I appreciate the question, because I think we think of it wrong when we assess the use of the extraordinary tools to gather intelligence in this country, we are not looking at it through the criminal justice system lens; we're looking at it through national security. The mentality of national security review is that the Fourth Amendment does not apply.

Once you cross that line, you no longer are concerned about whether or not you're following certain constitutional protections, and that should scare American citizens, that we have people that will exercise that power who have crossed that line and are no longer thinking of it in terms of what they traditionally would as a prosecutor.

Mr. RASKIN. Thank you, Mr. Chair.

Chair JORDAN. You bet. The gentleman from Arizona is recognized, Mr. Biggs.

Mr. BIGGS. Thank you, Mr. Chair. It's good to see all of you again, and hopefully, we have an even better outcome this coming year than we had last time.

Let's just talk about this for a second. Is the idea that an executive agency is going to have a manager, a supervisor, review to determine whether you should actually have access to sensitive data, is that the same thing as an independent judicial body requiring you to produce probable cause to get a warrant to search for that same sensitive data? Just each one of you, is that the same thing?

Mr. SCHAERR. Not at all.

Mr. BIGGS. Yes.

Mr. SCHAERR. It may be useful, but the process the Constitution puts in place for dealing with those kinds of controversies is that the Article III branch serves as an independent check on the Executive Branch to ensure that Americans' privacy is protected. We shouldn't abandon that lightly.

Mr. BIGGS. Others, quickly.

Mr. TOLMAN. I would quickly say, where you stand on an issue depend on where you sit. I rarely had any supervisor that pushed back against any request I had to approach either the grand jury or a judge for a warrant.

Mr. BIGGS. Yes.

Mr. CZERNIAWSKI. Yes, I agree with what's been said. I think that simply having a manager in place doesn't go and have the same kind of protection as a judge.

Mr. BIGGS. Ms. Goitein?

Ms. GOITEIN. I couldn't agree more. Also, it's a different standard. Probable cause is a very different standard from reasonably likely to produce foreign intelligence.

Mr. BIGGS. Yes, it's not on a different standard; it's a different entity that the Constitution has established to protect the rights of all people, guilty and innocent. It protects everybody's rights.

When we say, OK, we are going to allow the FBI supervisor—we are going to trust the FBI supervisor, hey, have they been approved by either the voter or by the House of Representatives? No. They have been hired by somebody. They are working in the same agency, ostensibly, with the same objective, rather than the objective of protecting rights. So, that is an interesting dichotomy there.

The next thing is, when we get to this notion of the Fourth Amendment not for sale, have you seen instances where the Federal Government, State, or local government has attempted to go around constitutional protections by buying data from private entities, and then, circumventing the Fourth Amendment requirement?

Ms. Goitein?

Ms. GOITEIN. It happens constantly. The Supreme Court has held that cell phone location information, historical cell phone location information, in sufficient amounts, a week's worth of historical data, is protected by the Fourth Amendment and that the government actually needs a warrant to compel production of it.

Yet, multiple Federal agencies—the FBI, DEA, Secret Service, different components of DHS, the Department of Defense, and IRS—mostly all of them are buying access to vast databases of Americans' cell phone location information.

Mr. BIGGS. We also know that the definition of query is now under dispute, apparently. Can you expand on that, Mr. Schaerr? You have touched on it. Can you expand on that just for a second?

Mr. SCHAERR. Apparently, what the FBI did recently is they started treating a mechanism by which they sort data in the database, which, of course, requires them to look at the names and information, identifying information about specific people, but, apparently, they have some kind of a sorting process that they go through in looking at the data, and they don't count the sorting as a query. They only actually count it as query when they drill down on a specific individual. There is—

Mr. BIGGS. There is no way to determine how many actual, what used to be called queries, are taking place under the new system? We don't know?

Mr. SCHAERR. That's exactly right.

Mr. BIGGS. They have reported—the IG just reported a couple of months ago that it was 9,000.

Mr. SCHAERR. Right.

Mr. BIGGS. Nine thousand. If that is—let's just assume, arguendo, that this is the correct number. Well, then, that is a manageable number to require a judicial warrant before you conduct that query, is it not, Mr. Tolman?

Mr. TOLMAN. It absolutely is. In fact, my conversation with a former chief justice of the FISC was his greatest concern was the fact that there was so much pressure to grant everything that was presented to them, that they didn't have the ability to review it thoughtfully. Now, they do.

Mr. BIGGS. My time has expired. There is so much more I would like to ask. Mr. Chair, I have some articles I would like to include into the record, if I might.

Chair JORDAN. Sure. Sure.

Mr. BIGGS. This is *Truth* from April 10, 2024, from President Trump saying, "Kill FISA, it was illegally used against me and many others. They spied on my campaign."

This one is entitled, "Warrantless FISA Searches Are Unconstitutional, Judge Says in Landmark Ruling."

Next, "Government Surveillance Erodes Trust Between Citizens and Government."

Then, "More Than 30 Bipartisan Organizations Urge Congress Against Reauthorizing Spy Powers in Spending Bill."

Finally, one entitled, "Curbing the Power of Surveillance State: Section 702 Reform."

Chair JORDAN. Without objection.

Mr. BIGGS. Thank you, Mr. Chair.

Chair JORDAN. Yes. I would just add, before recognizing the gentlelady from California, to the gentleman's first point, not only is permission from a manager/supervisor in an agency different than probable cause, they didn't even follow the rules they had set up within the agency with the manager. They didn't even follow those rules. That is why we need the tried-and-true standard.

The gentlelady from California is recognized.

Ms. LOFGREN. Thank you, Mr. Chair.

As I listened to the witnesses, I was thinking back. It was a little more than 10 years ago that Mr. Massie and I offered an amendment, with the help of then-Congressman Justin Amash, that would have prevented all this. It did pass the House and never went into effect.

We have been over the years striving to do this. Somehow, no matter which party is in the Majority, the Intelligence Committee always manages to thwart our efforts for reform. I am hoping that this could change this year.

We certainly failed last year in fixing the core problems. We have a chance to change this. In fact, I am working to reintroduce an updated, bipartisan, bicameral Government Surveillance Reform Act, which will finally require warrants to read America's messages; ban dragnet surveillance; and stop the government from buying personal data. I'm hoping that many on this Committee will join in that effort, as we have in the past.

This is one of those issues where we do work together on a bipartisan basis, and I'm hoping that we can finally succeed this time.

The FISA Court itself has called out the FBI for repeated unlawful searches, snooping on political donors, journalists, Members of Congress, and even protestors. I think it is past time for us to fix this.

If the government wants to read an American's email or texts caught up in foreign surveillance, they should need a warrant. The FISA Court found that the FBI misused the loophole hundreds of thousands of times. The NSA can resume collecting communications that merely mention a foreign target. That is permitted by law. They can still buy private data, like location, web browsing, and messages. We are seeing, as we have mentioned, a growing

trend of Federal agencies, including defense and intelligence, contracting with companies like Palantir to compile data.

I'm hopeful that we can move forward, but I have a couple of quick questions.

Ms. Goitein, there is an expanded scope of who counts as an electronic communication service provider—you referenced that in your testimony—although the practical effects are classified. Could you briefly explain—

Ms. GOITEIN. Sure.

Ms. LOFGREN. —what kind of businesses could now be required to assist government surveillance, such as data centers, cloud storage providers, or even companies that simply manage equipment that carry communications?

Ms. GOITEIN. Sure. In the past, the way that the surveillance has worked is that the government has served directives on electronic communication service providers. We're talking about Verizon and Google, companies that actually have direct access to our communications because they facilitate our communications. That's the service that they provide. They would turn over the communications of targets.

There was a FISA Court opinion a few years ago which found that data centers for cloud computing—at least it was reported that was the type of provider at issue—did not qualify under that definition.

The Biden Administration wanted to make sure that they were included, but they didn't want to reveal that this was the type of provider at issue, because that information was and remains classified.

They deliberately solicited an overbroad amendment, one that was written in vague and very broad terms, so that no one could figure out what kind of provider it was.

What it now allows is the government can compel the assistance of any provider of any service, as long as that provider has access to equipment on which communications are routed or stored. Well, pretty much every American business and a lot of organizations provide some kind of service, and they all have access to communications equipment. That's a phone or a computer.

Ms. LOFGREN. Yes.

Ms. GOITEIN. There are some exceptions—hotels, restaurants, and libraries—but the vast majority of ordinary businesses that Americans frequent; for example, the commercial landlords of the buildings where tens of millions of Americans go to work every day, can be forced to assist the government with surveillance.

This part is really important: These businesses don't have the ability that Verizon or Google have to isolate and turn over specific communications, they may have to give NSA personnel direct access to their communications equipment and all the communications that run through that equipment, including purely domestic communications. Then, the NSA will, basically, be on the honor system to extract the communications of foreign targets.

Ms. LOFGREN. Thank you. Mr. Chair, I would just note that we also need to pass the privacy bill that Congresswoman Eshoo and I introduced a while ago, and I'm reintroducing, because we need

to get it at FISA, but we also need to get it at the source, so that people cannot sell our private data.

With that, I yield back.

Chair JORDAN. I thank the gentlelady. The gentleman from California is recognized.

Mr. ISSA. Thank you. Briefly, does anyone on this panel believe that Senator Blackburn, Senator Graham, Senator Hagerty, Senator Hawley, Senator Johnson, Senator Lummis, Senator Sullivan, Senator Tuberville, or Congressman Mike Kelly are a risk to national security or would be reasonably believed to be a risk, or should have been surveilled under a program targeting them? Seeing none, I will move on.

They are my friends. They were targeted because they were Republicans. That is unforgivable, and the FBI cannot expect anything other than a consent decree and criminal punishment if they ever do it again.

Anything less—and I will go to Mr. Tolman—if you were prosecuting a case, would you accept anything less from somebody who committed that crime, assuming you are not locking him up for years for doing it in the beginning?

Mr. TOLMAN. No, absolutely not. Our history shows, for example, in the attorney Kevin Clinesmith, that he was prosecuted for his misrepresentations of the FISC, but received no jail time. Is there meaningful deterrence? Presently, there is not.

Mr. ISSA. Well, it is true that no one is above the law, but there is a caveat: Unless you are the law. Unfortunately, the FBI and the Department of Justice are the law. Although, I trust the current inhabitants, I trusted the Bush people, and I was wrong. I trusted each of the successors, and I was wrong.

Let me just go through a couple of things to put it in perspective, maybe for the record and maybe for people who are truly laypeople.

If I wanted to find out if you were growing pot illegally in your house and I flew over with a heat sensor, and then, determined that you had hot spots, and then raided your house without a warrant, what would I be doing? Would that be OK?

Mr. TOLMAN. No, it would not be OK.

Mr. ISSA. Isn't it true that the *Kyllo* decision by the Court was right on that point? In that, if I understand correctly, what they did was they said that the reason it was unacceptable versus, let's say, just flying over in an airplane and seeing plants growing in your backyard, was because of the tools used. Correct?

Now, as we are talking about this data, is that kind of data available to Mr. Biggs or Mr. Jordan?

By definition, the first pillar of the *Kyllo* decision, which is that the tools are not readily available to the public—this massive amounts of data and the ability to gather it, they wouldn't pay $100 million if it was available any other way, right? If they could just get it themselves? They have met the first requirement.

What is any second requirement that you can see that would allow them, having met the first requirement that what they are getting is material, a tool, if you will, not available to the public—it is not ordinary eyesight; it is not just walking up and sniffing something at the door. If this tool is, by definition, special, then the use of the tools falls directly underneath this historic question of

Fourth Amendment without anything else. Does anyone see a way that they can carve their way out of this? Yes?

Ms. GOITEIN. Well, they will try to say that a lot of this information just isn't protected by the Fourth Amendment at all because we are voluntarily sharing it with—

Mr. ISSA. Aha. The Fourth Amendment—oh, you're absolutely right and I agree with you, except the Fourth Amendment, I personally—

Ms. GOITEIN. I don't think that.

Mr. ISSA. I personally—

Ms. GOITEIN. You're not in agreement with me—

Mr. ISSA. No, I agree with you that's what they will try to do.

I personally have seen this tool that can pick up heat and water damage above your ceiling. My son has one. It is fabulous. It lets you find where you have got a leaky pipe. It lets you find where there is a leak in your heating system. Every heating and air conditioning company either has one or should have one.

The fact that a special tool exists doesn't change the fact that it is a special tool, does it?

By the way, heat coming out of your house was never considered to be protected until the Court said the tool and the source of the tool is what determines that; it is not an ordinary eyesight.

I'm going to close, Mr. Chair, by saying: Shame on the Court for not already having taken a case up and done this. If they won't do it, this Committee must do it in reauthorization.

I yield back.

Chair JORDAN. The gentleman yields back. The gentleman from Tennessee is recognized.

Mr. COHEN. Thank you, Mr. Chair.

Ms. Goitein, we have been doing this—Ms. Goitein, we have been doing this for a long time on different issues. Let me ask you a question. The problem, is it the law or is it the enforcement of the law?

Ms. GOITEIN. It's both. Those two things are related. One of the things that I've wondered, when I look at these massive compliance failures over the years, I don't think all those compliance failures were intentional; I don't think all of them were negligent.

They have built a system that is so massive and so complex, and the rules are just so sort of arcane and intricate, that it might actually be impossible to completely enforce the rules as they would need to be enforced to protect Americans' privacy.

The one major advantage to the warrant requirement is that it's so much simpler. You've reduced the need for all these massive layers of oversight, for different rules, for different tools you might use, for different queries, figuring out, is this a query; is this not a query?

It's very, very simple. If the government wants to access an American's communications, they submit a warrant application. They go to the court, or a Title I application. It simplifies the process, and that will itself, even leaving aside the fact that you now have an independent branch of government performing this review, will make compliance achievable.

Mr. COHEN. With AI, are we going to have more and more problems because there will be more and more data?

Ms. GOITEIN. Absolutely. With AI, we're going to have to really reexamine how a U.S. person query is even defined. Because if AI is used in a way that can select you as person communications without actually using what we think of as U.S. person identifiers, then we are sort of right back where we were before with really no limits on governmental access to U.S. person communications. Yes, that is an issue we will have to—

Mr. COHEN. Has the FISA Court been fairly consistent in how they have dealt with these issues?

Ms. GOITEIN. What I would say is that the FISA Court has been remarkably tolerant of just this long history of abuses. We focus on the FBI's querying abuses in recent years. This program has been plagued with violations and noncompliance since its exception—since inception.

I'm not just talking about the FBI. I'm talking about the NSA, in particular; the CIA. The NSA was violating its query restrictions systemically for almost a decade after the program was put in place. Yet, every year, the FISA Court has reauthorized this program. A couple of times, they've waited a few months for new layers of oversight to be put in place.

To me, it's an example of: Fool me once, shame on you; fool me twice, shame on me. Because it's been a 17-year pattern of violations, extensive, and systemic violations. Yet, the FISA Court points out the violations; is upset about them; says they're unacceptable, and reauthorizes the program.

Mr. COHEN. Let me go to another issue, I guess. Mr. Issa asked you about those seven or eight, nine Senators and Reps, whether anybody thought that they should be subject to any reviews. As I understand it, the idea was not because they were Republicans; it was because they had—Mr. Smith had reason to believe that—a court agreed in issuing a warrant—that they had possible connections with the Trump White House and the overthrow of our government.

Would that not give any of you all beliefs that they should have been queried, looked at their records or their phone calls? Ms. Goitein?

Ms. GOITEIN. Oh, I'm so sorry, I thought you were asking—just repeat that?

Mr. COHEN. Yes, the idea that Jack Smith got a warrant,—

Ms. GOITEIN. Yes.

Mr. COHEN. —apparently, because he thought that these people might have some contact with the President and the Committee to overthrow the government whatever it was.

Ms. GOITEIN. Right. Right. What we're dealing with here is the fact that subpoenas for communications records are extremely easy to obtain. You actually don't have to show that the person in question is themselves involved in any sort of criminal activity. The standard is one of relevance. That's a very low standard.

When we're talking about communications metadata, which is incredibly revealing information—this is the information that the NSA was collecting in bulk—

Mr. COHEN. All right. Let me just go because my time is about to run out.

Ms. GOITEIN. I'm sorry.

Mr. COHEN. It's a million-dollar question.

Ms. GOITEIN. Yes?

Mr. COHEN. Do you think those nine people, because they had their metadata looked at, should get half-million to a million dollars, simply by going to Federal court, like no other—

Ms. GOITEIN. Well, if we're going to do that, then that should be open to everybody who's had their metadata acquired, based on this very, very low standard. That will be a little tricky.

Mr. COHEN. Thank you. I yield back, Mr. Chair.

Chair JORDAN. The gentleman yields back. Mr. Tolman, are we all in the database? Every single person? Every single American?

Mr. TOLMAN. Yes.

Chair JORDAN. Yes, this database is huge, right? They are getting information on foreigners, but we are all getting swept up in this. This is one giant—I call it the giant haystack of information. You got 10,000 people at the FBI who can just—I am going to search on Mr. Tolman, on Ms. Goitein. I am going to search on whoever I darn well—and they have demonstrated that they can't police themselves. Whatever the agency is, whatever rules they have, they can't police themselves. This is why Congress has to do it. Why not use the tried-and-true rule? That to me is how big this is.

I want to go down through a couple things here that have been raised. First, to the gentleman from Tennessee's questions on getting toll records. I do have a concern with this, because some of this was done for a long period of time. Mr. Smith went and got the toll records subpoenaed from the carriers, the toll records of the Speaker of the House of Representatives. Frankly, he waited until Mr. McCarthy became Speaker of the House to get his toll records from three years prior. The real concern I have with that is they did it for a two-month time span.

To Ms. Goitein's statement, you can pattern someone's life. You can figure out all kinds of things. Because they knew who Mr. McCarthy called, who called him, when the call took place, how long it lasted. If Kevin initiated the call, they knew where he was at when he did so. Well, shazam. You can figure all kinds of things out. That is the concern when they do this. We need to—frankly, that is why this Committee passed the nondisclosure—the gag order.

That is the other thing: They get that information and then they go to the judge, tell the carrier, and tell AT&T that they can't tell the customer that the government just got their phone logs for two months, can pattern their life, and know all that stuff I just talked about. That is a concern.

We have passed legislation out of this Committee; we hope to pass it to the House here soon, which puts limits and restrictions on that. Not just for the Members of Congress, of course, but again to everyone.

Think that is a good piece of legislation we passed, Mr. Tolman? I will come to you.

Mr. TOLMAN. It's essential.

Chair JORDAN. Yes, it is essential. Everyone agree with that?

Mr. SCHAERR. Yes.

Chair JORDAN. Yes. We got the NDO issue. Mr. Raskin and I were talking about these areas of concern with privacy. We have the third-party data, purchasing data, this—what we call the Fourth Amendment is not for sale, because if you can buy stuff that would otherwise require a warrant, and shouldn't be able to do that. We got to do some work on that issue. Then there is the fundamental question we are asking for FISA 702. Go get a warrant before you get the ability to search people's—and then there is this compilation of data.

I am just interested in any thoughts you have on—we are trying to strategize, the Ranking Member and I, and the Committee, how much do we try to put in 702? Do we do a separate legislation? We are trying to figure that out, too. I am just curious, any thoughts that you would have. Maybe we will just go down the line. Let's start with the Democrat—or Ms. Goitein and then we will move across.

Ms. GOITEIN. Yes, you really can't address Section 702 in isolation, because Section 702 is part of a vast ecosystem of often-overlapping surveillance authorities. If you cutoff one avenue of surveillance, the government might be able to turn to another, or to exploit gaps in this network of laws to conduct surveillance without any statutory authorization.

Chair JORDAN. You think we should try it all together?

Ms. GOITEIN. Well, it's not that. Frankly, there's a lot you could address. We're not really talking about everything here. The four reforms that have been specified here today are—

Chair JORDAN. Yes.

Ms. GOITEIN. —certainly, a good place to start, right? That is a warrant for—or a Title I order for back door searches. That's closing the data broker loophole. Fixing the electronic communications service provider definition and shoring up the role of amici in the FISA Court.

Chair JORDAN. Thank you.

Mr. CZERNIAWSKI. I agree with Ms. Goitein that, at least for the purposes of FISA, that we want to focus on those four key reforms because I think that those are the most promising things that we can get addressed. Then, for the other kinds of things that you're highlighting there are other vehicles that we can go and explore in terms of pushing forward.

Mr. SCHAERR. I would not limit yourselves to FISA reforms written narrowly.

Chair JORDAN. Yes.

Mr. SCHAERR. As you all are much more aware than we are, there are only limited windows when legislation can actually get passed by both chambers and signed by the President. Those don't come along all that often, and it's important to take advantage of them when they do.

Chair JORDAN. Thank you.

Mr. TOLMAN. I would just last say, why aren't they capable of self-governing in this area? We have to remember post-9/11 we shifted the FBI and the Department of Justice's overarching mandate to intelligence gathering for national security purposes. Once you do that their mentality is not to self-govern.

Chair JORDAN. Twelve billion dollars we give to the FBI. That is their budget. Over half of it is used on the surveillance stuff versus—you go to talk to the average American, they would say like what? I thought the FBI was supposed to be going after traditional bad guys, not spying on Americans. You are exactly right. That is a problem.

One last thing. I know I am a little overtime. I will give a little more time to the next Democrat witness.

Someone said let it expire. I forgot which of you said that in your opening. Mr. Tolman. The guy who helped put it together. Well, give me your thoughts on that.

Mr. TOLMAN. Well, without wisdom—and in my youth I bought everything that was argued by the Department of Justice as to why they needed it.

Chair JORDAN. Yes.

Mr. TOLMAN. Then, you see their incapability of actually governing themselves with such power. It would be like 215. We let that expire and here we are still stopping national security threats.

Chair JORDAN. Yes.

Mr. TOLMAN. We didn't think that it was possible when 215 expired.

Chair JORDAN. Yes. Yes. OK. All right. The gentleman from Georgia is recognized.

Mr. JOHNSON. Thank you, Mr. Chair. I don't view this Committee meeting as the most serious effort when it comes to FISA reform because if it was, we would have someone from the intelligence community sitting on this panel to give that viewpoint.

Now, it is clear that this Committee also is not interested in protecting the security, the personal, private security, and the data of American citizens. That is because it was complicit when this President set up DOGE, the Department of Government Efficiency, put it in the hands of Elon Musk, and then unleashed Elon Musk to collect the private data of citizens through capturing the data of the Social Security Administration, the Treasury Department, the Office of Personnel Management, Health and Human Services, the VA, the Consumer Financial Protection Bureau, the Department of Commerce, the Department of Education, the Department of Energy, the Department of Labor, the Department of Transportation, and others, collecting this data.

The goal was to create a single centralized government database. This effort was unprecedented and unauthorized by Congress. While it was happening this Committee, as it does today, stood silent and complicit and let it happen, and is not concerned about it. I am concerned about that data.

I am wondering, Ms. Goitein, if you are as it relates to Section 702?

Ms. GOITEIN. I'm very concerned about what you're talking about. In fact, I was speaking about it earlier when we were talking about sort of removing the quote, "silos." That the access to data, private sensitive data of Americans that is collected by the government on occasion for legitimate reasons, and then may sometimes for less legitimate reasons when the government is simply buying up massive databases—making that data widely available to anyone in government is a major privacy and civil liberties issue.

Mr. JOHNSON. Yes. This Committee has not been interested in that.

Let me ask a question: The Fourth Amendment, which requires probable cause to conduct a search, also has exceptions to it such as stop and frisk, evidence in plain view, search incident to a lawful arrest, and exigent circumstances. Am I right? That is for people on the street though, regular people.

People in the suites—before I say that I will note that on February 20th of this year, Trump issued an Executive Order forbidding the Federal Government, the DOJ, the SEC, and others from applying or investigating the Foreign Corrupt Practices Act. You all know that this is true. They are not enforcing that.

At this point international crime perpetrated by American citizens, Trump in the lead with the acceptance of a $400 million jet—he just the other day accepted a Peace Prize from FIFA. Then, the next day they announced that an indictment of FIFA is withdrawn and is being dismissed; Corruption. Pay-to-play is what is happening under this administration.

Let me ask this question: Why shouldn't there be an exception to the warrant requirement in a situation where an FBI agent has a reasonable suspicion that a U.S. person should be queried because that FBI agent has evidence that the U.S. is engaged in an international conspiracy to commit a mass murder of Americans, and that FBI agent wants to query the 702 database? Why shouldn't there be an exception to the warrant requirement that allows that FBI agent to do that?

By the way, I should say that the FBI under Kash Patel and the DOJ under Pam Bondi—I don't have any confidence that they would apply the law justly, that they would act in a legal fashion. I am afraid of what they will do. It implicates how I am going to vote this time when it comes to this reauthorize of FISA.

If someone could answer that question. Why shouldn't there be an exception to the warrant requirement?

Ms. GOITEIN. Well, certainly, if there was an immediate threat and a risk of life or safety there would be an exception. That's for exigent circumstances. If not, if there's time for the FBI to use its usual investigative techniques, the ones that are less intrusive that don't infringe on a reasonable expectation of privacy under the Fourth Amendment. They would have time. You said they had evidence. Maybe they have enough evidence already to get a warrant. If not, they have other investigative techniques at their disposal that are less intrusive, which is simply saying—

Mr. JOHNSON. Well, they are surely going to have a whole bunch more material to work with also after this DOGE situation has unfolded. I will yield back.

Chair JORDAN. The gentleman yields back. I would just point out that we had those exceptions in the language. In fact, I would think many of us thought we almost had too broad of exception language in there for imminent threat, for cybersecurity, a situation if the person gave permission. We had that in the language. We were as generous as you could possibly be, I thought.

Mr. JOHNSON. Well, I will tell you, I am going to be looking at it through a different set of eyes now that this Trump Administration is in place.

Chair JORDAN. Fair enough. Fair enough. Long as you are a yes vote, we don't care how you get there.

[Laughter.]

Mr. JOHNSON. Well, let's not stand up here and act like Democrats are the need through Biden is the need—

Chair JORDAN. I have not done that. I have not done that.

Mr. JOHNSON. —Carter Page and all of that. Let's not stand up here and act like that is the reason why we need to reform.

Chair JORDAN. I have done that. I would just remind the gentleman you can—

Mr. JOHNSON. That is all that we have up here among these witnesses—

Chair JORDAN. I think you are the one who has been partisan, not me.

Mr. JOHNSON. —among the three Republican witnesses are Carter Page aficionados.

Chair JORDAN. The time of the gentleman has expired, and we will recognize the gentleman from California for five minutes.

Mr. MCCLINTOCK. Well, thank you, Mr. Chair. First, I am not sure the data provided by an individual to the government in say an application or a tax return shouldn't be reviewed by the government. That is very different than the government searching for and seizing data that is held by an individual. That is the distinction my friend from Georgia misses. Other than those—

Mr. JOHNSON. I am not missing anything, sir.

Mr. MCCLINTOCK. Other than those remarks I am very heartened by the fact that there is a broad bipartisan concern on this issue reflected by all the panelists and almost all of the Members.

As you know, the history of this goes back to 1761, the trial of James Otis, challenging the writs of assistance, the general warrants of the Crown. There was a 25-year-old attorney in the audience in that trial who was named John Adams. Many years later he reflected on the trial and said this:

> Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance. Then and there the child Independence was born.

In Adams' view that was the birth of the American Revolution, was the abuse of searches by the Crown. Of course, it was also the birth of the Fourth Amendment.

FISA is abused under Democratic and Republican administrations, because it is human nature to acquire power and once acquired to use it. That is why we divide the powers of government and that is the reason we have a Fourth Amendment that divides the power of searches between the Executive and the Judicial Branches.

The Fourth Amendment to me is very clear: If you want to look through my stuff, you have got to convince a judge that there is evidence I have committed a crime and list the stuff you want to search for. We are told that doesn't include metadata like phone records. It seems to me that metadata is a record of my electronic activities.

Isn't it, Mr. Schaerr?

Mr. SCHAERR. It certainly is.

Mr. MCCLINTOCK. Why would that not be equally protected under the Fourth Amendment? What am I missing?

Mr. SCHAERR. Well, it is protected under the Fourth Amendment. The reason for excluding metadata searches in the last version of the reform bill was just that searching mere metadata is less intrusive, less dangerous than searching the communications themselves. They both are protected by the Fourth Amendment.

Mr. MCCLINTOCK. They are records of my communications, even if it is not a verbatim transcript of them. Then is that not used to get a warrant to review a transcript?

Mr. SCHAERR. Yes, it could be used to get a warrant.

Mr. MCCLINTOCK. Basically, a general warrant could be used. What is an effective general warrant could be used to get a specific warrant, correct?

Mr. SCHAERR. You could view it that way.

Mr. MCCLINTOCK. There is no protection left if we are going to go down that road, it seems to me. One ultimately has to lead to the other.

Mr. SCHAERR. Yes, I guess I would still say that communication itself is more sensitive and more—should be subject to higher protection. You're right, there is a bit of a slippery slope there. As the Chair said, "the last version was quite generous."

Mr. MCCLINTOCK. You dealt with the FISA Court quite a bit. I have been concerned about the secret and centralized nature of that special court. I remember looking at statistics from like 10 years ago and there were like 34,000 warrants that had been requested by the government at that point. Only 11 had been rejected by the FISA Court.

Mr. SCHAERR. Right.

Mr. MCCLINTOCK. Of course, the approval of warrants of individuals like Carter Page were backed by false statements. Not only were those claims not seriously questioned to begin with, as they should have been, but when it came to light that the FBI had lied in its applications, I am aware of very few disciplinary actions taken by the FISA Court. There was one prosecution that ended with a slap on the wrist. What are they to make of this?

Mr. SCHAERR. Well, I think you've just made the case once again for adopting a robust amicus process in the FISC. Obviously, the individuals who were subject to—who were being investigated can't be told that they're being investigated. There's a need to have an independent privacy expert, somebody with a security clearance who can be present in especially sensitive FISA investigations.

Mr. MCCLINTOCK. Before the FISC we dispersed that responsibility across the entire court system, did we not? To get a warrant you had to go to a District Court judge.

Mr. SCHAERR. That's typically true. In the FISA Title I context though of course you go to the FISA Court.

Mr. MCCLINTOCK. Right, but my question is why don't we go back to the dispersed system where you at least have some decentralization of this awesome power?

Mr. SCHAERR. Well, there's an argument for that. What would be more important is to be sure that in those decentralized proceedings, if they don't actually give notice to the person who's the subject of the investigation, that the amicus process should be in-

cluded there as well. It may be more efficient to centralize it in FISC though.

Chair JORDAN. The gentlelady from Washington is recognized.

Ms. JAYAPAL. Thank you, Mr. Chair. Thank you for holding this hearing. Thank you to the group of us on both sides of the aisle that have been very consistent on this and have taken on our own party in power. It does seem like it gets very difficult. People change their views based on who is in power. I appreciate the work we have done on a bipartisan basis to really protect the privacy of Americans and make sure that we are upholding our constitutional obligations.

I want to go back to this question of queries, Ms. Goitein, because you talked about it quite a bit in your opening statement. These preliminary numbers are not really—we just have no idea what they really show. I want to talk a little bit more about why we need to approach that current number that's been given to us with caution. Also, because this is a clear example of how the FBI just changed the rules and they are not complying—how do we make sure that whatever we write into law—it appears now we have to define query. What ideas do you have for when we approach this again that we are actually ensuring compliance with our intent?

Ms. GOITEIN. Well, Congress did define query. I have racked my brain to try to figure out why somebody at the FBI decided that these were not queries. This was a system that allowed FBI agents to retrieve communications associated with a particular case file or facility, which is basically the communications of a particular target.

Ms. JAYAPAL. Yes.

Ms. GOITEIN. It also allowed them to search for, particular, participants and pull up those participants' communications. Those could include U.S. persons. It was basically a way to run queries on a subset of Section 702 data. The query could be for a U.S. person's communications within that pool.

It's hard for me to understand why they didn't consider this to be a query. One possibility is that there was a drop-down menu involved and the definition includes the use of one or more terms to retrieve the unminimized content. Maybe if you're clicking on a U.S. person's account rather than typing it in maybe that's not being counted as a query. I don't know this for sure. I'm just trying to understand.

Ms. JAYAPAL. Yes.

Ms. GOITEIN. One of the things that also puzzles me is that apparently the National Security Division just happened to find out about this in August 2024, and the practice wasn't suspended until early 2025. Why did it take that long to look at the definition, look at what was happening?

Ms. JAYAPAL. Well, that is right. It seems to me, Mr. Chair, that we might be able to do some sort of our own inquiry into this right away and at least get the correct numbers and make sure that we are operating with full data.

I want to ask you, Ms. Goitein, also about the question of 702 does not allow for the targeting of U.S. persons, and yet millions of Americans have been targeted for surveillance under the statute.

Why is it important to protect everyone in the United States from warrantless surveillance? Does include American citizens and all persons in the United States?

Ms. GOITEIN. Yes, first, as a constitutional matter, the Fourth Amendment protects everybody in this country. If you believe that a warrant requirement is a constitutional requirement, as a District Court held a year ago, as a unanimous panel of the Second Circuit seems to indicate in their earlier decision, then it applies to everyone in this country. There are practical reasons as well.

Just as collection of the communications of non-U.S. persons incidentally pulls in U.S. person communications, queries, any query an incidentally retrieve the communications of Americans. That's because even if you're querying a non-U.S. person inside this country and pulling up the communications they have with a non-U.S. person target, those communications can have other people involved in them. It can be a group email or a group text that includes any number of U.S. persons. If the non-U.S. person being queried is in this country, that vastly increases the chances that they're going to be in frequent communication with Americans in this country. These are queries that pose particular risks to Americans.

Ms. JAYAPAL. We have been hit with lots of opposition arguments, and so I want to give you one and ask you to refute it. Some people view the apparent decrease in back door with some alarm and asked whether the FBI is not making queries that it should be making. How would enacting a warrant requirement both protect Fourth Amendment rights while providing a clear process for the FBI to do its work? This was just something raised all the time to us.

Ms. GOITEIN. Yes. Well, if it is in fact the case that FBI agents are not performing legitimate queries because there's too many layers of oversight or they're worried that they will be penalized if somebody later decides that they shouldn't have made the query, there's really a simple answer to that.

Needless to say, the answer is not to get rid of the oversight and go back to all the queries of Congress persons and protestors and all that. The answer is to have the government get a warrant to put the burden on gatekeeping these searches where it belongs, which is with the courts. That would reduce the need for all these layers of internal oversight and whatever sort of administrative paperwork and burden is associated with those layers. It would also remove any motive that might exist for FBI agents to be excessively cautious.

FBI agents would be free to do their job, to vigorously pursue investigations within the law and their professional obligations. Then, the courts could do their job.

Ms. JAYAPAL. Their job.

Ms. GOITEIN. The job that they do and pretty much every context except 702.

Ms. JAYAPAL. Yes.

Ms. GOITEIN. Which determines whether there is a lawful basis for the search.

Ms. JAYAPAL. Thank you, Mr. Chair. I hope we can work together on actually getting compliance with the real numbers around the queries. Thank you. Yield back.

Chair JORDAN. The tried-and-true method, going to a separate and equal branch of government, getting a probable cause warrant with imminent threat exceptions, is the answer. Doesn't take a genius to figure this stuff out.

The gentleman from Wisconsin is recognized.

Mr. TIFFANY. First, Merry Christmas to all of you. Remember, St. Nicholas is watching and we are hoping that—he does not need a warrant, but we are hoping we can get the Federal Government to make sure they get a warrant.

Mr. Czerniawski, last time you were here we discussed the concern with RISAA and the definitional expansion of electronic communication service provider. Is that concern still there? If it is, how are we going to fix it?

Mr. CZERNIAWSKI. Yes, that concern is still very much there, unfortunately. As Ms. Goitein pointed out, it radically and drastically expanded the definition of what would be captured underneath an electronic service—communication service provider. Because that threat is still there, that there's an opportunity with this upcoming reauthorization discussion to go and reign that back in.

Now, to their credit, in the Senate, Senator Mark Warner did try to go and get some fixes to that definition, but it was stripped out of the Intelligence Authorization Act process. That problem is still there, and I hope that with this upcoming debate that we can get the fix that's so desperately needed.

Mr. TIFFANY. Is there anyone, in particular, that you would point to that you would say we got to have this in terms of a fix?

Mr. CZERNIAWSKI. Yes. Again, the most fundamental one is getting a warrant, closing that back door search loophole is really, really integral.

This electronic communication service provider jumps right up there with it, because again it is just way too expansive. It goes and conscripts a whole host of businesses into the surveillance apparatus that had no intention of ever being in there, so much so that it was a rare instance where you even saw technology go—industries go and speak out against this particular definition of language. ITI had submitted a letter to Congress going and asking to go and fix that definitional issue. Yes, very important.

Mr. TIFFANY. Mr. Tolman, how can we limit this data broker loophole without hurting intelligence?

Mr. TOLMAN. The fact that it's so secret and it's contained exclusively within those that present to the FISC, those powers—and we're really talking about internal powers of the FBI—without being able to shed light on what they're doing and who they're contracting with—it's very difficult to stop its use. It will continue to be a challenge unless we are putting, for example, third parties capable of reviewing what they're searching for and who they're contracting with. If we prevent and put guard rails on the scope of contracting, we might be able to make an impact on its abuse.

Mr. TIFFANY. Mr. Schaerr, we have seen some political judges across the country really abusing their authority. Are there guard rails against this with FISA?

Mr. SCHAERR. Well, the warrant requirement itself is going to help bring some accountability to the agencies. There's always a chance that a judge will grant a warrant that he or she shouldn't grant and there's always a chance that a judge will deny a warrant that he or she shouldn't grant, but at least in the judiciary there's an opportunity for appeal.

Mr. TIFFANY. You see what Judge Boasberg has done. He has served on the FISC. It is really of concern that he is going to abuse that authority.

Mr. SCHAERR. Well, no solution is perfect, but the mechanism that the framers of the Constitution put in place to deal with these issues is as perfect and as good a system as we've seen. There will be lapses, there will be mistakes, but there will be many fewer than we currently see.

Mr. TIFFANY. It was talked about earlier, but amicus briefs are allowed, correct, in the FISC?

Mr. SCHAERR. I suppose they are technically allowed, but since the FISC operates in secret nobody knows what the FISC is considering. Nobody really—unless they're told, nobody knows whether there's an opportunity to submit an amicus brief. Part of the amicus system is that the FISC itself would appoint an amicus and tell them we have this proceeding dealing with this particular target. Can you give us your thoughts on it?

Mr. TIFFANY. I am going to take it that there is some limited ability. Should it be expanded?

Mr. SCHAERR. The amicus program I believe should be expanded. There are a lot of politically sensitive investigations that currently are not subject to the amicus provisions at all. There are several politically sensitive investigations where FISC should be effectively required to appoint an amicus to give it independent advice when it's considering a Title I warrant.

Mr. TIFFANY. Once again, with the amicus, if that is allowed, what will that engender that will be helpful in this process in your mind?

Mr. SCHAERR. Well, two things: First, the amicus may actually find real problems with the government's case and be able to prevent an investigation or prevent surveillance that should not have gone forward. At a minimum the presence of an amicus is going to have a big deterrent effect on the FBI and the DOJ.

In the Carter Page situation, for example, I am convinced that if there had been an amicus in the room and in the proceeding that Clinesmith would never have lied and that the other misdeeds that occurred in connection with Carter Page would likely not have occurred because they would have been afraid that the amicus would recognize them and point them out to the court.

Mr. TOLMAN. May I respond to that question Mr. Chairman?

Mr. TIFFANY. Sure. One of the things that it would prevent is what happens currently, which is where there's a deficiency in a warrant, Title I warrant, the FISC judge will actually go back to DOJ and ask them to fix or provide additional information on a deficient warrant. An amicus system would prevent that.

Mr. TIFFANY. Thank you for letting me exceed by time, Mr. Chair.

Chair JORDAN. You bet. The gentlelady from Pennsylvania is recognized.

Ms. SCANLON. Thank you. I want to thank the Chair for calling this hearing. FISA reform is a key area of bipartisan agreement in this Committee, one where our shared interests in limited government, protecting civil rights, and liberties overlap substantially. The abuse of FISA by the FBI and the intelligence community is pretty well-documented. Our witnesses have detailed some of those abuses and made some really good suggestions for reform to address that abuse.

One cause of the abuse of surveillance authority happens because there are few enforceable limits to collection of data and the use of that data. As long as we have to rely on the good faith of the FBI, or the intelligence committee—community regardless of who is in charge, surveillance can be ripe for abuse. When we don't put clear enforceable limits in law, like a warrant requirement, it means that Americans' most essential rights and liberties are at risk, including the right to speak their minds, to be free from unreasonable search and seizure, and even their essential privacy rights.

The importance of protecting Americans' essential rights and privacies has never been more clear than in the past year when we have seen the current administration with respect to its allies at DOGE and the Department of Justice mobilize the government to invade and collect Americans' private data, whether Social Security, tax, student loans, healthcare, voter registration, or SNAP data. When you add that to the growing purchase of online and social media data by the government, we see that data being used in illegal law enforcement activities, and even prosecutions of this administration's political enemies.

One example is where we have seen the White House weaponize government surveillance in law enforcement to target political opposition and stifle political speech with the National Security Presidential Memorandum 7, or NSPM–7, which directs the intelligence community and law enforcement to target organizations and individuals on the basis of their political beliefs or political speech, actions that are unambiguously protected by the First Amendment.

On the basis of that memo, we have seen Attorney General Bondi direct the FBI to compile a list of groups allegedly engaged in domestic terrorism, using examples of protected political speech as key criteria for inclusion on the list. If you strip away the pretext, then the purpose of these actions becomes clear. This administration is already using the Federal Government to target political opponents.

Given the known abuses of FISA by governments, past and presence, and the willingness of this administration to run roughshod over existing guard rails, it seems pretty clear that we have got to act to limit those abuses, or else we are going to see FISA being used illegally to spy on Americans who don't align with this administration's agenda.

Ms. Goitein, in your testimony you raise the very good point, that Americans should expect and be able to trust that Congress will protect their privacy and their freedoms. When Congress last considered FISA reauthorization last year we were told repeatedly by

the intelligence community that our Fourth Amendment concerns were best addressed by better stewardship of FISA authorities by the government.

Do you think that has played out in practice given the known abuse of surveillance authorities that we have seen and the failure to collect and report accurate data about the use of those authorities?

Ms. GOITEIN. Yes, one important point to bring up is that the failure to count these queries as queries and to follow the procedures required for U.S. person queries, like getting attorney approval or providing a written justification—those are themselves violations of the law that Congress passed last year.

While we don't know whether there were violations of the substantive standard for queries or how many violations there were, we know at least that there was a fairly systemic violation of several requirements of the law that have happened so far.

In terms of whether the particular queries met the standards, I'll point out that the government credits some of these procedural requirements: attorney approval, written justification, audits, for improved compliance. Those were not happening with these particular queries.

Ms. SCANLON. Yes.

Ms. GOITEIN. It would be reasonable to expect that you would see a higher rate of noncompliance with these queries. I don't know if we'll ever know that for sure.

No, I don't think the record has borne out this notion that internal oversight was the best way to go about protecting the Fourth Amendment. You can tell that by looking at the Fourth Amendment, which does not talk about internal oversight. It does not say if the government has a reasonable basis to believe that its search will yield important information, it can either go to a court and get a warrant or just do the search. Right? That's not what the Fourth Amendment says. That's not the way to protect Fourth Amendment rights.

Ms. SCANLON. Sure. The Constitution famously said you have to get approval from a different branch of government to avoid the kind of self-dealing or pay-no-attention-to-that-query-behind-the-curtain-kind of an approach to this.

Can you just address again how the warrant requirement protects people from potential targeting on the basis of their political beliefs?

Chair JORDAN. Quickly.

Ms. SCANLON. I am sorry. I did not realize my time has expired.

Chair JORDAN. The gentlelady yields back and we will recognize the gentleman from Kentucky.

Mr. MASSIE. Thank you, Mr. Chair. Thanks for having the hearing on this.

I have been working on this for over a decade with my colleague Ms. Zoe Lofgren. I was ecstatic a decade ago when we got an amendment passed to require a warrant, but somehow that got stripped out. It is like Lucy and the football in Charlie Brown. We get so close or we think we have won and then it gets pulled away.

I will talk a little bit about the elephant in the room. One of our colleagues here who used to be for FISA reform is now the Speaker

of the House and cast the deciding vote against FISA reform last Congress. We don't want to talk about that too much, but I am going to bring it up, because when he was asked why he changed his position, he said he learned some stuff in a SCIF. Well, the SCIF is like the magic room where they go to change your mind.

The problem with his story is—I spent three hours in the SCIF with him, and when we pressed the CIA Director, and the Director of National Intelligence, and the Head of the FBI—all of them were in the SCIF—give us one example where you couldn't have solved the crime or you couldn't have prevented some mass casualty event because of a warrant requirement. They could not give us a single example.

The only person in that room who had a decent argument about anything was a FISA judge who said you are going to need more SCIFs somewhere if we are going to review these—if you are—we are going to have to review warrants. It became a cost issue, but I thought that was kind of lame. It is going to cost some money to follow the Constitution. OK. What is it going to cost?

One of the things that Zoe Lofgren reminded me of is there is all these sorts of loopholes where we are afraid if we do get our FISA reform the intelligence agencies are going to use these loopholes to spy on Americans. The one I want to ask you all about today—well, there are actually three of them. One of them is Executive Order 12333. I see Ms. Goitein shaking her head, so I will ask her.

Should we be concerned about E.O. 12333 and what could we do about that Executive Order to hem it in?

Ms. GOITEIN. Yes, absolutely. Yes. Let me explain a little bit. As a general matter FISA applies when the government is collecting information inside the United States or from U.S. companies. If the government is collecting information overseas it usually is relying on a claim of inherent authority as governed by Executive Order 12333 and various other executive policies. This is a critical distinction because there are almost no legislative protections or guard rails for Executive Order 12333, and there is no judicial oversight.

Now, this distinction between collecting here and collecting there might have made sense in 1978 because, collection inside the U.S. usually meant collecting on Americans and collecting overseas usually meant collecting on foreigners overseas. As we all know, with the changes in technology that has completely changed. Communications, other sensitive information is routed and stored all over the world. In fact, that foreigners' communications were being stored by U.S. service providers in this country and therefore—the government would have needed to get a warrant for those before 702 is one of the reasons the government pushed to modernize FISA with 702.

They just didn't address the other half of the problem, which is that Americans' communications are routed and stored overseas in ways that can in some circumstances remove them from the protections of FISA. For example, when the government collects information in bulk overseas and it's inevitably pulling in Americans' communications.

Americans' communications are acquired incidentally. They are acquired as part of bulk collection under E.O. 12333. The only safe-

guards in place are those that the Executive Branch has chosen to put in place. It will not shock you that those rules and procedures are much more lax.

Mr. MASSIE. This isn't the answer I wanted. I wanted you to tell me we shouldn't be concerned about Executive Order 12333.

Ms. GOITEIN. You did? Sorry. You called on the wrong witness.

Mr. MASSIE. Another loophole that we have identified in the Weaponization Committee was the Financial Privacy Act of 1978, which is one of those bills that did the opposite of what it was supposed—what the name of it was. It created a loophole that allows the government to get bank records without any warrants or anything. Is anybody familiar with this?

Mr. TOLMAN. Yes, I am.

I would say there is the concern, overarching concern I have is you have 1978, you have 1981 on E.O. 12333. We didn't have the ability to collect the data that we do today, nor the access to it. It was a very different government that we were talking about back then when those Executive Orders came out.

Mr. MASSIE. That may mean updated as well, you think?

Mr. TOLMAN. Absolutely it does.

Mr. MASSIE. Because we have, we identified where they have been using it recently. A lot of this stuff actually comes through whistleblowers.

Just in closing, I am disappointed that our Committee didn't find the Arctic Frost spying on the Senators. It wasn't—we are responsible for oversight. We couldn't even find them spying on us. It was a whistleblower.

We need to tighten up our oversight over these Committees. That, well, we did find that they were spying on the Speaker of the House and the Members of this—well, at least one Member that we know of.

Just one more thing before I close. I know we got some—I would prefer to fix the law for everybody, not for the Members of Congress.

Mr. TOLMAN. I totally agree.

Mr. MASSIE. One of our colleagues was very vocal about making sure it was fixed for the Members of Congress. The fix was to report the spying to the Speaker of the House and maybe a couple Chairs of the Committees. Why not report it to the person they were spying on, the Member of Congress? That is my concern.

I yield back.

Chair JORDAN. That is why we did the nondisclosure order NDO Fairness Act that we passed out of this Committee to help in that regard. The gentleman from Colorado is recognized.

Mr. NEGUSE. Thank you, Mr. Chair. I see my colleague Mr. Massie. I don't know if you wanted to finish that thought, Mr. Massie? I would be happy to yield a moment.

Mr. MASSIE. He gave me an extra minute, so I am good.

Mr. NEGUSE. All right. Well, thank you, Chair, for holding this hearing. Certainly, thank you to all the witnesses.

I share the concerns with my colleagues on both sides of the aisle with respect to FISA visas in the past and the necessity for reforms.

Mr. Schaerr, I want to ask you a couple of questions, sir. You testified today about your representation of Mr. Carter Page, former campaign advisor, in his ongoing lawsuit against the United States based on the 2019 finding by the Department of Justice that the FBI had used invalid warrants to monitor Mr. Page under Section 702.

Mr. SCHAERR. Right.

Mr. NEGUSE. In 2020, five years ago, the Special Counsel at Department of Justice Tom Durham secured a guilty plea from an FBI attorney who doctored an email that was used in that warrant application. Is that a fair characterization of the events so far?

Mr. SCHAERR. He actually went to trial. You are talking about Kevin Clinesmith?

Mr. NEGUSE. Correct.

Mr. SCHAERR. Yes.

Mr. NEGUSE. Went to trial. Got it and ultimately was convicted?

Mr. SCHAERR. He was convicted but didn't get any jail time.

Mr. NEGUSE. Correct. My understanding is that to address, at least in part, some of the 702 abuses Attorney General Bill Barr, in 2020, directed the creation of an Office of Internal Auditing. You are familiar with that?

Mr. SCHAERR. Yes.

Mr. NEGUSE. All right. That Office of Internal Auditing which was created by former President—or not former, President Trump's former Attorney General in the first term was assigned to scrutinize the 702 process, to prevent these kinds of abuses from happening in the future?

Mr. SCHAERR. It was designed to scrutinize Title I processes. The other provision of of FISA.

Mr. NEGUSE. Correct. Right.

Mr. SCHAERR. Yes.

Mr. NEGUSE. I assume you agree that this is a worthy goal?

Mr. SCHAERR. Certainly, a worthy goal and one that would be advanced even further by adopting the amicus mechanisms that we have discussed here and that passed the Senate with 77 votes a couple years ago.

Mr. NEGUSE. Sure. Also, assume you are aware that the Office of Internal Auditing no longer exists?

Mr. SCHAERR. I wasn't aware of that.

Mr. NEGUSE. Yes. The Director of the FBI Kash Patel earlier this year eliminated the Office of Internal Auditing at the FBI. This was an office that the Republican Attorney General Bill Barr created five years ago in response to the work done by Chair Jordan, and the Republicans and Democrats on this Committee.

It doesn't seem like that accomplishes a whole lot. I have yet to understand the rationale as to why the FBI Director who, by the way, at least prior to his appointment as FBI Director, had expressed all kinds of misgivings about 702, FISA, and the like, has now decided to eliminate the Office of Internal Auditing at the FBI. I wonder why that is? I don't know if you care to perhaps make an educated guess.

Mr. SCHAERR. Well, that is all the more reason why Congress needs to act.

Mr. NEGUSE. Sure.

Mr. SCHAERR. Congress, as the representative of the people, needs to be the entity that is protecting the rights of Americans.

Mr. NEGUSE. Yes. I don't disagree with you.

Mr. SCHAERR. Yes.

Mr. NEGUSE. Clearly, there is an impetus for Congress to do something. That is the, obviously, the rationale for this particular hearing.

It would be nice to perhaps hear from our Chair and my colleagues on the other side of the aisle, who I know have direct relationships with the Attorney General of the United States and the Director of the FBI, it would be nice to hear them defend the Office of Internal Auditing that I presume they supported in here five years ago. Doesn't really make much sense to me why that would be eliminated.

I see, I am getting near the end of my time. As I said, that there is a bipartisan consensus in the Congress that is emerging this is an area ripe for reform. Again, it is something I am supportive of. I look forward to working with my colleagues on both sides of the aisle to try to make some progress in that regard.

I will yield back the balance of my time.

Chair JORDAN. The gentleman yields back. The gentleman from Texas is recognized.

Mr. ROY. I thank the Chair. I thank the witnesses; appreciate you all for being here.

Let me just ask this question among the four of you. I know the answer. I will start with Mr. Tolman and I will move across the panel. Is there any legitimate reason why we should not have the warrant protection included in a reform to FISA? Mr. Tolman?

Mr. TOLMAN. No. In fact, the reasons stated are illegitimate. You take the argument that the FBI can do it themselves, that is, I have never believed in the fox being able to—

Mr. ROY. Right?

Mr. TOLMAN. —analyze and control what the fox does in the henhouse.

Mr. ROY. Sure.

Mr. SCHAERR. Absolutely. There is no reason not to, not to include it. It should be included.

Mr. CZERNIAWSKI. That is a "must have" thing if we are going to go and reauthorize FISA.

Mr. ROY. Ms. Goitein?

Ms. GOITEIN. No reason not to.

Mr. ROY. OK. With all due respect to one of our colleagues on the other side of the aisle who was expressing some concerns about not having somebody from the intel community here, the intel community are the ones running the show, including by the way, with all due respect, a lot of our colleagues on the Intel Committee here who are a part of the show.

Judiciary exists to focus on the Constitution and the rights of citizens to not have this occur. That is why the Chair is absolutely correct to have this witness panel.

I would just note that all four witnesses, including the Democrat witness, just said there is no legitimate basis for us not to include a warrant protection requirement in FISA reform.

I want that to ring through the halls of Congress between now and April so that when we are faced with the vote that is inevitably going to occur on this issue, that we not have what happened almost tow years ago where we left the American people without the protection the Constitution affords them from a tool that is being used on a bipartisan basis to target the American people and collect their data, which is offensive and it is wrong. There cannot be this cloak of secrecy surrounding intel.

To that point, I wonder if, Ms. Goitein, you might be able to help me out here a little bit. I offered a couple of amendments to FISA last time, and one of which was to demand that we get all the reports of the queries. In that amendment we settled on quarterly. I wanted it to be monthly or whatever, but regular reporting.

We gave them a year at their wailing and gnashing of teeth. They wouldn't be able to get this done and figured it out within a year, OK? That year expired last, I will call spring.

Well, do you know and are you aware have we gotten any kind of data and reporting information out of the System 1 efforts that we can look at the data specifically with respect to these queries? Can you illuminate us?

Ms. GOITEIN. I actually don't know the answer to that question in terms of what you have received from the FBI. It looks like Congresswoman Ross may?

Oh, OK. Yes, I am not sure. If you are not, if you are not getting the data that you are supposed to be getting under the law, needless to say, that is a very serious problem.

Mr. ROY. Well, what we are advised of is that we are—is that the System 1 is not even really recording these queries and set up in a way—

Ms. GOITEIN. Oh, I am sorry. Yes, I am sorry. The System 1, exactly, that data, so what happened was that in it was March 2025, the National Security Division told the FISA Court that it was currently cooperating or coordinating with the FBI to determine whether any records of this functionality had been generated.

Absolutely, this Committee should be following up on that to determine whether any such records were located. If not, whether they can be forensically reconstructed. That is information you should have.

Mr. ROY. Then, I have a limited amount of time, I just want to stipulate for this Committee that we need to see that data. We need to see the results of the queries. We need to be able to identify that information. I want to see more changes in FISA to force more information and compile our ability to see it.

I would note, also, that we included provisions there for the Chair and Ranking Member of Judiciary, as well as leadership, to be able to go into FISC proceedings. That has been allowed pursuant to the law, however, the FBI has then stipulated at times that individuals would have to be removed, and that they would need to leave for certain sensitive conversations.

Which, by the way, the statute never contemplated, and what we passed did not contemplate, that Members of Congress who have full clearance, that in the statute they are supposed to be able to go in there in these FISC proceedings and monitor them.

The FBI has no basis, whether that was the FBI under the Biden Administration or the FBI under the Trump Administration, to then say it is too sensitive, the Members of Congress need to leave these proceedings.

Whatever we do in both carrying out our oversight function of the Executive Branch, or whatever we do in FISA reauthorization—unless we let it expire from Mr. Tolman's I think wise advice—then we need to make sure that if we are putting the Members of Congress in there to oversee this stuff, the FBI doesn't walk in and say, sorry, you have seen enough, you can't see the rest of this.

That is just facially absurd. I yield back to the Chair.

Chair JORDAN. The gentleman yields back. The gentlelady from North Carolina is recognized.

Ms. ROSS. Thank you, Mr. Chair and the Ranking Member, for holding this really important hearing. I am so glad that we continue to have bipartisan support, particularly for the warrant requirement. Thank you very much for the amicus requirement, which is something that I have worked on in the past.

As we are weighing this reauthorization of FISA, and until we can get some of these safeguards that we want, it is very important that we use the previously created internal safety checks and guardrails. I am concerned that this Administration has weakened that.

Maybe this response to Mr. Roy's initial point, but there was a requirement that the Office of Inspector General review the querying practices. They did file a report this past October which found that the FBI has made progress in reducing the number of noncompliant hearings.

Not enough. We agree. The Inspector General was not able to conclude, based on their limited time, that the querying compliance are entire—the problems are entirely in the past.

This really shows that we need to continue to have this oversight with the tools that we have until we can get stronger protections for the American public.

Ms. Goitein, the Privacy and Civil Liberties Oversight Board serves an important oversight role, especially regarding FISA. The board has published numerous reports and recommendations about the different surveillance programs. Released a report in September 2023 about Section 702 that contained multiple recommendations to protect the rights of Americans.

In January, almost immediately after he was sworn in as President, Trump fired the Democratic board members. The board now has one part-time member and lacks a quorum to begin new investigations or issue reports signed by the board.

Could you tell us why ensuring the independence of this board is so important and why it is important for it to have a quorum?

Ms. GOITEIN. The Privacy and Civil Liberties Oversight Board is the only independent agency within the government that is charged with ensuring the protection of Americans' civil liberties. It is a small board with a fairly small staff and a huge and absolutely vital remit.

If you don't have the Privacy and Civil Liberties Oversight Board doing its job, then all the oversight that is coming from the Execu-

tive Branch will effectively be internal oversight. That is sort of happening within these agencies.

PCLOB, as we call it, has been vital in bringing to light, first, how the Section 702 program worked. If it weren't for the PCLOB's 2014 report, most of what we are saying today about how 702 works we wouldn't be able to say. The PCLOB managed to get that information declassified and put it out to the American people.

Because of the PCLOB's work we found out in 2023 that the claim that warrantless backdoor searches were important for national security, a claim we heard from the Government, was not true. That the Government had only been able to identify a handful of instances where these U.S. person queries had been useful. In pretty much every case they could have either gotten a warrant, consent, or invoke the exigent circumstances exception.

It is because of the PCLOB that you had the tools that you needed last year to enact this, and that you will have the tools that you need now in reauthorizing Section 702 this year.

Now, if people on the PCLOB can simply be removed at will, that will chill. First, there is no quorum, right, so there are no people right now, essentially. That is a problem.

Unless Congress—it is not enough to just appoint people to PCLOB. The independence of PCLOB must be protected because if Members know that they can be removed if the President doesn't like the investigations that they are conducting or the results that they came up with, then that is going to chill their oversight. We need them to be a robust oversight body.

There was a provision in the PCLOB authorizing statute saying they could be removed at will. Congress removed that. It seems clear that they can't be removed at will. In fact, there are lawsuits right now challenging their removal. Congress should make that explicit. Congress should make very clear that Members of PCLOB can only be removed for cause.

Ms. ROSS. Well, it is my great hope that at least in this area we use our power and we have a check on the Administration. With that, I yield back.

Chair JORDAN. The gentlelady yields back. The gentleman from Virginia is recognized.

Mr. CLINE. I thank the Chair. I thank the Committee for all their work on this important issue.

The Constitution is under the jurisdiction of this Committee. The Fourth Amendment is pretty clear:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

No asterisk, no footnote that says "but except for this case or in cases of national security or otherwise."

Let me just ask Ms. Goitein, under 702 the Government is prohibited from engaging in reverse targeting. Can you describe what reverse targeting is and why it is problematic?

Ms. GOITEIN. Reverse targeting is when the Government claims to be interested in a foreigner overseas but, in fact, the reason is collecting those communications is because they are interested in

the communications of an American who may be communicating with a foreign partner.

Mr. CLINE. What penalties, if any, does Section 702 levy against Government actors that engage in reverse targeting or otherwise abuse the RISAA framework?

Ms. GOITEIN. Well, right now there are internal accountability procedures that have been adopted by the FBI. I don't think that they are public. They were required by RISAA. I don't think that they have been made public and there is no public information. I am not aware of anyone having been disciplined for it.

Mr. CLINE. Do you have an estimate of the volume of Americans' communications that has been collected as part of Section 702 surveillance?

Ms. GOITEIN. The Government has refused to provide that estimate. Members of Congress have been asking for it since 2011.

Mr. CLINE. Has the FBI ever estimated the volume, to your knowledge?

Ms. GOITEIN. Not to my knowledge. I am not sure that they are particularly interested in that number.

Mr. CLINE. Now, as you have discussed, according to the ODNI report, queries by FBI were up to 2.9 million in 2021, 2.9 million, declining to 119,000 in 2022, 57,000 in 2023. Between April 2024–April 2025 down to 9,000.

Can you estimate as to why there was such a large number of queries in 2021 and why that number has come down dramatically in recent years?

Ms. GOITEIN. Yes. What we have been told by the FBI is that there were a lot of batch queries or perhaps even just one particularly large batch query. That is when a bunch of, a large number of individuals were queried at the same time under the same rationale, relating to a potential cybersecurity threat.

That, it is still hard to quite figure out the math and how they got to 2.9 million with that. The argument for why the queries have come down is because there has been an effort to put more oversight in place. That there has been a lot more attention.

Mr. CLINE. More sunlight.

Ms. GOITEIN. Exactly.

Mr. CLINE. More, more eyes on.

Ms. GOITEIN. There has been a lot more attention paid. Certainly, the reauthorization was coming up and, so, we saw a decrease. I just want to remind you that this last number, 9,000, that is the number of known and counted queries. We don't know the actual total number.

Mr. CLINE. All right. Let me go to Mr. Schaerr and talk about RISAA. When we passed RISAA what would you say were the most important reforms that RISAA implemented?

Mr. SCHAERR. Certainly, one of the most important was the provision allowing the Chairs of relevant Committees in this body and in the Senate to be present in FISC proceedings, and to be able to understand what is happening in that body.

I don't know how you provide oversight to an institution like that unless you can at least attend its proceedings once in a while.

Mr. CLINE. We are all cleared.

Mr. SCHAERR. Right.

Mr. CLINE. Would it be problematic to say "or the designee of the Chair on the Committee"?

Mr. SCHAERR. That would be a wonderful addition.

Mr. CLINE. Help us spread the burden, wouldn't you say?

Mr. SCHAERR. Yes.

Mr. CLINE. All right.

Mr. SCHAERR. The accountability.

Mr. CLINE. It is a small room, but there are many of us on this Committee who would be willing to go down there and spend some time there.

Mr. SCHAERR. Yes.

Mr. CLINE. Let me just say, a reporting requirement of RISAA, DOJ OIG would release the report which found that the reforms implemented have "significantly reduced the number of noncompliant queries identified."

Now, what further reforms? To reduce this number of noncompliant queries down to zero is a warrant requirement necessary?

Mr. SCHAERR. I think so. Even with a warrant there will still be some mistakes made by the courts. The number is going to go down very substantially if you have an independent judge looking at these requests.

Mr. CLINE. Thank you. I yield back.

Chair JORDAN. The gentleman yields back. I believe the law says we can designate a staff person to go, yes. We should try to work on making sure it could be a Member. Mr. Cline would be great because he sits on this Committee and also the Intel Committee. That would be ideal. If I could really quick, before I recognize the gentlelady from Vermont.

What do we think the number is? If it is not 9,000 and we think they have got this other route that they are taking, what do we think the number is? Anyone hazard a guess?

Mr. TOLMAN. The number is very close to what it has been historically. They eliminated the girlfriend searches and things like that. I believe it is a product of identification.

Chair JORDAN. Still way high.

Mr. TOLMAN. It's way, way up there. They have changed the way that they—

Chair JORDAN. Because the impression that was given is it was two hundred and some thousand, or a hundred, I get that it is some hundreds of thousands. Now they are pounding their chests, like, oh, we got it down to 9,000. Nine thousand is still a concern, but we think it is much higher. Is that fair to say?

Mr. TOLMAN. Probably.

Mr. CZERNIAWSKI. Yes.

Chair JORDAN. Is Mr. Tolman right that it is probably where it was?

Mr. CZERNIAWSKI. Yes.

Ms. GOITEIN. I would hesitate to say simply because if it turns out that this is not the case, it doesn't change my opinion in terms of whether or not we should have a warrant.

Chair JORDAN. I don't think it says any number.

Ms. GOITEIN. I don't want to set some bar that if they go below it, suddenly everything is OK.

I do want to mention that this system, System 1, or the advanced filter function, that is one instance we know where the FBI basically decided that something wasn't a query and that it was instead a filter.

Chair JORDAN. Yes.

Ms. GOITEIN. An important question for you all to ask is whether there are other such ways that they are obtaining U.S. person information—

Chairman JORDAN. Yes. I know it is.

Ms. GOITEIN. —that they consider to be a filter, or a sorting rather than a query. Because if that were true, the number could be even higher.

Chair JORDAN. I apologize—

Mr. TOLMAN. Mr. Chair, when the FBI was being criticized that violent crime was on the rise, they changed the way they collected violent crime data.

Chair JORDAN. Good point. Very good point. Good point. I am sorry. I recognize the gentlelady from Vermont.

Ms. BALINT. Thank you, Mr. Chair. Thank you to all the witnesses for your time. Ms. Goitein, thank you so much for being here. I want to break this down in simple terms of the millions and millions of Americans who have never heard of FISA, who, who have no idea when we talk about the Foreign Intelligence Surveillance Act what we are talking about.

If you will indulge me, I would like to walk through it piece by piece. When we talk about communications data we are talking about texts, we are talking about emails, phone numbers, DMs, that kind of thing; is that right?

Ms. GOITEIN. Sort of any, it is actually any information that can be acquired under Section 702, any foreign intelligence information of any kind. It could include other types of data.

The focus tends to be on communications because communications are some of the most private sort of information that we have in exchange.

Ms. BALINT. Section 702 allows the Government to take huge sets of data from companies like Verizon, or T-Mobile as part of its stated mission of trying to track down terrorists and other security threats.

Ms. GOITEIN. No, that is actually there are sort of two separate issues there.

One is sort of this data broker loophole by which the Government buys data under no statutory authority whatsoever. Right? That is not under FISA, it is not under Section 702, it is just they do it because they think they can, because they decided they can. We are trying to change, right?

Ms. BALINT. That is important. That is a really important distinction.

Ms. GOITEIN. Yes. Yes, 702 there is a target. They are collecting information concerning that target. They are collecting the target's communications data on the target.

The issue, of course, is the foreign target doesn't have to be suspected of any wrongdoing. All of that foreign target's communications with Americans, would be swept up as well.

That data may also include Americans' personal, private information, right? There is a large amount, and the PCLOB used that word. We don't have an estimate. Government refuses to give us one. There is a large amount of Americans' personal data, information, and communications.

Ms. BALINT. I know this is something that the Vermonters care deeply about who is protecting their personal private information. I am sure that is true for many of us on this Committee.

OK, now here is the rub, right, essentially there is this huge secret database containing all kinds of information on Americans, and non-Americans as you said. The Government says it can search that database without a warrant. That is what they are claiming. Is that right?

Ms. GOITEIN. Yes.

Ms. BALINT. Let's say my emails were caught up in one of these data sets, landed in the database. Could the FBI search the database for Becca Balint and access those emails without a warrant?

Ms. GOITEIN. Yes.

Ms. BALINT. This is what we have been referring to today as kind of a backdoor search; is that, is that correct?

Ms. GOITEIN. Yes.

Ms. BALINT. Has Section 702 ever been used to spy on a Member of Congress? In other words, has the Government used a backdoor search to find data on elected officials?

Ms. GOITEIN. The Government has run backdoor searches on the Members of Congress. We don't know whether any data was returned or whether they used that data. They have attempted to find and use data of the Members of Congress.

Ms. BALINT. Obviously, deeply concerning these backdoor searches, deeply concerning.

Who is vulnerable? Are regular people vulnerable? This is the thing that I want Americans outside of this Committee, outside of Congress to understand. Is anyone vulnerable to this?

Ms. GOITEIN. If you communicate with foreigners overseas, you are vulnerable.

Ms. BALINT. If you communicate with foreigners overseas, you are vulnerable to this backdoor search?

Ms. GOITEIN. Yes.

The Government has to have a foreign intelligence purpose for the Section 702 program. Foreign intelligence is defined so broadly—

Ms. BALINT. Yes.

Ms. GOITEIN. —that it can include information that simply relates to the U.S. conduct of foreign affairs.

Ms. BALINT. Essentially, any person with an email account or a cell phone could potentially be a target of Government surveillance by our Government, and there is no requirement that the Government get an actual warrant to spy on our personal communications. Is that what we are trying to get at here?

Ms. GOITEIN. Yes. The Government would say that you are not a target because the target was a foreigner overseas. Of course, if they are then looking for and using your information, that kind of feels like targeting to me. It becomes a bit of a semantic sleight of hand.

Ms. BALINT. I agree. What would happen if we just let Section 702 expire?

Ms. GOITEIN. I would be concerned about that for a couple of reasons.

Ms. BALINT. OK.

Ms. GOITEIN. I would be concerned, first, that the Government would try, go ahead and obtain the same information in other ways that actually come with less oversight. Whether it is buying up data from data brokers, whether it is other forms of surveillance under Executive Order 12333. There are even fewer protections for Americans' privacy and civil liberties in those contexts than under Section 702.

Also, I would point out that the Government actually has made a case that Section 702 is valuable for national security insofar as it permits the collection of foreigners' communications. The foreigners' communications that have been obtained have been shown to have national security value.

What the Government hasn't shown is evidence that warrantless searches for Americans' communications have had any significant national security value.

Ms. BALINT. I appreciate it. I see that my time has expired. I just want to say, one of the things that I try to do on this Committee is try to break it down for people outside of these halls, these powerful halls of Congress, to explain why it is that we do the work that we do.

Again, I appreciate all your time. I yield back.

Chair JORDAN. The gentlelady yields back.

You did break it down. Everyone is in there. They can't police themselves. Much so that they actually searched the Members of Congress, individuals in the body responsible for setting their budget. If that is not a problem, I don't know what it is.

The gentleman from Alabama is recognized.

Mr. MOORE. Thank you, Mr. Chair. Mr. Schaerr, what is the purpose of Woods Procedures?

Mr. SCHAERR. As I understand it, the Woods Procedures are an internal mechanism in the Justice Department and the FBI to try to be sure that there is adequate vetting before a warrant application is filed in the FISA Court.

Mr. MOORE. Do you think the Woods Procedures should be codified, given that the FBI is going to follow their own procedures?

Mr. SCHAERR. I am not sure codifying would be that useful. Much more useful would be to adopt a kind of amicus participation position mechanism that we have discussed earlier.

Mr. MOORE. What other kind of procedure is in place to protect against malign use of the FISA? What? What would you recommend? You mentioned the amicus. Are there other procedures in place that should be protecting American citizens?

Mr. SCHAERR. With respect to the Title, Title 1 process, the amicus provision that we have discussed is the most useful.

If we look at FISA more broadly and include Section 702, then the other three reforms that we have discussed here today would be, would be extremely important. A general warrant requirement before, before the FBI can search the communications of Americans, for one thing.

Tightening up the Electronic Communications Service Provider definition that was, unfortunately, broadened in the last version of the reauthorization, tightening that up so that it excludes, really that it excludes any entities other than data centers, which apparently is what the FBI was trying to ensure that they could get at there.

There is just no reason to basically dragoon churches and small businesses into conducting surveillance on behalf of the NSA and the FBI.

Then, closing the data broker loophole so that if the Government wants to buy data from data brokers that contains lots of personal data about individuals, before they can search that data they have to get a warrant to do that, just like we are proposing that they have to get a warrant to search the 702 database.

Mr. MOORE. I am going to change gears on you for a minute, Mr. Schaerr, you represented Carter Page in his lawsuits against the FBI, correct?

Mr. SCHAERR. Correct.

Mr. MOORE. During Crossfire Hurricane investigation Mr. Page actually reached out to the FBI and offered to be intermediary; is that correct?

Mr. SCHAERR. Offered to help them, yes.

Mr. MOORE. Yes.

Mr. SCHAERR. Yes.

Mr. MOORE. Why did he reach out to the FBI, I guess would be the first question.

Mr. SCHAERR. Well, he was already helping the CIA with concerns that they had about things going on in Russia. When he learned that there was an FBI interest, he felt like maybe I can be helpful to the FBI as well.

Mr. MOORE. Why do you think they turned down the opportunity to interview Mr. Page?

Mr. SCHAERR. Well, the independent investigation of that showed that the FBI was, or elements of the Justice Department were trying to investigate the incoming administration. They were trying to create the appearance of a tie between the incoming administration and Russia.

Carter Page was the one staffer who had some well-established contacts in Russia. They chose to focus on him.

Mr. MOORE. Was that part of the reason they went after General Flynn, too, do you think, the whole Russian collusion narrative was part of that? Or was that a separate investigation on its own?

Mr. SCHAERR. It was closely related.

Mr. MOORE. OK, thank you. Mr. Holman, I mean Mr. Tolman, I am going to hit really quick with you. What type of information does law enforcement agencies, what are they purchasing from data brokers and what are they using it for?

Mr. TOLMAN. Well, as you know, there is so much data that is collected from outside the government that there is really no limit to what they can purchase that can be obtained through online use, emails, other data points, and financial institutions.

There really, if you think about it could be in worst form, the ability to collect everything that they can't collect under a warrant, without a warrant.

Mr. MOORE. Very dangerous I would assume.

Mr. TOLMAN. Correct.

Mr. MOORE. For personal privacy and, certainly, for our amendments to protect those privacies.

In 2023, the FBI admitted to buying precise geolocation data grabbed from mobile phone advertising. What should Congress do about this?

Mr. TOLMAN. I became aware of individuals, for example, that travel to Washington, DC, were not traveling on January 6th to the rally, were not entering the Capitol, they simply were traveling. All their location was obtained. No warrant.

Congress has to recognize that any thought that internal regulation is going to control the use of power by the FBI is going to fail.

Mr. MOORE. Does that get back to the fox guarding the henhouse referred to earlier?

Mr. TOLMAN. That is correct.

Mr. MOORE. Thank you. Mr. Chair, I am running out of time, so I will yield back. Thank you. Thank you.

Chair JORDAN. Yes, not only their location, but they also got their bank records, and they got what they bought. They overlaid that if they banked at the Bank of America. They overlaid that with if they ever purchased a firearm.

So, well, well said. The gentleman from Illinois is recognized.

Mr. GARCIA. Thank you, Chair Jordan. This hearing—Oh wait. Give me just one second.

Chair JORDAN. Sure.

Mr. GARCIA. I apologize. You guys have been going for 2½ hours. If any of you need a break, make sure, we will give you a break and we will keep going. I just thought of that because I just took a break.

Chair JORDAN. The gentleman is recognized. You get your full time.

Mr. GARCIA. Thank you, Chair Jordan. This hearing, of course, marks the start of negotiations over the reauthorization of FISA Section 702. At a time when our civil liberties are under assault, and the public lacks trust in government, the stakes could not be higher.

As my colleagues and witnesses have pointed out, Section 702 has been repeatedly abused under both Republican and Democratic administrations. It has become a tool of mass domestic surveillance, and an end run around Fourth Amendment as well.

It should be clear by now that we cannot trust the Executive Branch to regulate itself. This is a crucial amendment for Congress to assert itself and its constitutional authority to protect our constituents from warrantless spying.

It is clear to me, and it is not clear to me that Section 702 can ever be reformed to the point where it doesn't threaten our constitutional rights. If Congress is going to reauthorize it, then we must insist on major changes.

That means requiring a warrant for U.S. person searches; closing the data broker loophole; reforming the FISA Court; narrowing the ECSP definition; and requiring more transparency and oversight.

It also means getting rid of the immigrant vetting provision that was included in RISAA. This overbroad law requires Section 702

querying procedures to "enable the vetting of all non-U.S. citizen persons who are being processed for travel to the United States."

This is a major separation—expansion, rather, of government surveillance powers. Instead of targeted surveillance aimed at specific national security risks, the intelligence agencies will now surveil over 10 million people, non-U.S. citizens entering the country without suspicion.

This will also affect the privacy of Americans whose communications will be accessed at much higher rates, and subject to further abuse by agencies that have shown complete disregard for our civil liberties.

It is not just progressive Democrats who oppose this provision. Chair Jordan opposed it and spoke against it on the House floor, highlighting that it would "authorize the surveillance of a whole new category of individuals." Ultimately, 80 Republicans voted against it.

Ms. Goitein, thank you for being here today. Can you speak to the potential harms of the immigrant vetting provision and the significance of the bipartisan opposition to it?

Ms. GOITEIN. Sure. Ordinarily, to conduct a query the rules of the agencies require them to reasonably believe that the query will yield foreign intelligence. That is a very low bar, given how broad the definition of foreign intelligence is.

Yet, despite how low the bar is, unfortunately, a provision that was adopted last year in RISAA and, as you mentioned, the Chair opposed it, most people in this room opposed it, but it was still adopted. That allows in some ways, it basically requires agencies to have procedures in place that permit suspicionless queries for people who are seeking to travel to the United States, whether it is as a tourist, or whether it is on a work visa, a student visa, or whatever the case may be.

Even if none of the many vetting mechanisms that the government already uses has turned out to be any reason to worry about these individuals. This is completely unnecessary. People should be able to travel to this country, to study and work in this country without turning over their personal communications to be read by the government.

There are plenty of vetting mechanisms in place to ensure that they don't pose a threat to national security. There is an impact on Americans' privacy and on U.S. persons' privacy as well, partly because these are totally suspicionless searches.

To the extent that these queries return communications that include Americans as participants, these are very likely to be completely innocuous conversations with no foreign intelligence in them. That is an intrusion on these Americans' privacy.

Also, as we have already seen, there have been significant compliance problems with this travel vetting provision. Including multiple queries of U.S. persons under this authority.

Mr. GARCIA. Thank you so much. You are underscoring that this is not a partisan issue. Of course, I look forward to working with Chair Jordan and the other Members in other parties to ensure that this provision is not included in the reauthorization of Section 702.

I thank you. I yield back, Mr. Chair.

Chair JORDAN. The gentleman yields back. The gentleman from New Jersey is recognized.

Mr. VAN DREW. Thank you, Chair. Hey, it is good to see because especially in a Committee where we debate a lot, we argue a lot, we have different viewpoints on, quite frankly, just about everything, that we are on, by and large, all of us on the same page with this. It is heartening and it is good.

The FISA, the misuse of FISA was truly, I believe, one of the low points of our republic. What happened, invading people's personal lives, if there is anything—and you all know this, you are smart—historically that this country, what this republic was supposed to stand for was that individual freedom and individual rights, and not to have the government, because of political reasons, social reasons, or religious, for any reason, invade our privacy, invade our family, and invade our lives.

We had hearings, as you all know. We were all here. Most of us were here at the time. Really dug deep. I want to thank the Chair as well, he never gives up. We are going to get this done.

We had hearings and there was some disagreement. Not so much within this, among us, but more the disagreement was with other Committees and other individuals in Congress.

So, here is my question. This is what I want to get down to. Good legislation, was an improvement, was a compromise, that is all wonderful. We want to still do better.

If you could, and we will start with Mr. Tolman, just go down the line relatively briefly, what has worked well? Where have we done a good job?

By the way, if you think we haven't done a good job anywhere, you can say that. Nobody is going to get mad. Where are we vulnerable? Where do we still have problems? Where do you worry at night that we are going to use our precious freedom? Mr. Tolman?

Mr. TOLMAN. The first thing that comes to mind that you did well is that you won the public debate on this issue. It used to be very siloed, limited voices that were shouting this is a concern, and it is going to violate citizens' rights, and they are going to abuse it. It was not believed. The public was not aware.

This body, and I give this House the credit, not the Senate, I give this body, this Chair, and others that turned the tide in the public debate on this and the awareness. That, to me, is the battle.

I would say the thing that keeps me up at night is this: I would like our FBI to get back to finding bank robbers and less intelligence gathering. Until that happens, we will always need robust guidelines to reign them in.

Mr. SCHAERR. Thank you for the question.

We have discussed earlier four specific reforms that all of us agree with that need to be made. One of those is fixing something that happened with RISAA, which is the overexpansion of the definition of electronic service provider, which was expanded so much that it now includes many small businesses, and even churches and other institutions. That needs to be pared back and limited to its original purpose, which is to allow the FBI to reach data centers.

That is one important reform. We also talked about closing the backdoor search loophole in FISA that allow the government to

search Americans' information, and some of their most private information without a warrant.

We have also talked about closing the so-called data broker loophole which allows Government agencies to essentially buy their way around the Fourth Amendment just by buying data from data brokers.

Then, there's a real need still. There were some useful reforms made in RISAA to the oversight of the Foreign Intelligence Surveillance Court. There is an additional important reform that we believe needs to be made, which is to expand the amicus program within that court so that independent privacy experts are brought in sensitive cases to advise the court and act as kind of a counterweight to the FBI and the DOJ who, when they try to seek warrants, have somebody else in the room who has a responsibility for protecting Americans' privacy generally, to ensure that the FISA Court does that.

Mr. VAN DREW. Thank you. I only between the two of you have 17 seconds. If you can really just.

Mr. CZERNIAWSKI. Sure. I will be really brief.

Second, everything that has been said. That this is critical to continue the conversation because, as I mentioned in my opening statement, this is a crisis in faith in the government, in a key agency and agencies that are responsible for protecting us. That is why if we get these reforms done that can go a long way toward fixing that problem.

Ms. GOITEIN. There were some helpful reforms in RISAA. The main problem is it just didn't go far enough. It didn't go far enough because there wasn't a warrant requirement.

There are a couple places where RICA—RISAA took some steps backward. That includes the ECSP provision. It also includes a couple of provisions that actually weaken amici that we haven't talked about yet. Maybe we can talk about them later. That is, yes, that.

Mr. VAN DREW. In plain vernacular, though, the FBI still needs a makeover, it still needs. We can't give up on this.

Mr. Chair, I know I am over. Just for a second, I love old mystery shows, old mysteries. I was watching an old mystery. It dates back to the 1940s, and they are talking to the FBI and how they overreached and were punishing somebody because they disagreed with something they did.

I was sitting with a friend of mine and said, "God, that would never happen." He said, "Boy, are you wrong." That show was right.

Thank you. I yield back.

Chair JORDAN. To the gentleman's point, I said this earlier, I do believe it is accurate to say of the $12 billion budget that the FBI has, over half that budget is spent on surveillance or surveillance-like activities.

I believe over half the personnel, to Mr. Tolman's point, you want them to go after the bad, the bank robbers, and the drug dealer, those kind of folks, versus what seems to be the focus the last several years.

The gentleman from Florida, the new Ranking Member is recognized.

Mr. MOSKOWITZ. Thank you, Mr. Chair.

Mr. KNOTT. Will the gentleman yield?

Mr. MOSKOWITZ. For a second. Sure.

Mr. KNOTT. I was kidding. Go ahead.

Mr. MOSKOWITZ. Oh. I was really interested in what was about to happen. You fooled me, too, Brad.

Well, I was going to say, Mr. Chair, thank you. I sit at the end of the dais. I am the last Democrat here. Many questions and comments have already been made on this important topic which is FISA. I am absolutely for FISA reform.

Mr. Chair, when I think about FISA, what I really think about? I think about affordability and the hopes of affordability, OK. Because, perhaps someone should tell the President that every time he says "affordability is a hoax," another Democrat spouts of the ground and lands in the House of Representatives. Eventually we will get a gavel.

If he doesn't like saying "affordability," that is fine. We can come up with another word. If he doesn't want to say that things are unaffordable, we could just say things are expensive. We could agree to just say that instead. We could just say things are expensive instead of unaffordable.

I really want to talk to the person who puts the words into the teleprompter. Because this is like a Ron Burgundy situation. Every time he says "affordability is a hoax," it—

Mr. VAN DREW. Will the gentleman yield?

Mr. MOSKOWITZ. In a second. Let me do this and then I will yield.

Every time he says "affordability is a hoax," it is like saying, "Go F— yourself, San Diego," OK? Is it San Diago? Scholars say the translation was lost long ago.

There is just no partisanship on the grocery store bill. I know what you are saying, Jared. Be honest. Tell the other side of the coin.

OK, gasoline prices are down. Right? See, I am being fair. Gasoline prices are down. That is great. Getting energy prices down is important.

They are not as down as much as he is projecting. The problem is you can't eat gasoline, right? Can't eat gasoline unless, of course, Kennedy proposed that as some sort of way to get rid of COVID. OK?

What I would say is that even though we all subscribe to our own set of facts these days, we do the only thing that still is a constant is that $2 + 2 = 4$, for now. OK.

When you go to the grocery store and you get the bill, there is no partisanship on the bill. There is no partisanship on that bill, it is just prices.

You can go to all the stadiums you want. You can fill all the stadiums you want. You can talk about this being a hoax all you want. As long as people are paying double and triple for groceries, rent, health insurance, home insurance, transportation, and car payments, that won't work. OK.

You are going to say, Jared, how do you know it won't work? We tried it. We tried it for a whole year during the election. The econ-

omy is great. The stock market is great. We tried to tell people how to feel. It didn't work.

In the weirdest plot twist ever, I can't believe Trump is copying your favorite President Joe Biden. I feel like any moment Trump is just going to be "Trumponomics is great."

It is just wild. I feel like Howard Lutnick is about to come on television and talk about how crudites prices are coming down. Right?

Let me just say this is why I believe in FISA reform, OK. Now, I will yield to your question.

Mr. VAN DREW. Well, you almost started to answer for me, so I love you, man, you are a great guy. Great Congressman. That doesn't have a damn thing to do with what we are talking about today.

Mr. MOSKOWITZ. I know, but 50—

Mr. VAN DREW. Let me just finish.

Mr. MOSKOWITZ. Fifty people already spoke and asked all the questions and comments.

Mr. VAN DREW. I know. The subject matter today is really, really important. I get it. I get the politics. I get the affordability. We can have that argument.

Mr. MOSKOWITZ. No, well, affordability is probably slightly more important.

Mr. VAN DREW. This is people's personal freedom. Let me tell you, people died multiple times, in many wars right back to the Revolutionary War, so people could believe what they want to believe, say what they want to say, believe in a god that they want to believe in.

Mr. MOSKOWITZ. Reclaiming my time quickly, and then I will yield back.

Listen, don't get me wrong, the Revolutionary War is very important. Most Americans care about what they are paying for goods today rather than what happened during the Revolutionary War.

Mr. VAN DREW. If the gentleman would yield again?

Mr. MOSKOWITZ. Yes, I will yield back.

Mr. VAN DREW. They do. They also care about the—they care if their daughter, or son, or brother, or sister is being surveilled, if they are losing their freedom, if the judicial system is going out to hurt them because they believe something different.

Mr. MOSKOWITZ. Reclaiming my time quickly.

Mr. VAN DREW. It is a big deal. That matters. That is what we should be doing today.

Mr. MOSKOWITZ. Yes, reclaiming my time. I know they do care about that. If they can't pay their rent and they can't feed their family, the rest of it is less important.

That is why I brought up affordability. Because, quite frankly, it is not a hoax. It is a real thing, just like FISA is. We are just not having hearings on that. I am still waiting for Pam Bondi to come back.

We have got a week left but—Oh, the Chair has got something on?

Chair JORDAN. No. I was just—

Mr. MOSKOWITZ. Oh, I didn't know if you had an announcement. I yield back, Mr. Chair.

Chair JORDAN. No, I was going to cut you off, but not until you had your full five minutes.

Mr. MOSKOWITZ. I appreciate my position on the Committee.

Chair JORDAN. Yes. Ms. Bondi is coming. She was scheduled and then we had this 43-day, month-and-a-half shutdown by the Democrats, so she wasn't able to be here.

Mr. MOSKOWITZ. Oh, then the Speaker furloughed us 55 days. I had never been furloughed before, by the way.

Chair JORDAN. We will have her. The gentlelady from Wyoming is recognized.

Ms. HAGERMAN. Classy Democrat ploy, deflect attention from every single thing that he described about affordability being caused by their policies, and then turning it around and attempting to blame us for the problems that they created with the housing, the increase in housing costs, and the increasing food costs.

We are fixing those things, the policies that they implemented. I have every expectation that we will see a decline in some of those prices next year.

I actually want to talk about why we are here today because it is a very important hearing.

I have long been a proponent for including sunsets in government programs and authorities. I believe we commit legislative malpractice in a lot of the things that we do when we don't include sunsets. I hold this principle to be especially true when dealing with technology and technological advances. We always seem to move much more faster than government. We could evolve when we are drafting our bills.

The FISA is a perfect example of this issue since its creation in 1978. The scope of FISA authorities has continually grown, as has its abuses. As the intelligence agencies we oversee push their surveillance abilities beyond the statutory allowances, that issue today is compounded by new technologies and the commercial availability of data. Today we, as legislators, face two unique challenges.

First, reforming Section 702 to correct past abuses, which for some appears to be a controversial exercise even of itself, although I don't see that as to why it should be controversial.

Second, we also need to update Federal laws and protections to account for the pace of technological advancement.

Here we are, we are actually talking about working on reforms with a chance to vote on those reforms in 2026 for the second time in my two terms in Congress, which I think is a really good deal. Why? Because Congress was wise enough to sense that these important authorities to aid in our ability to consistently review them.

Mr. Czerniawski, technological advancement and the private sector always seem to move faster than the government. Does maintaining these two-year reauthorizations of Section 702 provide a better chance for us to keep up with the pace of those changes, and also to address any violations that we may see?

Mr. CZERNIAWSKI. Thank you for the question, Representative.

That sunsets on a shorter timeframe are an amazing tool for you and this Committee, more broadly speaking, to assert its authority and its oversight function over these critical agencies. We want

them to be able to go and do their national security mission to keep this country safe.

At the same time, as you documented and as these witnesses documented, there is a litany of abuses that FISA has enabled. What better way to make sure that is on decline if not, hopefully, ideally, eliminated them by having these shorter reauthorization periods.

Ms. HAGERMAN. I have been an advocate for the warrant requirement and some of the other changes that we have made, some of the other modernization, and the safeguards that we have put in place.

You have been asked an awful lot of questions today. What I would like each of you briefly to do is to describe for me, for us, if you see any other reforms that we should be making when we revisit this in April of next year.

Mr. Tolman, starting with you, have we touched on all your proposed changes or do you have additional ideas that you would like us to consider?

Mr. TOLMAN. With respect to 702, we have addressed them.

With the FBI, we have work to do. Shifting their mission back to interdiction of drug and violent crime should be their central focus, and not the gathering of intelligence. Until then, we will see abuses that we have to reign in.

Ms. HAGERMAN. Just very quickly. I don't know if you are aware, but at the beginning of the 118th Congress when we were doing the Select Committee on Weaponization of the Federal Government we had a former FBI agent who came and testified. He talked about how the mission had been shifted after 9/11. You touched on that briefly today as well.

I agree with you. We need to get back to a pre-9/11 mentality with regard to the FBI. It is important and I appreciate your advice in that regard. Mr. Schaerr?

Mr. SCHAERR. Thank you for the question. If I could add one thing to the four specific reforms that I mentioned earlier, I would add the NDO Fairness Act, which I know this Committee has already passed and reported out.

Perhaps that could be attached as part of the 702 reauthorization bill, because it is certainly closely related to the items in that bill. I suggest adding that.

Ms. HAGERMAN. Thank you. Mr. Czerniawski?

Mr. CZERNIAWSKI. Yes. I would second Mr. Schaerr's point about adding the NDO Fairness Act into that, and everything else, the four core ones that we mentioned, too.

Mr. HAGERMAN. Thank you. Ms. Goitein?

Ms. GOITEIN. If there is one thing I would add to those four things, which I agree with, it would be closing the backdoor search loophole for Executive Order 12333 collection.

Mr. HAGERMAN. OK. Thank you. I appreciate it. With that, I yield back.

Chair JORDAN. The gentlelady yields back

If the gentleman from South Carolina, we are going to just flip. Because Mr. Grothman has to go, we will go with Mr. Grothman, and then we will come right to you, Mr. Fry.

Mr. Grothman is recognized.

Mr. GROTHMAN. Thank you.

Mr. Schaerr, when the FBI asks for, asks the FISA Court for a Title I warrant to surveil someone in a politically sensitive case, let's say a Member of Congress, an employee of a Presidential campaign—this actually happened to President Trump—this all takes place in a secret proceeding, right?

Mr. SCHAERR. Correct.

Mr. GROTHMAN. Generally speaking, is there anyone in the proceeding advocating for privacy rights in the Constitution?

Mr. SCHAERR. No. Currently there is not and that is a big problem.

That was a process which if it had been in place during the Carter Page investigation would have prevented the shenanigans that happened there. In fact, it could well have deterred the FBI and the Justice Department from even seeking that warrant at all.

Mr. GROTHMAN. Can you give us a suggestion on what to do about it?

Mr. SCHAERR. Yes. The best solution is to adopt something along the lines of the Lee–Leahy reform that was adopted by the Senate about four years ago by a vote of 77–20, or something like that. What that reform would do is ensure that there is, in particularly sensitive investigations, that there is an amicus in the room and as part of the process when the FISC considers granting a warrant in those kinds of cases.

It would be somebody who is trained in privacy, somebody who has a full security clearance and can serve as a check, a counterweight if you will, to the Justice Department lawyers who, of course, will be seeking the warrant, but somebody who can be there and knows enough about the process to be able to help the FISC judges ask the right kinds of questions to be sure that there aren't any shenanigans going on.

Mr. GROTHMAN. OK. You have spoken about the data broker loophole where Federal agencies, ranging from FBI, the IRS, buy geolocation, internet search, purchase history, and other sensitive information about Americans, all without a warrant or any reason to believe most of these people have done anything wrong.

As we consider Section 702, a surveillance authority that has been repeatedly abused by the FBI, why is it important to also look at other Government practices like data purchases that violate Americans' constitutional privacy rights?

Mr. SCHAERR. Well, thank you. Thank you for that question. You are absolutely right that purchasing data can be an effective way, currently, for agencies to do an end run about the Fourth—around the Fourth Amendment. They shouldn't be allowed to do that.

Whether or not they are allowed to purchase the data, they shouldn't be allowed to use it to surveil Americans without going through the same warrant process that we have been talking about with respect to the Section 702 database.

Mr. GROTHMAN. Are there any procedures in place now to protect against the malignant use of FISA?

Mr. SCHAERR. From the malignant use of FISA?

Mr. GROTHMAN. Malignant use of FISA, yes.

Mr. SCHAERR. Well, there are some procedures in place, and some that were enacted by this body a couple of years ago that are

useful and important. There are a number of others that need to be added like the warrant requirement for backdoor searches.

Mr. GROTHMAN. Are there any consequences for FBI agents that conduct improper searches?

Mr. SCHAERR. I understand there are potentially some administrative consequences that they can lose their security clearances if they are found to have violated the department's own rules.

Mr. GROTHMAN. Have they ever been used?

Mr. SCHAERR. Not that I know of.

Mr. GROTHMAN. OK. How did the FBI allow such a profound breakdown in internal communication and verification processes, investigators failed to properly report Carter Page's status as an operational contact, information they already possessed, ultimately enabling an attorney to alter communication and result in nearly a year of unlawful surveillance?

Mr. SCHAERR. Well, the independent counsels who investigated that whole sordid history, concluded that it was not just an innocent mistake.

Mr. GROTHMAN. OK. Mr. Tolman, we will try to get you a quick question at the end.

There are reports indicating that some agencies are spending tens of millions of dollars on multiyear contracts to purchase sensitive data on American citizens. Can you elaborate what problems this poses?

Mr. TOLMAN. Well, first and foremost, if the internal guidelines to help prevent abuse become effective, the FBI's response is to not stop wanting to get that information. Instead, they've pushed it out to purchase that information, and it's the tip of the iceberg. If they expand that program, there's no end to what they can get without a warrant.

Mr. GROTHMAN. OK. Thank you very much.

Chair JORDAN. The gentleman yields back. We have about 20 more minutes. If that's good, we will just keep on moving. Oh, does someone need a break?

Ms. GOITEIN. Ideally. Two minutes.

Chair JORDAN. I understand. We will take a—you can take a break.

Ms. GOITEIN. OK.

Chair JORDAN. If your questions are going to the gentlelady, we will hold. If not, we will let you, Mr. Fry, continue with the three remaining witnesses.

Mr. FRY. We will move around. We have got a lot of questions.

Chair JORDAN. All right. All right.

Mr. FRY. Thank you, Mr. Chair.

Mr. Schaerr, would you agree that the Woods Procedures serve as a good-faith oversight safeguard and that obstructing them in any way removes and undermines public trust in the FISA process?

Mr. SCHAERR. I'm not proposing that they be removed or obstructed. If they work properly, then they serve a useful function, but they're no substitute for Congress' playing its role in ensuring accountability.

Mr. FRY. Do you agree that they serve as an oversight safeguard?

Mr. SCHAERR. Yes.

Mr. FRY. Violating them by some government official would undermine public trust in what the government is—

Mr. SCHAERR. I'm sorry, I misunderstood your question. You're right, violating them would undermine the public trust, I agree.

Mr. FRY. Thank you for that. Mr. Tolman, during Crossfire Hurricane, FBI attorney Kevin Clinesmith altered an official document using a FISA application, enabling the government to illegally surveil Carter Page for 11 months. Clinesmith, ultimately, received 12 months—only 12 months of probation. Do you believe that's sufficient punishment for his violation?

Mr. TOLMAN. It serves as no deterrence. Deterrence is the predictability of being held accountable, and—

Mr. FRY. That was my next question, too, which was, to the extent that you didn't think that it was sufficient, would that be an actual deterrent for other people seeking to violate, seeking to violate FISA? Are there additional avenues that exist to hold the FBI accountable in lieu of that?

Mr. TOLMAN. There really are no avenues. In fact, the ethics investigations that would be conducted are all handled in-house. Subsequently, any Solicitor General or Office of Inspector General that would actually attempt to investigate it, they're limited, in that they can't themselves bring any criminal action. I would say there's no current deterrence.

Mr. FRY. How would we increase that deterrence?

Mr. TOLMAN. Well, certainly not relying on the courts and a Washington, DC, jury to actually administer accountability.

Mr. FRY. Mr. Tolman, are you saying that Washington, DC, doesn't have all the answers for the American people?

Mr. TOLMAN. I think that's exactly right. This is why Congress is so important right now.

[Laughter.]

Mr. FRY. Thank you for that. I wholeheartedly agree.

Mr. Schaerr, back to you. In 2019, the U.S. Court of Appeals for the 2nd Circuit raised concerns about Section 702's ability to enable broad queries of Americans' communication. The Court, essentially, held that law enforcement cannot search people's communications without any suspicion just to see if something incriminating turns up, which, of course, it would violate their Fourth Amendment rights.

Is this an example, though, of government fishing for criminal evidence at the expense of the Constitution and people's Fourth Amendment rights?

Mr. SCHAERR. I think that's a fair characterization.

Mr. FRY. How widespread to you believe this practice is?

Mr. SCHAERR. Well, just from the number of queries that are run, it seems like it's quite widespread, and yet another reason why it's important to have a warrant requirement before the 702 databases can be searched.

Mr. FRY. Well, I agree with you there, too. The number of queries and the amount of people that have access to this is very alarming as well.

What do you think this also reveals about the culture within the FBI, that they do this with impunity without regard to people's constitutional rights and without any reasonable suspicion that any

particular person has engaged in some criminal activity—unless they just happen to dig it up?

Mr. SCHAERR. Well, certainly, the whole Carter Page fiasco and many of the other examples that we've discussed today are examples of an investigation culture that seems to have run amuck, and yet another reason why the Article III branch should be brought into the mix to exercise some oversight.

Mr. FRY. Thank you for that. I'm going to switch gears just a little bit to just about government data purchasing. Obviously, government agencies are using this. In what ways should Congress look to close these loopholes that allow them to purchase this data that evades people's Fourth Amendment liberties?

Mr. SCHAERR. Is that to me?

Mr. FRY. Yes, sir.

Mr. SCHAERR. Well, whether or not Congress decides to allow the agencies to purchase the data, how they use it is the key question. Before the government can search any database, whether it's the 702 database or a database consisting of data that has been purchased, there should be a requirement that if they're looking at sensitive personal data, including people's communications, that they ought to have to get a warrant to search it.

Mr. FRY. Thank you for that. Mr. Chair, I see my time has expired and I yield back.

Chair JORDAN. The gentleman yields back. The gentleman from North Carolina is recognized.

Mr. KNOTT. Thank you, Mr. Chair. Thank you for holding this hearing. To the witnesses, we certainly appreciate your duration, your endurance, and the candid answers that you have given.

I have got to say that every time we bring this statement up, it stuns me. We pass a law to surveil foreign threats to the country, and we abuse it by spying on the United States citizens that we are tasked to protect. When you boil it down in that simple term, it is stunning. It is stunning.

Warrantless access is allowed under a trust agreement with those who are investigating, this comes from someone, myself, who worked with agents. I worked with law enforcement professionals all over this country who are very proficient at investigating. I was proud to do it. I was honored to do it.

I must say that this particular set of the law is entirely too secretive. It is entirely too bureaucratic. There is absolutely no disinfectant of the bright lights of a courtroom that people have access to.

When you look at the kind of the construct, plainly speaking, with this power, it enables the investigators to target people, not criminal behavior. That is the inherent danger that I see here.

When you open up just the documented abuses—again, even the documented abuses we receive in a report and we trust that those are all the abuses, right? That is, to me, again, a very problematic posture.

Some of the abuses include intrusive searches for nefarious or creepy reasons, right? Personal reasons from bureaucrats who are nameless and faceless, who have not been fired or punished.

Some of these intrusive searches are for political motivations. Again, see Carter Page, right? There is no disinfectant of the bright light.

When I was doing these investigations, we would observe criminal conduct. We would seek authority to get the information, and then we would get the warrant. Right? Then, once the information was in hand, we would go through it to determine what charges, if any, would come forward.

With that as my basis, let me just ask: Is it a problem that the information is already in hand before any warrant is ever needed in the process? Mr. Schaerr?

Mr. SCHAERR. It is a problem. It's probably inherent in the whole Section 702 collection process and in the legitimate need to engage in surveillance of foreigners. It's a problem that is easily solved with a warrant requirement.

Mr. KNOTT. How?

Mr. SCHAERR. Before the information can be queried on individual Americans, then there needs to be a warrant in place.

Mr. KNOTT. Well, that is getting to the root of my problem.

Mr. SCHAERR. Yes.

Mr. KNOTT. The "query" is a fancy word for "search."

Mr. SCHAERR. Correct.

Mr. KNOTT. There is no way to prevent searches in the back channels of a deep government bureaucracy, correct?

Mr. SCHAERR. There may be no way to prevent them, but there's certainly ways to deter them.

Mr. KNOTT. Sure, but we are not doing that. Again, you have a pot of information—

Mr. SCHAERR. Yes.

Mr. KNOTT. —in the back channels of a bureaucracy, and we are trusting them not to abuse access. Is there a way to preclude access to that information without a warrant?

Mr. SCHAERR. Not that I'm aware of, which is why a warrant requirement is so important.

Mr. KNOTT. That's my problem. Yes, that's my problem.

Is there a way to preclude—or is there a way to gauge whether or not there have been queries, if they want to hide those queries? "They" being the FBI.

Mr. SCHAERR. Yes. I'm not sure there's a way to do it.

Mr. KNOTT. Mr. Tolman?

Mr. TOLMAN. No. My concern is, if, for example, take the analogy that the searches are large boxes in an Amazon truck, right?

Mr. KNOTT. Right.

Mr. TOLMAN. If the FBI knows that each box has multiple individuals in it, my concern is they'll say, "We're only going to search this box"—

Mr. KNOTT. Right.

Mr. TOLMAN. —where the target actually is—but there's multiple individuals that deserve protection under the Fourth Amendment.

Mr. KNOTT. Right.

Mr. TOLMAN. We don't get to when they're searching those.

Mr. KNOTT. Right. You were raising your hand, ma'am?

Ms. GOITEIN. Yes. You raise an excellent point, which is, if they collect pretty much everything, any of these back-end protections, including the requirement to get a warrant, are going to be imperfect necessarily.

Mr. KNOTT. Right.

Ms. GOITEIN. That is a very good reason to limit the collection on the front end.

Mr. KNOTT. Yes.

Ms. GOITEIN. One of the reforms—

Mr. KNOTT. Just so people know, we would have evidence that a criminal actor was using his or her cell phone. We would ascertain the number through investigative means, and then we would apply for a warrant to get location data, who they were calling. Then, if need be, the most intrusive search was a Title III wiretap. We had to bend over backward to demonstrate the need to get the information that the government right now is collecting en masse—with no warrant. It is really astounding to me.

If there is no way to protect against abuse, I wonder what the solution is? I will turn it over—if you could go down in sequence, starting with you, ma'am, what are ways that we can protect that information, in addition to the warrant requirement?

Ms. GOITEIN. Well, what I was going to say is that the initial scope of surveillance right now is too broad. Any foreigner can be targeted overseas under this broad definition, extremely broad, of foreign intelligence.

What that means is foreigners who there's no evidence or reason to believe that they pose any threat to the United States or their interests, they are subject to surveillance. What that means for Americans is that the pool of Americans' communications that can be incidentally collected is enormous.

Mr. KNOTT. Right. Right.

Ms. GOITEIN. It's likely to be these innocuous conversations. Refining the foreign targets at the front end would be an enormous protection for Americans. That is something I talk about in my written testimony.

Mr. KNOTT. Thank you. Briefly.

Mr. CZERNIAWSKI. Yes, I will just say what Liza said; refining down the scope of surveillance.

Then, I know RISAA already did this with reducing the number of FBI agents that have access to that database. I would say exploring how we can and further reduce that number. Chair Jordan mentioned 10,000 before, like—

Mr. KNOTT. A shared custody of it.

Mr. CZERNIAWSKI. Yes, exactly.

Mr. KNOTT. Something.

Mr. CZERNIAWSKI. Yes.

Mr. KNOTT. Mr. Schaerr?

Mr. SCHAERR. I agree with those comments.

Mr. TOLMAN. I would say perhaps we established something like the taint team. You recall how we utilized that, where we would not allow those access to documents and data that might be violative. Perhaps there's a layer that could be put in there that would prevent investigators from actually looking at the data until they've satisfied those protocols.

Mr. KNOTT. Mr. Chair, I yield the balance of my time to the Representative from Texas. Thank you all.

Chair JORDAN. The gentleman from Texas is recognized for five minutes.

Mr. GILL. Thank you, Mr. Chair. Thank you to the witnesses for taking the time to be here and for your expertise.

I entirely associate myself with the great line of questioning from my friend, Mr. Knott of North Carolina. I want to begin and just kind of break this down really quickly on a basic level. Ms. Goitein, what is the Section 702 database?

Ms. GOITEIN. It's not a single database per se. Section 702 enables the government to collect the communications of certain foreign targets, which is pretty much any foreigner, if the government has a foreign intelligence purpose, and to collect any information on them, including all their communications, and that includes communications with Americans. All that gets fed into various different data systems that different agencies have.

Mr. GILL. How vast are these data systems? In other words, what types of information is being collected and about whom?

Ms. GOITEIN. Right. We have very little public information about that. In 2011, which I think is the last time this particular statistic was reported, there were 250 million communications, internet communications, obtained. That was when there were far fewer targets.

If you extrapolate with the number of targets we have today, it's about a billion communications, internet communications, collected every year. Because they reside in these systems for at least five years, several billion communications right now in storage, collected under 702.

Mr. GILL. What are these communications? Are these calls, texts, emails, and location data?

Ms. GOITEIN. It can be anything and it doesn't have to be communications. It can be any kind of foreign intelligence information, or information that qualifies as foreign intelligence. Actually, it doesn't have to be foreign intelligence. The government just has to have a foreign intelligence purpose. It can be any kind of information imaginable but, definitely, it includes electronic surveillance which is communications.

Mr. GILL. Got it. Who could be tied up in this database in terms of American citizens, Members of Congress, everyday American citizens? Who all could be caught up in this?

Ms. GOITEIN. Right. There are almost 300,000 foreign targets, and they do not, as I said before, they don't have to be suspected of any wrongdoing. Anybody who has the misfortune of being in communication with someone who has been designated as one of these targets, their communications will be swept up.

Mr. GILL. We have billions of data points from American citizens who have never been convicted of a crime?

Ms. GOITEIN. Well, not all the billions involve Americans. We don't know what proportion involves Americans because they won't give us an estimate.

Mr. GILL. We don't know, but a large number?

Ms. GOITEIN. Presumably, because of the prevalence of international communications.

Mr. GILL. Presumably, a large number? Where does all this information sit?

Ms. GOITEIN. Different databases in different agencies.

Mr. GILL. Uh-hum. That's all within the Federal Government that various actors have access to?

Ms. GOITEIN. Yes.

Mr. GILL. Who? Who has access to this information?

Ms. GOITEIN. Agents who are working on cases. I think it's a lot. We heard earlier it's basically 10,000 FBI agents. It's any FBI leaving aside the NSA and the CIA. It's agents in field offices all around the country.

Mr. GILL. They don't need a warrant to access any of it?

Ms. GOITEIN. No.

Mr. GILL. OK. What types of protocols or procedures are in place to help protect privacy of American citizens' data that's, it sounds like, all within multiple agencies of the Federal Government?

Ms. GOITEIN. Right. There have been reforms that were put in place through last year's reauthorization of Section 702 that required things like attorney approval. The U.S. person queries, it required people to keep a written justification of their queries—agents. It requires an audit every six months by the National Security Division of queries. It required supervisory approval for certain sensitive queries.

It's there, sort of layers on layers of these sort of internal review or oversight mechanisms. Many of these were in place well before RISAA codified them, and even after these internal mechanisms had been adopted, we were still seeing abuses. We were seeing searches for the communications of a U.S. Senator, a State Senator, a State court judge who had contacted the FBI to report civil rights violations by a police chief. That was after many of these reforms had been adopted.

Have they helped? Probably. Again, we don't have complete data from this past year. They're not enough.

Mr. GILL. There's millions of—potentially more—bits of communication information of American citizens sitting in various government databases that FBI agents have access to without requiring—obtaining a warrant. That seems like a pretty egregious violation of the Fourth Amendment, does it not?

Ms. GOITEIN. To me, that is a violation right there. Even if every single query complies with the internal standards and procedures that have been adopted, it's not probable cause and a warrant, and therefore, it's a Fourth Amendment problem.

Mr. GILL. Agree. Thank you.

Chair JORDAN. The gentleman yields back. The gentleman from North Carolina is recognized.

Mr. HARRIS. Thank you, Mr. Chair. I thank all of you for your time and patience and apologize for being in and out with three different committees holding hearings and markups all today.

Listen, as a freshman Member of Congress, as I have had the opportunity to listen today, I'm delighted to see that this Committee is united in defending Americans' Fourth Amendment rights. As we approach FISA reauthorization, I do think it is important to build on the progress made last Congress in protecting Americans from unconstitutional searches.

That starts with addressing some of the shortfalls of last year's reauthorization and the Reforming Intelligence and Securing America Act, also known as RISAA. Obviously, my biggest concern is the

failure to include a warrant requirement, which failed as an amendment on the House floor. However, I understand there were other provisions in the bill that ought to be addressed.

One concern I have is the expansion of the definition of electronic communication service providers. I have been a pastor for 36 years, and I often worry about the ways in which government can be weaponized against churches and other religious institutions.

Mr. Schaerr, does the expanded electronic communications service provider provision in RISAA mean that even churches and other places of worship could be demanded to facilitate the warrantless surveillance of their people?

Mr. SCHAERR. I believe so. If you look at the requirements for being considered in ECSP—an ECSP, an electronic communications service provider, most churches are providing Wi–Fi service to their parishioners when they come. My church does; I suspect your church does. They do that using communications equipment, right? A Wi–Fi router that may be installed in the ceiling or somewhere else.

They really fit the definition of an ECSP, and therefore, at any moment, somebody from the FBI could come along and say, "You have somebody in your congregation that we're suspicious of and we want you to give us access electronically to everything that they're doing on their phone when they use your Wi–Fi service during the service."

They could force you, as a pastor, to do that. They could also order you that you can't tell the person about it. Right? It's they're really dragooning people into secret surveillance of their parishioners or customers, if they're a small business, or whatever it may be.

Mr. HARRIS. Wow, that's pretty scary.

Mr. SCHAERR. We don't know if it's actually happened, but the way the law was drafted, that would be allowed.

Mr. HARRIS. Exactly. Well, Mr. Schaerr, your group, the Project for Privacy and Surveillance Accountability, lists on its website, quote, "Solutions to protect privacy and restore appropriate legal protections."

The first solution on this list is requiring annual audits of surveillance programs. How does oversight of the use of FISA by government agencies currently operate?

Mr. SCHAERR. Well, the most effective oversight right now is this process of having to have it reauthorized every couple of years. In the old days when it was every five years the agency would, basically, do what they wanted until about a year before the reauthorization, and then they would try to clean up their act. They can't do that anymore. Just this annual process—or this biannual process is useful.

Mr. HARRIS. Are there specific additional steps that you believe Congress can take to improve the oversight of the use of FISA by our government agencies?

Mr. SCHAERR. Demanding more information from the FBI and the Justice Department about how these programs are actually being used, and then, following up when they inevitably don't respond.

Mr. HARRIS. Well, thank you very much for that.

Mr. Czerniawski, in your written testimony, you mentioned that the intelligence community has used artificial intelligence to assist in conducting surveillance. While we all want our intelligence community to be able to conduct proper surveillance of foreign actors who seek to do us harm, we have got to ensure that developing technology is not used to further violate our Fourth Amendment.

In just the last few seconds we have left, what steps would you say that Congress can take to ensure law enforcement uses AI in a way that respects Americans' Fourth Amendment rights?

Mr. CZERNIAWSKI. Absolutely. Thank you for the question, Representative.

That we don't want to necessarily deter agencies from using new technologies to help them carry out their public mission. That being said, as that technology's capacity to go and help them potentially violate people's rights gets that much greater, it makes that much more important that we have these guardrails in place.

Having that warrant requirement, as Congressman Knott was talking about before, the procedural elements of getting that warrant are very important to carrying out the mission, but they don't even have to worry about that right now, right?

If we're going to be leveraging these powerful technologies, let's make sure that we have those processes and procedures in place to minimize, and hopefully, ideally, eliminate the misuses that have been well-documented for years.

Mr. HARRIS. Well, thank you so much. Thank you all again for your time and your persistence. Thank you, Mr. Chair. I yield back.

Chair JORDAN. The gentleman yields back. We are almost there. The gentlelady from Texas is recognized.

Ms. CROCKETT. Thank you so much, Mr. Chair. I share the concerns of all my colleagues that they have mentioned this morning as this hearing has been taking place.

The most important part of making reforms to government surveillance programs is ensuring that Americans' privacy rights are not being violated, but that requires Congress to do its job and conduct oversight of these Executive Branch programs.

We all agree that significant reforms are needed for FISA, but over the past year, Republicans in the House and Senate have allowed this President to be careless with Americans' private data. This administration can't even prevent American citizens from being arrested in their mass deportation machine. Why should we believe that they will be able to prevent Americans' private data from being unconstitutionally collected throughout government surveillance programs?

For FISA to actually work as intended, Federal agencies need enough staff and resources, but most importantly, they need competent leadership. Unfortunately, this President and his Cabinet have shown themselves to be incapable of understanding the seriousness of handling sensitive information or protecting Americans' private data.

When you have the Defense Secretary sending classified information to the Vice President through Signal, or when extremist billionaires are allowed to have access to Americans' private data, or when ICE signs contracts to use surveillance technologies against Americans who are critical of their violent deportation tactics, all

this shows that this administration isn't serious about following the rule of law or protecting Americans' privacy rights.

We can talk for hours about legislative reforms needed for FISA, but none of it will matter if Republicans refuse to conduct actual oversight, or if they continue to allow the administration to dismantle Federal oversight offices and positions.

Under this administration, numerous Federal agencies have fired internal agency record officers, used auto-delete technology when communicating, and stopped requiring the preservation of Federal records.

Ms. Goitein, OK, we often learn about abuses in Federal surveillance programs through whistleblowers. Can you explain how the destruction of Federal records can incentivize agencies to violate Americans' privacy records?

Ms. GOITEIN. I'm sorry, the destruction of Federal records?

Ms. CROCKETT. Yes.

Ms. GOITEIN. OK.

Ms. CROCKETT. Can you explain—

Ms. GOITEIN. Oh. Oh, OK. OK. Sorry, yes, my apologies. Yes, I'm following you.

Yes, there's reasons why there are records retention schedules in the law, and it's because this is the official record of the official action. It is needed for all kinds of purposes. It's needed for continuity over time with other administrations. At times, it can be needed for litigation.

It, certainly, can be important to reveal misconduct—fraud, waste, abuse—whether through internal oversight channels, whether through oversight by Congress, the courts, or through whistleblowers. Yes, it's important to preserve Federal records, in accordance with the preservation schedules.

Ms. CROCKETT. Thank you so much. How have unchecked surveillance powers historically been used against marginalized groups?

Ms. GOITEIN. Oh, it is such a long story. It's not just in this country, right? It's around the world. Surveillance is a tool by which governments have oppressed marginalized communities of all kinds.

In this country during the cold war, there was widespread spying by the FBI, the CIA, NSA, and their predecessor names for them. That surveillance was targeted against antiwar protestors. It was targeted against social justice movements. It was targeted against Martin Luther King, Jr. It was targeted against political opponents of—whether it was the President or people high up in the administrations.

That is a feature of this country's history that actually led Congress to pass FISA and to get some kind of control over foreign intelligence surveillance. A lot of these abuses were in the name of foreign intelligence. These were purported attempts to find out if there was foreign influence over certain movements. It led to a number of other reforms by Congress.

The problem is that, since then, and especially since 9/11, some of the protections that were built into the law, including FISA, that were meant to deter this kind of spying based on politics, race, ideology, and religion, have been stripped out. Particularly after 9/11,

they were stripped out very, very quickly, based on a sort of misguided sense that this was the way that we were going to stop a future terrorist attack.

Ms. CROCKETT. Thank you so much.

Ms. GOITEIN. As a result, we're vulnerable once again. I'm sorry I took so much time.

Ms. CROCKETT. No, no, no. That's OK. Thank you so much. I appreciate you. With that, Mr. Chair, I will yield.

Chair JORDAN. The gentlelady yields back. I want to thank you all.

It seems to me everyone is probably in this giant database, wherever it may reside. We have tried reform after reform, and while helpful, it never seems to fully correct the problem.

The deterrence, the penalties, probably aren't there for those who continue to abuse it, as evidenced by the one guy who actually, on the Title I side of things, lied to the FISA Court. He changed a document. He is back practicing law; got his law license, and never really got any kind of real sentence.

The only answer, it seems to me, is what we have been spending 3½ hours talking about—is to get the warrant requirement in there. We will continue to do that, continue to work on that, and hopefully, get it done.

You guys have been a tremendous panel. We appreciate you being here and the excellent testimony that you gave.

That concludes today's hearing. We want to thank all our witnesses again.

Without objection, all Members will have five legislative days to submit additional written questions for the witnesses or additional materials for the record.

Without objection, the hearing is adjourned.

[Whereupon, at 12:31 p.m., the Committee was adjourned.]

All materials submitted for the record by Members of the Committee on the Judiciary can be found at: *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118740*.

○