

A CONTINUED PATTERN OF GOVERNMENT SURVEILLANCE OF U.S. CITIZENS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

TUESDAY, APRIL 8, 2025

Serial No. 119–15

Printed for the use of the Committee on the Judiciary



Available via: <http://judiciary.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California	JAMIE RASKIN, Maryland, <i>Ranking Member</i>
ANDY BIGGS, Arizona	JERROLD NADLER, New York
TOM McCLINTOCK, California	ZOE LOFGREN, California
THOMAS P. TIFFANY, Wisconsin	STEVE COHEN, Tennessee
THOMAS MASSIE, Kentucky	HENRY C. "HANK" JOHNSON, JR., Georgia
CHIP ROY, Texas	ERIC SWALWELL, California
SCOTT FITZGERALD, Wisconsin	TED LIEU, California
BEN CLINE, Virginia	PRAMILA JAYAPAL, Washington
LANCE GOODEN, Texas	J. LUIS CORREA, California
JEFFERSON VAN DREW, New Jersey	MARY GAY SCANLON, Pennsylvania
TROY E. NEHLS, Texas	JOE NEGUSE, Colorado
BARRY MOORE, Alabama	LUCY McBATH, Georgia
KEVIN KILEY, California	DEBORAH K. ROSS, North Carolina
HARRIET M. HAGEMAN, Wyoming	BECCA BALINT, Vermont
LAUREL M. LEE, Florida	JESÚS G. "CHUY" GARCÍA, Illinois
WESLEY HUNT, Texas	SYDNEY KAMLAGER-DOVE, California
RUSSELL FRY, South Carolina	JARED MOSKOWITZ, Florida
GLENN GROTHMAN, Wisconsin	DANIEL S. GOLDMAN, New York
BRAD KNOTT, North Carolina	JASMINE CROCKETT, Texas
MARK HARRIS, North Carolina	
ROBERT F. ONDER, Jr., Missouri	
DEREK SCHMIDT, Kansas	
BRANDON GILL, Texas	
MICHAEL BAUMGARTNER, Washington	

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

ANDY BIGGS, Arizona, *Chair*

TOM TIFFANY, Wisconsin	LUCY McBATH, Georgia, <i>Ranking Member</i>
TROY NEHLS, Texas	JARED MOSKOWITZ, Florida
BARRY MOORE, Alabama	DAN GOLDMAN, New York
KEVIN KILEY, California	STEVE COHEN, Tennessee
LAUREL LEE, Florida	ERIC SWALWELL, California
BRAD KNOTT, North Carolina	

CHRISTOPHER HIXON, *Majority Staff Director*
JULIE TAGEN, *Minority Staff Director*

C O N T E N T S

TUESDAY, APRIL 8, 2025

OPENING STATEMENTS

	Page
The Honorable Andy Biggs, Chair of the Subcommittee on Crime and Federal Government Surveillance from the State of Arizona	1
The Honorable Jamie Raskin, Ranking Member of the Committee on the Judiciary from the State of Maryland	3
The Honorable Jim Jordan, Chair of the Committee on the Judiciary from the State of Ohio	5

WITNESSES

James Czerniawski, Senior Policy Analyst, Technology & Innovation, Americans for Prosperity	
Oral Testimony	7
Prepared Testimony	9
Kia Hamadanchy, Senior Policy Counsel, National Political Advocacy Division, American Civil Liberties Union	
Oral Testimony	16
Prepared Testimony	18
Philip G. Kiko, Principal, Williams & Jensen	
Oral Testimony	31
Prepared Testimony	33
Gene Schaerr, General Counsel, Project for Privacy & Surveillance Accountability	
Oral Testimony	50
Prepared Testimony	52

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

All materials submitted by the Subcommittee on Crime and Federal Government Surveillance, for the record	76
--	----

APPENDIX

A statement from Jake Laperruque, Deputy Director, Security and Surveillance Project, The Center for Democracy & Technology (CDT), Apr. 8, 2025, submitted by the Honorable Jamie Raskin, Ranking Member of the Committee on the Judiciary from the State of Maryland, for the record

A CONTINUED PATTERN OF GOVERNMENT SURVEILLANCE OF U.S. CITIZENS

Tuesday, April 8, 2025

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT
SURVEILLANCE

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to notice, at 10 a.m., in Room 2141, Rayburn House Office Building, the Hon. Andy Biggs [Chair of the Subcommittee] presiding.

Members present: Representatives Biggs, Tiffany, Moore, Kiley, Lee, Knott, Cline, and Goldman.

Mr. BIGGS. The Subcommittee 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 Federal Government Surveillance.

I now recognize the gentleman from Alabama, Mr. Moore, 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.

Mr. BIGGS. I now recognize myself for an opening statement. I welcome my colleagues to this important hearing, and I welcome our witnesses and thank them for being here today.

The Fourth Amendment guarantees all Americans the right to be free of unreasonable government searches and seizures. With advances in technology, Americans' personal data has become easily tracked and collected and the Government can and does obtain this information without acquiring a warrant and without ever notifying an individual who is subject to a search. This is especially prevalent in the context of the Foreign Intelligence Surveillance Act.

Reports in recent years detail how the FBI, under the leadership of past FBI Directors, abused its authorities under FISA. The FBI used its authorities under Section 702 of FISA to conduct millions of queries of U.S. person communications. At its peak, the FBI conducted nearly three million such searches in 2021. In recent years, those numbers have begun to decline, but the FBI still conducts thousands of U.S. person-queries every month. These actions vio-

late the privacy and civil liberties of Americans and likely infringe on the Fourth Amendment protections.

I have called for serious reforms to FISA for years and last Congress, we undertook the task of attempting to rein in years of FISA abuses. Congress enacted a bill that included various reforms such as new and heightened criminal and civil penalties for those who violate FISA. We significantly reduced the number of FBI personnel authorized to approve queries. We required audits of U.S. person queries and implemented many new reporting and transparency measures. We must still work to protect the Fourth Amendment rights of all Americans.

I introduced an amendment to require a warrant for all U.S. person queries. This amendment included various exceptions to allow the FBI and the intelligence community to do its vital work of defending our homeland, while protecting Americans' privacy rights. This amendment has broad, bipartisan support and we worked closely with our colleagues across the aisle in an attempt to address this issue. I believe such a reform is necessary to end the abuses of Americans' rights.

While reforming FISA itself is not enough. The Government has plenty of other tools at its disposal to collect information on Americans. Currently, the laws governing law—excuse me, governing how the Fourth Amendment is applied in the digital context is the Wild West. Key legislation in this space is the Electronics Communications Privacy Act which was written in 1986 and did not take into account all the advances in digital communications that have occurred since. The IPO, for example, did not show up for two decades after this law was written. These cell phones have become such an integral part of our lives that as the Supreme Court has held now “hold for many Americans the privacies of life.”

Federal agencies are able to sidestep the requirements of the Fourth Amendment and access and collect massive amounts of private information on Americans while exploiting a legal loophole in this act. Rather than obtain a warrant, government agencies like the Federal Bureau of Investigation, the Intelligence Research Specialist, the Drug Enforcement Agency, and the Department of Homeland Security can simply turn to data brokers and purchase mass amounts of Americans' data. This includes such private information as location and health information and so on. Apparently, with a disturbing amount of frequency, data brokers sell Americans' personal information to law enforcement and intelligence agencies without any court oversight in contrast to strict rules that prevent phone companies and social media sites from selling such information to the Government.

We also are aware of reports by the Federal Government using facial recognition technology. This is a powerful tool that can be used to help solve crimes, but this technology also raises serious issues concerning First and Fourth Amendment rights. Law enforcement agencies could potentially use this technology to surveil individuals who are not engaged in any illegal activity whatsoever. For example, we have seen reports of ATF using facial recognition to find gun owners.

The Federal Government has also turned to private companies like Clearview AI to purchase access to facial recognition tech-

nology. Clearview AI pulls publicly available photographs from social media sites and puts them into a database marketed to law enforcement. Clearview AI's founders call the service a search engine for faces. The Government Accountability Office has conducted studies of Federal law enforcement entities' use of this technology in recent years. It found that Federal law enforcement agencies had not properly assessed privacy and other risks associated with the use of this technology. Some did not even know which systems their agents were using.

As technology continues to develop, the Government has more and more information about Americans available to it. Used improperly, this will continue a pattern of government surveillance of U.S. citizens that we have fought so hard against. Congress must protect the privacy rights of Americans and uphold the guarantees of the Fourth Amendment.

I look forward to this opportunity to discuss the dangers of mass surveillance and explore meaningful reforms. I appreciate our witnesses and the Members for being here today and the public for attending as well.

I now recognize the Ranking Member of the entire Committee, Mr. Raskin, for his opening statement.

Mr. RASKIN. Vote taken. Thank you, very much Chair Biggs and thanks to our distinguished witnesses for joining us here today.

The Fourth Amendment guarantees the right of the people to be secure in their person, houses, papers, and effects against unreasonable searches and seizures. That right is the same today as it was when it was written centuries ago, but the facts on the ground have obviously changed. Members of Congress didn't have cell phones in their pockets. We didn't have Zoom. We didn't email. The times have changed and while the concept to the right of privacy has not changed, new technologies make it a lot harder to rein in government intrusion in the lives of the people.

Artificial intelligence turbo charges surveillance capabilities by sifting through mountains of personal data in seconds, data brokers aggregate and re-identify so-called de-identified data blocked from apps and then sold to others, including the Government, allowing them real-time access to Americans' locations, purchasing habits, and healthcare needs. Cameras equipped with facial recognition technology can scan a crowd and instantaneously pick out specific people whether law enforcement targets or undocumented immigrants. You name it, all without a warrant.

In an 1829 speech at the Virginia Constitutional Convention, Madison said to his colleagues,

The essence of Government is power; and power, lodged as it must be in human hands, will ever be liable to abuse.

The U.S. Government has broad surveillance authorities. When properly implemented, they keep us safe from terrorists and foreign adversaries and gangs. Such broad grants of power are also fertile ground for abuse. I believe Congress has a duty to balance the Government's need for Americans' private data. With our rights, I have voted in favor of government surveillance authorities when they do not trespass on our constitutional rights, and I voted against them when they don't. We obviously need to keep ourselves

safe both from criminals and fraudsters who would do us harm, as well as those in power who would violate our freedom.

When we last reauthorized Section 702 of FISA which allows warrantless collection of the communications of non-U.S. persons located overseas, including when those people are interacting with Americans, our solution to that tension between privacy and security was to establish more checks on the Government. Congress previously imposed rules dictating when the FBI can search for Americans' identifying information in the 702 databases, but we know those rules had been honored only in the breach. Rather than review a sampling of those U.S. person searches, the FBI's National Security Division now must audit every search for the communications of an American. These watchdogs within the FBI and in other government agencies are an essential line of defense against government overreach. The problem today is that President Trump has fired all those people.

A week after he was sworn in, President Trump fired every democratic member of the Privacy and Civil Liberties Oversight Board. This is the board created by Congress in 2004 to make sure the Government does not violate Americans' civil liberties in the name of keeping us safe. The work of these Democratic Members have been lauded even by Republican Members of our Committee, who recognized and shared their commitment to protecting our rights against government overreach. Trump has left the Privacy and Civil Liberties Oversight Board with only one member, a single member who has been stripped of all authority because the board needs a quorum, which is three, to act. He cannot issue recommendations on Section 702, U.S. person searches. He cannot hold public meetings. Without the fired members, it is as though the board simply doesn't even exist. The President did not stop there. Remember those monthly audits of every single U.S. person searched of the 702 databases. He removed the individual responsible for managing that and rescinded offers extended to those who had been recruited to help her. Congress cannot receive the audit reports required by law because there is simply nobody left to audit these warrantless searches, much less provide the mandatory report to Congress which is why I am also concerned all the other things that have been done to remove the safeguards around Americans' right to privacy against government invasion. The President fired at least 17 Inspectors General, dismantled the Cyber Safety Review Board, and removed the Director of the NSA, the person in charge of collecting 702 data responsibly and within statutory limitations.

Just last week, he fired their four-star general in charge of the NSA and U.S. Cyber Command with other high ranking security officials because according to reports, Laura Loomer told him to do that. In a system that works, surveillance and privacy are inextricably tied and made consistent. Those conducting surveillance understand the threat posed to the country and its civil liberties and that is applied to rules in a precise and disciplined way. Franklin famously said that,

Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety.

While Trump has defied even Ben Franklin because in 78 days, we have lost both privacy and safety. We are less safe, and we are less free than we were on January 19, 2025. President Trump knows he is placed in charge of the FBI, like Kash Patel talked about using the power of the Government to visit retribution on anyone the President sees as an enemy.

Over the last 78 days, we have watched the administration attack journalists, the free press, colleges, peaceful protesters, Members of Congress, lawyers and law firms, and even the Federal judges because they have countered his assault on the rights and freedoms of the people. Never have I felt more concerned about the extremely broad warrantless surveillance powers that have been entrusted to the Executive Branch.

Chair Jordan and I have disagreed about various things in the past, but I must say he has shown commendable and strong leadership and worked across the aisle to ensure that Republicans and Democrats alike understand the dangers of unchecked government surveillance and the times bear him out. I am looking forward to working with him closely on a bipartisan basis in this set of hearings and the lead up to the expiration of FISA Section 702 next year to stand up for all Americans' civil liberties. I thank him for his leadership. I thank you, Mr. Chair, and I yield back.

Mr. BIGGS. The gentleman yields back. The Chair recognizes the Chair of the Full Committee, Mr. Jordan, for his opening statement.

Mr. JORDAN. Thank you, Mr. Chair. Section 702 of the Foreign Intelligence Surveillance Act allows Government to conduct surveillance of foreigners, as the title would suggest, outside of the United States for intelligence information. OK, that is all well and good. We like that. They get that information. They bring in this giant database, what I call the haystack of information, and then they do queries which is a fancy word for search and they search Americans, American phone numbers, names, email addresses, and they search Americans. They call it queries, but a query is a fancy name for search.

Three million times they did it in 2021. Here is the kicker. The FBI, when they did all these searches, didn't even follow their own rules. You don't have to take our word for it. The Inspector General said 278,000 times, the FBI didn't even follow their rules for conducting these searches on Americans, not foreigners. The Ranking Member is right. We have got 12 months from now when we get a chance to go to this issue again. We were close last time. We lost the warrant requirement in a vote 212–212. I am going to do everything, and I know the Chair is and I appreciate the Ranking Member's comments. We are going to do everything we can to make sure we have that warrant requirement.

Here is the way it works in our country. You are an American citizen, and the Government wants to go look at your stuff. They have got to go to a separate equal branch of Government and get a warrant. It is pretty simple. That is what we want. Plain and simple and we were one vote away from passing it in the House. Who knows what would have happened in the Senate, but I know I am committed. I know the Chair of the Subcommittee is committed and the Ranking Member, I appreciate what he has done

over the years in defending the Constitution, the Bill of Rights, and we look forward to working with him on this issue.

We need to do this to protect American citizens and as the Ranking Member said, “The way it has always worked, if you want to look at someone’s stuff, go get a warrant.” Go to a separate branch of Government, get a warrant. That is how probable cause—and here is the other thing. We even put exceptions in there, exigent circumstances, something really bad is going to happen or you give permission because there is some cyber-attack on you or your company. We put exceptions in there. We will put them back in again. Sometimes I thought we made too many exceptions. We will do it again. We have got to win. We have got to win this issue 12 months from now, April—I forget the date in April, but it is April of next year and we have got to make sure we win this, and I appreciate the Chair bringing our witnesses here. Thank you for coming and having this hearing on this very important—a fundamental issue for the American people. I yield back.

Mr. BIGGS. The gentleman yields back. Without objection, all other opening statements will be included in the record. We will now introduce today’s witnesses.

First, Mr. James Czerniawski. Mr. Czerniawski is a Senior Policy Analyst at Americans for Prosperity where he focuses on issues surrounding technology and innovation. Prior to joining AFP, he was a technology and innovation policy analyst at the Libertas Institute.

Mr. Philip Kiko is a Principal at Williams & Jenson, PLLC. He is a former Chief Administrative Officer in the House of Representatives. He has signed everybody here’s checks at some point or other and has served on a number of positions with Members of Congress and the Committees including the Judiciary Committee. He also served in the Executive Branch at the Interior Department and the Department of Education.

Mr. Gene Scaerr is a partner at Scaerr Jaffey LLP and serves as the General Counsel at the Project for Privacy and Surveillance Accountability. The Project for Privacy and Surveillance Accountability advocates for greater protection for Americans’ privacy rights and civil liberties in government surveillance programs.

Mr. Kia Hamadanchy, did I hit it?

Mr. HAMADANCHY. Hamadanchy.

Mr. BIGGS. Hamadanchy. OK. Very good. Mr. Hamadanchy is a Senior Policy Counsel to the ACLU where he focuses on civil liberties, among other issues. He previously served as a House and Senate staffer.

We welcome each of our witnesses and thank you for appearing today. We will begin by swearing you in. Would you please rise, and raise your right hand?

Do you each of 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 the witnesses have answered in the affirmative. Thank you, you may be seated.

Your written testimony will be entered into the record in its entirety. Accordingly, we ask that you summarize your testimony in

five minutes. We are going to go first to you, Mr. Czerniaski, and you may begin for your five minutes.

STATEMENT OF JAMES CZERNIAWSKI

Mr. CZERNIAWSKI. Thank you, Mr. Chair, Ranking Member Raskin, and the Full Chair of the Committee, Mr. Jordan, for holding this important hearing here today. This is an incredibly important topic, Government surveillance of U.S. citizens. This matter isn't just a question of policy or politics. It is a matter of principle. 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 under the guise of national security.

I do not believe that many would deny the importance of national security. Many, including myself, recognize that the world is a dangerous place and that there are people in this world that would seek to do harm to our great Nation and its people. I would know this firsthand growing up in Queens, New York, and experiencing the terrible events and aftermath of 9/11, a solemn day in American history that I will never forget. It was also a day that served as a catalyst for pushing our Nation down this path of increased surveillance.

However, while national security is important, it cannot and must not come at the expense of the very freedoms that define us. Looking back at history sends a stark warning of all the dangers in allowing an unchecked government too much power. Oftentimes, unfortunately, we know all too well that granting such powers to the Government can result in outcomes where that very power gets leveraged against the very people it was meant to protect.

Time and time again, we have caught the intelligence community with their hand in the constitutional cookie jar, if you will, as they use their spy powers to surveil Americans and when questioned on their wrongdoing and what they are going to do to fix it, the agency, rather than taking the moment seriously and implementing significant changes, puts out platitudes and promises that it will never happen again, until it does.

One might take from this exercise that the agencies are seemingly more concerned with the notion of managing bad headlines than they are with the sanctity of Americans' privacy and constitutional protections against overreach and tyranny. This repeated cycle of violations of Americans' rights, coupled with the lack of serious accountability, has led to a significant decline in public trust in the very institutions charged with keep them safe.

In December 2024, *CNN's* Harry Enten was on air covering recent Gallup polling that found that support for the FBI, in particular, was at an all-time low with just 41 percent of respondents thinking that the FBI is doing either an excellent or great job, representing an 18 percent drop in favorability in just 10 years. That is a damning indictment against one of the key agencies responsible for keeping Americans safe.

When it comes to the question of what can be done to address this issue, particularly when it comes to FISA, there are a litany of great ideas floating out there, but here are three key ones I would like to highlight for you here today: (1) Closing the back door

search loophole; (2) closing the data broker loophole; and (3) strengthening third-party oversight at the FISA Court.

The key reforms I just highlighted here today will not end any surveillance that is going on right now or prevent those authorities from being utilized to ensure our national security. What they will do is ensure that the rights of Americans are not trampled on in the process of carrying out those duties. This is not a moment for complacency. This is a moment for action. We must reaffirm our commitment to the values that make our Nation exceptional. We must demand policies that protect our privacy, uphold our liberty, and preserve the Constitution as the cornerstone of our democracy. As Members of the Committee with primary jurisdiction, you are in the position to shape policies that properly balance security with liberty and to safeguard the very founding principles that make our Nation worth protecting.

Thank you for the opportunity to share our thoughts with you today. I look forward to the conversation and answering any questions you may have.

[The prepared statement of Mr. Czerniawski follows:]



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

James Czerniawski, Senior Policy Analyst: Technology and Innovation, Americans for Prosperity

Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary

U.S. House of Representatives

April 8th, 2025

Dear Chair Biggs, Ranking Member McBath, and Members of the Subcommittee

On behalf of Americans for Prosperity and the millions of activists it represents across all 50 states, we thank you for the opportunity to provide our view on the increasingly problematic and invasive nature of government surveillance of U.S. citizens. In a nation founded on the principles of liberty and limited government, the ever-growing surveillance state is one of the greatest threats to individual freedom. Under the guise of national security, the federal government has overstepped its constitutional limits in empowering and emboldening a national security apparatus that has engaged in warrantless surveillance of Americans with little to no accountability. What began as a program meant for counterterrorism has morphed into a surveillance apparatus that erodes privacy, chills free speech, and undermines faith in key institutions of government critical to protecting Americans.

The revelations of years of numerous documented abuses coupled with a lack of accountability has resulted in an erosion of trust between the American people and the key institutions within government charged with protecting them. At Americans for Prosperity, we believe that national security and constitutionally protected rights are not mutually exclusive. National security should not come at the expense of personal liberties. The intelligence community is bipartisan in its targeting of Americans for surveillance, and it is good to see that Congress is coming together in a bipartisan nature to tackle this critical issue. We hope this hearing can serve as an opportunity to find pathways towards securing bipartisan reforms that can both advance our national security interests and better protect Americans civil liberties.

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

Passed in 2008, Section 702 of the Foreign Surveillance Act granted the government greater powers to conduct warrantless surveillance of suspected foreign terrorists. While this may sound like a reasonable approach to national security, its implementation has often blurred the line between foreign and domestic surveillance. Unfortunately, Section 702 has become a go to

resource for the government to access Americans' communications without the proper protections of a warrant. For example, the Federal Bureau of Investigation (FBI) conducted 200,000 warrantless searches of the communications of American citizens in 2022 alone using the Section 702 data.¹

The FISA Court revealed how the government had improperly queried the database to spy on people present at the capitol on January 6th, 2021, information on Black Lives Matter protestors in the summer of 2020², 19,000 donors to a congressional campaign³, and targeted elected officials, including a sitting U.S. Senator.⁴ These incidents are far outside the scope of Section 702's intended use for foreigners outside of the United States and goes to the heart of the Fourth Amendment and our fundamental natural rights.

Unfortunately, rather than implement appropriate guardrails to ensure they are following the rules, intelligence agencies have failed to implement any meaningful reforms that place privacy at the forefront of policy discussions. Instead, agencies spent time and resources in 2023 issuing a report describing how they were changing their methodology in a way that would decrease the reported number of queries.⁵ Essentially, the agencies are seemingly more concerned with the optics of headlines than they are with the sanctity of Americans' privacy and Constitutional protections against 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 feel that would be a grave misstep. Back in 2020, Congress let Section 215 of the PATRIOT Act sunset as they could not come to consensus on which reforms to the program were necessary to keep it in place. An unintended consequence of this outcome was that it did not stop the intelligence agencies from engaging in this type of surveillance. Rather, they simply carried out similar activities under other surveillance authorities like Executive Order 12333, a worse outcome as it comes without the added transparency required under statute coupled with oversight from Congress.

During the most recent reauthorization debate surrounding Section 702, after granting a short-term extension of the authorities in December of 2023 by including it in the must-pass National

¹ Office of the Director of National Intelligence. Annual 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.

² 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/>.

³ Foreign Intelligence Surveillance Court. 2021 FISC Certification Opinion. 2021, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.

⁴ 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-data-senators-name-00107621.

⁵ https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf

Defense Authorization Act⁶, Congress ultimately reauthorized the surveillance authority under H.R. 7888, the Reforming Intelligence and Securing America Act (RISSA).⁷ Proponents of this “solution” argued that it contained meaningful reforms, however, we believe that legislation did little in the form of reforms while simultaneously dangerously expanding the scope of surveillance by changing the definition of what was considered an electronic communications service provider (ECSP).⁸

Those “reforms” largely codified internal guidelines from the FBI, and analysis from the Center for Democracy and Technology found that the FBI conducted an estimated 4,000 queries violating these very guidelines, further reinforcing how insufficient that standard is.⁹ While Senator Mark Warner committed to working with colleagues to narrow that definition to address this concern¹⁰, the most recent attempt to do so in the Intelligence Authorization Act was stripped out.¹¹

We believe that Congress made serious gains in understanding the necessity for reforms to this surveillance authority, and that this Congress is in a position to build off that momentum with the coming reauthorization of FISA in 2026 to secure serious and meaningful reforms to this program once and for all. While there are many avenues for reform, here are several key areas of reform that Congress should focus on that we would like to highlight, such as:

- **Closing the backdoor search loophole**

The backdoor search loophole allows for intelligence agencies like the CIA, FBI and NSA to tap into the 702 databases, which is meant to be used to target only non-U.S. persons located overseas, to search billions of international communications to ultimately find and review Americans’ phone calls, texts messages and emails. Engaging in such practices explicitly undermines the 4th Amendment rights of Americans. As mentioned earlier, these backdoor searches have been abused to spy on 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.”¹² During the reauthorization debates,

⁶ 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.

⁷ <https://www.cnn.com/2023/12/07/politics/ndaa-fisa-extension/index.html>

⁸ U.S. Congress. (2024). H.R. 7888 – Reforming Intelligence and Securing America Act. 118th Congress. Retrieved from <https://www.congress.gov/bills/118/congress/house-bills/7888/text>

⁹ Id.

¹⁰ 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/>.

¹¹ <https://www.congress.gov/118/crec/2024/04/18/170/68/CREC-2024-04-18-pt1-PgS2837.pdf>

¹² 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-approves-bill>

¹³ <https://demandprogresseducationfund.org/new-polling-as-mass-surveillance-debate-reaches-final-stages-in-congress-americans-demonstrate-overwhelming-support-for-increased-privacy-protections/>.

amendments were put forward that sought to strike a balance that would accommodate legitimate security needs, such as exigent circumstances, certain cybersecurity-related queries, and consent queries, where queries are performed merely for identification or aiding of potential victims. Such a warrant requirement wouldn't be necessary for searches of metadata, thus allowing the FBI the flexibility to determine whether U.S. persons are in contact with foreign targets.

- **Closing the Data Broker Loophole**

Congress should continue to push for reforms to prevent the government from being able to circumvent Americans' constitutional rights by purchasing their personal data from private actors without a warrant. The purchase of such information by the government creates an additional threat, as law enforcement can then use this data tied to Americans engaging in constitutionally protected activities and subject them to additional surveillance via other technologies. Coupled with the backdoor search loophole, these end runs around the Fourth Amendment naturally have a chilling effect on the free speech rights of millions of Americans as they would fear being subjected to unwarranted government spying. Similar to the backdoor search loophole, Americans strongly agree with this proposal. According to that same polling, 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."¹³ The Fourth Amendment is Not for Sale Act, which passed the house this past Congress, offers a real solution to tackling 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 processes as additional scenarios arise that threaten Americans' rights. Congress should consider requiring FISA Court judges to appoint amicus curiae to cases with "sensitive investigative matter" as long as the court doesn't find it to be inappropriate. For example, if the court feels that appointing an amicus could jeopardize an ongoing investigation or reveal sensitive methods, it can choose not to do so. 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 document and information related to the surveillance application. This would be a significant improvement to due process and increase civil liberties protections for Americans at the courts by ensuring that decisions about surveillance didn't happen entirely in secret without any counterarguments or checks. Congress considered this issue in the past, when the Senate voted to adopt the Lee-Leahy amendment with overwhelmingly strong bipartisan support with a vote of 77-19 to the USA Freedom Act. During the most recent FISA reauthorization debate, the Government Surveillance Reform Act included a section based on that very amendment.

¹³ *Id.*

It's important to note that key reforms such as these will not end any surveillance authorities or prevent them from being used to ensure national security, but they will play a critical role in ensuring that the rights of American citizens aren't trampled on in the process.

II. Government's use of Technology for Surveillance

The government is no stranger to utilizing technology to aid in its mission of public safety. Technology is an incredibly powerful tool in the hands of law enforcement, as it can aid with their duties surrounding crime prevention, investigation and response. However, without proper guardrails, they are ripe for abuse in ways that undermine the communities' trust in them, running directly against their public safety mission.

For example, Facial recognition is a powerful technology that in a commercial setting can provide some benefits for users, but in the hands of government presents some highly problematic questions.

While facial recognition technology is older than perhaps people may realize, dating back to the 1960s when Woodrow Bledsoe developed a semi-automated facial recognition system to analyze facial features within an image¹⁴, the technology itself has experienced rapid gains in recent years. While the technology is impressive, it's still imperfect and can needlessly place innocent people in the crosshairs of law enforcement. A federal study in 2019 showed that Asian and African American people were up to 100 times more likely to 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.¹⁵

At the state level, Robert Williams presents a case study of what happens when law enforcement becomes overly reliant on technology. In January of 2020, police in Detroit 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 in front of his family. Ultimately, the charges against Williams were dropped, but not before he had spent 30 hours in jail and had to make bail for a crime he didn't commit.¹⁶ 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

¹⁴ 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>.

¹⁵ 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/>

¹⁶ 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>.

its surveillance practices to help analysts sift through the vast amounts of intercepted communications.¹⁷

Predictive Policing, which uses machine learning algorithms, analyzes large datasets to predict where and when crimes are likely to occur. 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”.¹⁸ The program was so problematic that the county unsurprisingly got sued by the Institute for Justice, ultimately settling and admitting that the program had repeated constitutional violations.¹⁹

Congress should explore ways to ensure there are guardrails around law enforcement use by executive agencies and work with their state counterparts to ensure similar efforts are taken up there.

Lastly, recent revelations around the bankruptcy announcement for 23andMe present interesting questions about biometric privacy.²⁰ 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.²¹ The company has roughly 15 million customers around the globe.²² FTC Chair Andrew Ferguson understands some of the privacy concerns presented here, recently issuing a letter stating that the promises made by 23andMe must be kept by whomever ultimately purchases that information.²³ 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 subcommittee and the committee more broadly should potentially explore.

¹⁷ 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>

¹⁸ 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/>

¹⁹ 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/>.

²⁰ 23andMe. Questions Related to 23andMe’s Chapter 11 Filing. March 26, 2025. <https://customer.care.23andme.com/hc/en-us/articles/30805135934615-Questions-related-to-23andMe-s-Chapter-11-Filing>.

²¹ 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>

²² Id.

²³ 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

III. Conclusion

Keeping Americans safe is a laudable goal and one we strongly support. It is impossible to ignore that we live in a dangerous world and that there are powers that seek to do harm against the United States. We appreciate the work of the dedicated individuals at these agencies trying to protect us from those dangers. However, that mission of public safety can't come at any expense or without considering other tradeoffs. As we have repeatedly said, protecting our constitutional rights and national security are not mutually exclusive goals. We appreciate the work of this subcommittee and the Judiciary Committee as a whole in trying to pursue the critical and needed reforms to curb the pattern of continued surveillance of U.S. citizens. It builds upon the committee's admirable and uniquely bipartisan efforts to reform surveillance abuses last year, reflecting the overwhelming and bipartisan demand from the public for strong privacy protections from government predations, something we wish to see continue this Congress. We stand ready to work with you and look forward to answering any questions you may have.

Mr. BIGGS. Thank you for your testimony.

Mr. Hamadanchy, I recognize you now for your five minutes.

STATEMENT OF KIA HAMADANCHY

Mr. HAMADANCHY. Chair Biggs, and the Members of the Subcommittee, thank you for the opportunity to testify today on behalf of American Civil Liberties Union regarding the myriads of government surveillance programs that impact Americans of all backgrounds.

At the start of my testimony, I want to express the optimism and hope of the ACLU as the Subcommittee and this Congress can use the next 12 months to put into Federal statute not only long-overdue protections against the misuse of foreign surveillance authorities, but also protections for everyone across our country against the largely unaccountable surveillance State.

A little over a year from now, Section 702 of the Foreign Intelligence Surveillance Act is scheduled to expire. While Section 702 requires that surveillance must be targeted at foreigners overseas, large quantities of communications that Americans exchange with people abroad are also swept up and stored for future investigations. The FBI, NSA, and CIA then conduct searches of their Section 702 databases for the communications of Americans without having to demonstrate a probable cause as the Fourth Amendment would otherwise require.

Last year, Congress, reauthorized Section 702 for two years with the Reforming Intelligence and Securing America Act. While we await further reporting from the Intelligence Committee on the impact of its changes, there is one recent development since reauthorization I would like to note. In December, the District Court for the Eastern District of New York ruled in a criminal case that the warrantless searches that the FBI conducted under Section 702 violated the Fourth Amendment. This ruling is the first of its kind and one of the rare cases where criminal defendants have received notice of Section 702 surveillance. While Section 702 is of particular importance to this Subcommittee because it is an issue that Congress has no choice but what to address over the course of the next year, it is not the only form of government surveillance that raises concerns and I would like to briefly touch on a few related topics.

First, as this Subcommittee is familiar, in recent years we have seen the ever-growing practice of law enforcement and intelligence agencies circumventing constitutional protections by purchasing access to data that they would otherwise need a warrant to obtain. According to former Deputy Director of the CIA, Michael Morrel,

The information that is available commercially would kind of knock your socks off. If we collected it using traditional intelligence methods, you would keep it Top Secret Sensitive and you wouldn't put it in a database. You would keep it in a safe.

The only way to ensure that protections against Federal agencies circumventing the Fourth Amendment by purchasing such data is through legislation like the Fourth Amendment Is Not For Sale, which passed the House Judiciary Committee last Congress without a single no vote.

The second additional form of surveillance I would like to highlight is reverse warrants such as reverse location or geofence warrants and reverse key word warrants which allow law enforcement to secure information that implicates law numbers of people who are not suspected of any wrong doing. These broad, suspicionless dragnet searches are deeply problematic and are tantamount to the Revolutionary War Era general warrants that led our Nation's Founders to prohibit their use through the adoption of the Fourth Amendment. As the Fifth Circuit Court of Appeals recently held, the reverse location warrants are modern day general warrants and are unconstitutional under the Fourth Amendment.

The next issue I would like to highlight is cross-agency data linkages. On March 20th, President Trump issued Executive Order 14243 directing Federal agencies to facilitate the sharing and consolidation of agency records with the stated goal of combating waste and fraud. However, the broad and unregulated access to sensitive data not only breaches privacy, but risks the creation of a database that creates a single searchable profile of every American without transparency or clear, legal limits. Without robust privacy protections, this could risk the eventual creation of a vast and unaccountable surveillance State capable of tracking every citizen's activities, movements, and associations.

Finally, all these surveillance programs run the risk of being super charged by the rapid growth and use of artificial intelligence. This Subcommittee should undertake a comprehensive review of AI technologies used for surveillance under its jurisdiction and assess their impact on privacy and civil liberties. This Committee and this Congress have an unparalleled opportunity over the next 12 months to protect all Americans by fundamentally reforming Section 702 starting with imposing a warrant requirement.

We look forward to working with you and getting these long, overdue reforms to the President's desk by next April. At the same time, we strongly urge this Committee to also address the massive and growing privacy problems for Americans raised by the broader surveillance ecosystem.

[The prepared statement of Mr. Hamadanchy follows:]



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

For a Hearing on
“A Continued Pattern of Government Surveillance of U.S. Citizens”

Before the
United House of Representatives
House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

April 8, 2025

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

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

I. Section 702 of the Foreign Intelligence Surveillance Act

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

The FBI, NSA, and CIA then conducts searches of their Section 702 databases for the communications of Americans—without having to demonstrate probable cause, as the Fourth Amendment would otherwise require. The FBI conducted more than 57,000 of these warrantless searches, through what is known as the "backdoor search" loophole, in 2023 alone. A recent report from the Privacy and Civil Liberties Oversight Board (PCLOB) found very little justification as to the value for the close to 5 million U.S. person queries conducted by the FBI from 2019 to 2022.¹ The reality is that Section 702 has been abused under presidents from both political parties, and it has been used to unlawfully query the communications of individuals and groups across the political spectrum.

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

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

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

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

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

a. Unconstitutional Queries

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

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

² *United States v. Hasbajrami*, No. 11-cr-00623-LDH, slip op. (E.D.N.Y. Jan. 21, 2025).

³ *United States v. Hasbajrami*, No. 15-2684, slip op. (2d Cir. Dec. 18, 2019).

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

b. Failure to Provide Notice of Section 702 Surveillance

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

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

Given the details presented in the Politico article and Director Wray's speech, only one criminal prosecution appeared to fit FBI officials' description, based on the ACLU's review of federal criminal dockets around the country. The defendant in that case subsequently filed a motion to compel the government to provide notice of use of Section 702.⁶ After reviewing secret government submissions, the judge ruled that no notice was required because he was satisfied that the government would not use evidence gathered pursuant to Section 702.⁷

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

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

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

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

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

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

Indeed, based on the ACLU's review of public court dockets, DOJ does not appear to have provided any Section 702 notices whatsoever since 2018.⁹ This subcommittee should closely scrutinize why that is the case, and whether parallel construction is being used to evade this important protection.

c. Transparency and Oversight

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

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

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

II. Commercial data purchases by law enforcement and intelligence agencies

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

⁸ As confirmed by the PCLOB's 2023 report.

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

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

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

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

- Information from individuals’ visits to health clinics¹², as well as reproductive tracking applications installed on people’s phones,¹³ and
- Information regarding people’s race, ethnicity, gender, sexual orientation, income, and political and religious affiliations.¹⁴

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

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

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

¹⁰ Byron Tau, IRS Used Cell Phone Location Data to Try to Find Suspects, WALL ST. J. (Jun. 19, 2020) ([here](#)).

¹¹ Byron Tau, U.S. Spy Agencies Know Your Secrets. They Bought Them., WALL ST. J. (Mar. 8, 2024), ([here](#)).

¹² Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, VICE (May 3, 2022), ([here](#)).

¹³ Joseph Cox, Data Marketplace Selling Info About Who Uses Period Tracking Apps, VICE (May 17, 2022), ([here](#)).

¹⁴ Joseph Cox, How the U.S. Military Buys Location Data from Ordinary Apps, VICE (Nov. 16, 2020), ([here](#)).

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

III. Reverse Warrants

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

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

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

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

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

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

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

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

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

IV. Cross Agency Data Linkage

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

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

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

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

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

V. Increased use of Artificial Intelligence in Surveillance

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

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

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

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

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

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

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

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

a. Facial Recognition Technology

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

¹⁹ Nat'l Sec. Comm'n on A.I. (NSCAI), Final Report at 110 (2021) ([here](#)).

²⁰ National Security Agency/Central Security Service, Our Mission (visited July 1, 2024) ([here](#)).

²¹ Artificial Intelligence: Next Frontier is Cybersecurity, NSA.gov (July 23, 2021) ([here](#)); Jay Stanley, Will ChatGPT Revolutionize Surveillance?, ACLU (Apr. 19, 2023) ([here](#)); An Interview with Paul M. Nakasone, Joint Force Quarterly, 92 at 4 (Jan. 2019) ([here](#)); Justin Doubleday, NSA Working on New AI 'Roadmap' as Intel Agencies Grapple with Recent Advances, Federal News Network (July 14, 2023) ([here](#)); Matt Kapko, 3 Areas of Generative AI the NSA Is Watching in Cybersecurity, Cybersecurity Dive (May 1, 2023) ([here](#)); Carolyn Shapiro, The Intelligence Community Is Developing New Uses for AI, FedTech (Oct. 4, 2022) ([here](#)).

²² Nat'l Sec. Comm'n on A.I. (NSCAI), Final Report at 108–10, 143–45. (2021) ([here](#)).

²³ ACLU, Re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Executive Order 14074, Section 13(e)), (Jan. 19, 2024) ([here](#)). ACLU, Response to U.S. Commission on Civil Rights Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology (April 8, 2024) ([here](#)).

²⁴ More than 20 jurisdictions—including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont—have enacted legislation halting most or all law enforcement or government use of face recognition technology. Others, such as the states of Maine and Montana, have enacted significant restrictions on law enforcement use of the technology. And law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited use of Clearview AI, an FRT vendor that markets a particular privacy destroying system built on a database of tens of billions of non-consensually collected faceprints.

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

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

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

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

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

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

²⁸ *Id.* at 24, 56–57.

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

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

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

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

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

Highlights of the settlement include:

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

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

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

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

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

VI. Conclusion

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

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

Mr. BIGGS. Thank you.

The Chair now recognizes Mr. Kiko for his five minutes.

STATEMENT OF PHILIP G. KIKO

Mr. KIKO. Thank you, Chai Biggs and the distinguished Members of Congress, including Chair Jordan and Ranking Member Raskin.

As you know, the Judiciary Committee has a long, distinguished, and complicated history with terrorism laws. I discussed the history and other legislative efforts in the testimony I delivered two years ago as an addendum to my written statement. The overreach of government agencies and FISA and using FISA authorities is well documented and Inspector General reports, FISA Court opinions, and Congress' oversight work.

As a backdrop, one must contend with internet-enabled platforms that connect almost everyone to an extraordinary complex digital world which captures users' personnel data, records likes and dislikes, preferences, and creates a personality profile for every digital user some firms compile and sell this data to third parties. Users consent to such dissemination of their data by signing lengthy Byzantine terms of service agreements and there are passive ways that data is collected as well for facial recognition cameras to license plate readers that enable law enforcement to identify and investigate crime in the real world. The rise of AI makes all this more complicated. In a very real way, we live in a modern, albeit consensual surveillance State. What is needed is the continued bipartisan oversight by this body to rein in and protect the guarantees of the Fourth Amendment.

How do we do this? Well, one way is continued targeted legislative reforms that were accomplished in the previous Congress in H.R. 7888. Additionally, in an age where massive amounts of user data has been commercialized by data brokers, you should ask yourself, if the Government can obtain information from a company or a third-party data broker which ordinary would require a determination of probable cause from a detached magistrate or judge as the Fourth Amendment requires, and they obtain information by paying for it without that time honored legal process, that undermines a crucial safeguard of civil liberty. I would expect we can deal with that in the next reiteration of 702.

The legislative reforms are only half the battle. What is absolutely required here is continued vigorous targeted oversight by the Legislative Branch, not passing laws or oversight. Just as law enforcement is increasingly able to identify and interdict crime in real time, Congress' FISA oversight must also be in real time. What does that mean? Congress must insist on timely disclosure of information. Through no fault of their own, committees have received information in response to reporting requirements that are months and sometimes years old. This information is useless.

This after-the-fact approach can be problematic. The provisions of H.R. 7888 are a valuable step in solving this problem, but this would only work if Congress received timely access to the information. All this must happen promptly. Information must be shared promptly, and Congress must allow real-time access. I would also direct Members' attention to Section 18(b) of H.R. 7888, which re-

quires the Director of National Intelligence to commission a study on technological enhancements for the FBI to monitor compliance of the Bureau's 702 information systems in their real time.

Should Congress use AI to modernize FBI's compliance with FISA? Consider something like this in the next iteration of FISA. Why couldn't Congress be entitled to access of that information on an on-going or even rolling basis? AI would make that allowable. Of course, Congress must continue to include Sunset Provisions in the FISA reauthorization. The Sunset Provisions give Congress the leverage it needs to ensure compliance.

In short, the short leash must be on the Intelligence Committee, not Congress. I would also make a pitch because I believe that there are over a million people in the Executive Branch that have access to SCI clearances, and I just wonder how many people on the Judiciary Committee or how many people in Congress have access to those to do oversight and I would just make a pitch to increase those clearances.

In any event, I am not someone who is hostile to strong, national security laws or Federal enforcement. Congress should not repeal 702. However, it is Congress' constitutional duty as Congress' constitutional entity closer to the people, it must continue its vital and constitutional oversight. Thank you again for the opportunity to testify.

[The prepared statement of Mr. Kiko follows:]

**Statement for United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance
“A Continued Pattern of Government Surveillance of U.S. Citizens”
April 8, 2025**

Thank you, Chairman Biggs, Ranking Member McBath, and distinguished Members of this Subcommittee. I'm delighted to be back testifying before the Subcommittee, and hope my testimony is helpful as, once again, you grapple with the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act, or FISA.

As you know, the Judiciary Committee has a long, distinguished, and complicated history with this law. Since 9/11, this Committee has initiated legislation to give the executive branch the tools to enforce antiterrorism laws against the foreign terrorists that attacked us, while attempting to preserve Congress's ability to conduct vigorous oversight of the enforcement of the law. I served on the Judiciary Committee following the 9/11 attacks when Chairman Jim Sensenbrenner and Ranking Member John Conyers helped shepherd the PATRIOT Act through Congress. The goal was modernizing surveillance for critical intelligence priorities, while ensuring the Executive Branch was operating within the bounds of the law and respecting American's cherished civil liberties. I discussed that history and other legislative efforts in the testimony I delivered to the Committee almost two years ago, which is attached as an addendum to this written statement

As a private citizen, I now have concerns about how these laws are being implemented, and that the government agencies implementing them have strayed away from what Congress originally intended. The errors and overreach of the intelligence community in using FISA authorities are well-documented in a series of publicly available Inspector General reports and FISA court opinions and have also come to light as a result of Congress's oversight work.

One must also contend with a rapidly changing environment, particularly as technology advances. Today, Internet-enabled platforms connect almost everyone to an extraordinarily complex digital world, which captures users' personal data, records "likes," preferences, and "dislikes," and creates a personality profile for every digital user. Some firms compile and sell this data to third parties.

Users, of course, often consent to such dissemination of their data when signing up to use these services. However, they often do so via lengthy, byzantine "terms of service" agreements, which they don't read in any meaningful way and would take several lawyers to decipher.

And there are passive ways that data is collected as well - from facial recognition cameras to license plate readers - that enable law enforcement to identify and investigate crime in real time. The rise of artificial intelligence only promises to make all of this more complicated and penetrating.

So, in a very real way, what our society has is a MODERN, ALBEIT CONSENSUAL, SURVEILLANCE STATE. Modern technology, including artificial intelligence, is amazing and has the potential to improve our lives in immeasurable ways. But it also has the potential for significant abuse. It is Congress's obligation to examine these authorities, the Executive's use of the authorities, and to ensure the authorities aren't being used in unforeseen, unintended ways that harm our civil liberties and violate the constitution.

What is needed, Members of this Subcommittee, is a renewed, bipartisan oversight effort by this body, to rein in abuse and protect Americans' expectations of privacy. It is in that spirit that I come before you today.

How do we do this? Well, one way is through targeted legislative reforms some of which were accomplished over the last several decades, and most recently in last Congress's FISA reauthorization. Bipartisan reforms like those in the recently enacted H.R. 7888, the Reforming Intelligence and Securing America Act (RISAA), are good and welcome. For example, requiring audits of all U.S. person queries and targeting procedures will help ensure Americans aren't targeted by a law that is explicitly aimed at "non-U.S. persons reasonably perceived to be located outside of the United States." Reforming Foreign Intelligence Surveillance Court (FISC) procedures as in Section 5 of RISAA, and requiring that exculpatory information be included in FISA applications, are positive. And these were not the only needed provisions that were enacted into law. Fortunately, there were many more.

Additionally, in an age where massive amounts of user data have been commercialized by data brokers, you should ask yourselves: If the government can obtain information from a company, or a third party data broker, which would ordinarily require a determination of probable cause from a detached magistrate, as the Fourth Amendment requires, does obtaining information by paying for it, without that time-honored legal process, undermine a crucial constitutional safeguard and civil liberty? I would submit that it does.

Last Congress, this Committee approved and the House passed H.R. 4639, the Fourth Amendment is Not for Sale Act. I would encourage you to do so again.

But legislative reforms are only half the battle. What is also absolutely required here is vigorous, targeted oversight by the legislative branch. And just as law enforcement is increasingly able to identify and interdict crime in real time, Congress's FISA oversight must also be in real time.

What does that mean? It means that the disclosure of the information I described above must be timely. Congress must insist it is timely. For too long, our Congressional Committees have received information, in response to reporting requirements, that is months, or even years, old in addition to being poorly organized and in many instances incomplete. I worked in two cabinet departments and know firsthand what it means to receive a “Congressional Oversight” letter.

The last time I appeared before this committee, I talked about how this “after-the-fact” approach was problematic. It remains so today. The numerous legislative reform provisions, in H.R. 7888 including the reporting and transparency measures are a valuable first step in solving this problem, but this will only work if through its oversight responsibilities Congress receives access to information in a timely manner. Make sure all these reforms are implemented promptly and within the next year prior to reauthorization. Congress must be allowed real-time access to this information to the greatest extent possible to ensure proper analysis and implementation by the agency is occurring.

Congress has the ability to receive, secure, and hold classified information. Every Member of Congress, under the U.S. Constitution and federal law (50 U.S.C. 3163), has access to classified material. However, the number of Congressional staff who hold TS/SCI clearances is very low, especially compared to the number of Executive branch employees who hold clearances. Do you know how many Judiciary Committee staffers hold a clearance today? I suspect it’s fewer than you think. Congress should consider amending its rules to increase the number of qualified staff with clearances for classified material and briefings.

I would also direct Members’ attention to section 18(b) of H.R. 7888, which requires the Director of National Intelligence to commission a study on technological enhancements that would enable the FBI to monitor compliance of the Bureau’s 702 information systems in near-real time. Could

we use Artificial Intelligence to monitor, in near-real time, the FBI's compliance with FISA? If we could, why wouldn't Congress be entitled to that information on an ongoing or even rolling basis?

And of course, Congress must continue to include sunset provisions in FISA reauthorization. Without sunset provisions, we may never have learned about much of this abuse. Without sunset provisions, Congress will simply continue to cede its Constitutional, Article I, legislative and oversight authority to unelected entities within the Executive branch. FISA is up for reauthorization in another year. If it is reauthorized, I would suggest it be no longer than a two- or three-year period to ensure Congress can evaluate and update both the implementation and progress associated with its extension.

In conclusion: The short leash must be on the intelligence community, not on Congress.

Mr. Chairman, Ranking Member McBath, I am not someone who is hostile to strong national security laws or federal law enforcement. Congress should not repeal section 702. It is an important tool that provides vital intelligence on a range of foreign threats and has successfully foiled terrorist attacks. Congress should not neuter FISA—which was, of course, put in place in the 1970s to constrain the government's use of surveillance authorities against American citizens.

However, Congress, as the constitutional entity closest to the people, must reassert its vital and constitutional oversight role, to protect the people.

Thank you for the opportunity to testify.

**Statement for United States House of Representatives
Committee on the Judiciary
Fixing FISA, Part II
Philip G. Kiko
July 14, 2023**

Good morning. Thank you for the opportunity to appear and testify before the Committee.

Introduction

It is an honor for me to return to the Committee where I worked with former Chairman Jim Sensenbrenner as the Staff Director and General Counsel. My years working with the Judiciary Committee were one of the highlights of my professional career, and I will always be grateful to the Committee and all of its Members for the opportunity to serve you and the public.

The Critical Balance Between Protection of our National Security and Our Civil Liberties

At the outset, I want to underscore the importance of this hearing and the Committee's oversight and examination of the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA).¹ Historically, the Committee has played a central role in protecting our country and its citizens from foreign enemies – hostile governments, terrorists, and transnational criminal organizations. At every step, the Committee has carried out this responsibility with proper regard for protection of our constitutional rights and liberties.

I am proud of the work that former Chairman Sensenbrenner, and former Chairs Goodlatte, Smith, Conyers, and Nadler (currently Ranking Member), and other Members of the Committee, on both sides of the aisle, devoted to this weighty issue. Today's hearing is yet another example of the

¹ Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C. § 1801 (1978).

Committee's tradition of reviewing important issues with proper regard for the need to ensure the safety of all Americans while protecting against abuses that may threaten our cherished civil liberties. It speaks to the tension in areas of national security between Congress' constitutional authority to pass laws to define the government's role in this area of the law versus the inherent Executive authority in the sphere of national security.

We faced similar challenges in the aftermath of the horrible and tragic attack against our country on September 11, 2001, in which we lost hundreds of innocent Americans.

The Committee – and our country – then faced an important crossroads and today we face a similar one, where we must adhere to our Constitution and our fundamental civil liberties while taking appropriate steps to protect our nation's security.

The USA PATRIOT Act in the Aftermath of the 9-11 Attack

I want to take a moment to outline for the Committee the events leading to enactment of the original USA PATRIOT Act ("Patriot Act")², the difficult issues we faced, and the necessary protections that the Committee and Congress as a whole agreed to when we enacted the Patriot Act. In my view, this context will provide some important lessons learned that may be helpful for the Committee to weigh as it considers re-authorization of Section 702 of FISA.

In the days after 9-11, former Chairman Sensenbrenner, Ranking Member Conyers, Committee Members, and staff all knew that changes to our foreign intelligence and law enforcement systems had to be made to ensure that such an attack could never occur again. It was apparent that the 9-11 attack exposed serious deficiencies in our intelligence system for collecting and analyzing data to prevent our citizens from future terrorist attacks. We were united in our mission, and the need

² USA PATRIOT Act, Pub. L. 107-56, 115 Stat. 272 (2001).

for Congress to act quickly and effectively to ensure that our country was safe. At the same time, however, I want to emphasize that we carried out this mission with dedication, bipartisan commitment, and a strict adherence to ensuring that our shared and cherished civil liberties were protected. It was a simple equation in our view – we will protect the country, but we will not do so at the expense of our freedoms, and we will continue to be governed by constitutional principles.

Over the following weeks, former Chairman Sensenbrenner, Ranking Member Conyers, Committee Members, and staff worked tirelessly to get this done. The Bush Administration responded quickly, and the Justice Department and the intelligence community proposed important reforms to the FISA and other intelligence and law enforcement authorities. It should be noted the Financial Services Committee played an important role in updating money laundering provisions which became Title 3 of the Patriot Act, which has become an important tool in cutting off terrorist financing schemes. The Committee moved quickly, conducted hearings to examine the important issues, and engaged in a thoughtful and vigorous debate.

Chairman Sensenbrenner and Ranking Member Conyers directed the Committee's effort. We arrived at a critical point in the process –we all knew that these new and extraordinary changes to FISA and related authorities depended on the professionalism of the Federal Bureau of Investigation and the intelligence community to follow safeguards to protect against possible abuse that may threaten everyone's civil liberties – the right to privacy, protection against unreasonable intrusions from surveillance, and improper targeting of individuals for searches and seizures.

The Administration placed significant pressure on the Committee and Congress to quickly enact reforms that they characterized as critical to protect our country from future attacks. In fact, there were reports the Administration wanted a bill passed within a week. The public mood was one of resolve, revenge, fear, anger, and demand for protection of our country's security. We all agreed

that the expanded authorities set forth in the Patriot Act required everyone to “trust” the Department of Justice, the FBI, and the intelligence community to operate within the requirements of the law and the United States Constitution. Implicit within this was that the Executive Branch would develop an effective verification process to ensure that our civil liberties were protected.

It was at this juncture when the Committee raised the issue of including – and indeed, insisted on – sunset provisions that would require Congress to re-examine several of the key provisions in the Patriot Act in four (4) years. The Committee and the House rallied behind the sunset provisions because we all agreed that, if unchecked, the Patriot Act, as originally crafted, could easily undermine and threaten a number of our cherished civil liberties.

As it turned out over the following 20 years, the sunset provisions have become a critical mechanism for Congress to re-examine Patriot Act provisions, and to reassess law enforcement and the intelligence community’s performance, and the continued need for various authorities. In other words, we knew that the global threat and anti-terrorism requirements would evolve over time, and the sunset provisions were an important tool to ensure that the proper balance was struck between our national security needs and protecting our civil liberties.

And while the Members of the House Judiciary Committee agreed on the need for the sunset provisions, I wish I could tell you that everyone in the Administration and in the Senate agreed with us and that the provisions were simply added to the Patriot Act. But that is not how it happened.

Instead, House Leadership, Chairman Sensenbrenner and Ranking Member Conyers were subjected to extraordinary pressure and a torrent of calls – political, media generated, and public

opinion – to back down, to eliminate the sunset provisions and act quickly to protect our country from a future attack.

I can recall meetings with Leadership, our Senate counterparts, in addition to representatives from the White House, Justice, the intel community and others where Chairman Sensenbrenner stuck to the Committee’s position – we would enact the Patriot Act with extraordinary new authorizations for use by the Justice Department, the FBI and the intelligence community, but the House and the Judiciary Committee would insist on including the sunset provisions to ensure that our national security was protected without any threat or diminution to our civil liberties.

Eventually, as everyone knows, our position prevailed. The House Judiciary Committee reported out the Patriot Act unanimously with the sunset provisions. The Patriot Act passed the House by a vote of 357-66 and the Senate by a vote of 98-1.

The rest, as they say, is history. But we all stood together in a unified voice committed to one fundamental principle – protection of our national security had to be accomplished with proper regard for our constitutional protections. And, as it turns out, we were absolutely right to insist on sunset provisions as a means to ensure appropriate oversight, refinement of authorities, transparency, and continued assessment of DOJ, the FBI, and the intelligence community.

History’s Vindication: Protecting Our Country While Preserving Civil Liberties

Before addressing the current issue of re-authorization of Section 702, it is important to understand the origins of FISA, and the purpose that it serves as an important check on intelligence and law enforcement activities.

Following widespread wiretapping and surveillance abuses during the 1960s and 1970s,³ Congress enacted FISA as an important new mechanism to establish procedures and requirements for domestic electronic intercepts of foreign intelligence.⁴

FISA provides a statutory framework for government agencies to secure authorization to gather foreign intelligence by means of: (1) electronic surveillance; (2) physical searches; (3) pen registers and trap and trace devices; and (4) production of certain business records. In addition, FISA created two new Article III courts: the Foreign Intelligence Surveillance Court (FISC) and the appellate Foreign Intelligence Surveillance Court of Review (FISCR).⁵

The most significant reform to FISA, as I outlined above, was the enactment of the Patriot Act in 2001, which was passed to “provide enhanced investigative tools” to “assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities.” The Patriot Act included four-year sunset provisions applicable to 16 of its new authorities.⁶

³ S. Res. 21, 94th Cong (1975) (; 124 Cong. Rec. 34, 845 (1978); S. Rep. No. 94-755 (1976) (the Church Committee reports); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harvard J.L. & Public Policy 757 (2014) (discussing the history leading to heightened protections afforded to domestic collection of U.S. citizens’ information).

⁴ FISA’s definition of “foreign intelligence information” was modified by the Patriot Act to mean information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. 50 U.S.C. §3003(2). Congress initially restricted FISA to regulate use of electronic surveillance, but subsequently amended FISA to regulate other practices such as physical searches, the use of trap-and-trace and pen registers, and production of certain types of business records. See Laura K. Donohue, *The Evolution and Jurisprudence of The Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review*, 12 Harv. Nat’l Sec. J. (2021), available at <https://harvardnsj.org/2021/06/28/the-evolution-and-jurisprudence-of-the-foreign-intelligence-surveillance-court-and-foreign-intelligence-surveillance-court-of-review/>.

⁵ 50 U.S.C.A. § 1803(a)–(b).

⁶ In 2020, three FISA provisions expired under applicable sunsets: Section 206 “roving wiretaps”; Section 215 “business records”; and the “lone wolf” provision. See Edward C. Liu, CRS, *Foreign Intelligence Surveillance Act: An Overview*, at 1 (2021), available at <https://sgp.fas.org/crs/intel/IF11451.pdf>.

In 2008, Congress enacted the FISA Amendments Act and codified Title VII (including Section 702), which created procedures to collect foreign intelligence when communications travel through the United States' communications infrastructure.⁷ Under Section 702, the government may compel electronic communications service providers for a period of up to one year to assist in targeting non-U.S. persons reasonably believed to be located outside the United States. The Attorney General and the Director of National Intelligence (DNI) must jointly certify that they authorize any such targeting, and the FISC must approve any program under Section 702 before its implementation.

In 2013, the foreign intelligence world was rocked by Edward Snowden's disclosure of documents that revealed that the National Security Agency (NSA) was engaged in the bulk collection of telephone metadata under Section 215 of FISA. The Snowden leaks revealed that the NSA was over-collecting upstream Section 702 data, monitoring U.S. citizens' email and text communications in and out of the country, and conducting a variety of warrantless searches to build profiles of individuals. Snowden's revelations led to a public backlash and explosion in litigation before the FISC amid controversies relating to NSA abuses involving unauthorized collection of metadata, including calls and electronic communications occurring entirely within the United States.⁸

⁷ The FAA included important statutory and procedural protections regarding surveillance of U.S. persons located outside the United States. Congress reauthorized Title VII in early 2018 and included a five-year sunset, expiring in 2023. *See Id.* at 1-2.

⁸ Press reports cited the fact that the NSA was using "back-door" techniques to access data from U.S. Internet companies. For example, over a 30-day period, approximately 97 billion internet data records and 124 telephone data records had been collected. Inside the U.S., approximately 3 billion data elements were collected over a 30-day period in 2013 concerning U.S. citizen activity. *See Donahue, supra* at 21-22.

In response to this controversy, former Chairman Sensenbrenner, Ranking Member Conyers and Senate Judiciary Chairman Leahy proposed and eventually secured passage of the USA Freedom Act,⁹ which prohibited bulk collection under Section 215, FISA pen register/trap and trace authorities, and National Security Letters. The Act also required the appointment of at least five *amici* to appear before the FISC to address novel questions of law, and required a number of reports related to the operation of FISA authorities.

The Need to Reform Section 702

As I noted above, the Committee now stands at another important crossroads – the issues we face involve a delicate balance between two critical needs – we have to protect our country from foreign enemies and Section 702 is a critical tool for accomplishing that purpose. On the other side, however, Congress must enact real and meaningful reform to protect Americans’ civil liberties.

Since the leak of the Snowden documents and the public disclosure of abuses that resulted in the passage of the USA Freedom Act reforms, the country continues to witness escalating and serious concerns surrounding law enforcement and intelligence community misconduct and failures to comply with checks needed to protect our civil liberties.

Needless to say, the Department of Justice, law enforcement and the intelligence community’s record of compliance failures has been amply documented, cited and disclosed by various credible

⁹ *USA Freedom Act*, Pub. L. No. 114-23, 129 Stat. 268 (2015).

parties, including: (1) the FISC itself;¹⁰ (2) the Department of Justice's Inspector General;¹¹ and (3) this Committee's own oversight and investigative record.¹² The record of DOJ, the FBI and intelligence community is disturbing and cannot be ignored.

In its April 21, 2022, *Memorandum Opinion and Order*, the FISC cited numerous instances of noncompliance, misrepresentations, and unlawful access (over 278,000 times) to data collected pursuant to Section 702 over a multi-year period. The FISC's citation of violations and abuse of querying of Section 702-collected data is described in detail at pages 28 to 34 of its *Memorandum Opinion and Order*.

Similarly, the DOJ Inspector General has demonstrated the difficulties faced by the Department of Justice and the FBI in maintaining a proper balance between protecting national security and

¹⁰ See Document re: Section 702 2021 Certification, FISA Ct., April 21, 2022, (*Memorandum Opinion and Order*) available at: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf; see also, Donahue, *supra* at 54-71.

¹¹ See U.S. Dep't of Justice, Off. of Inspector Gen., *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (2019), available at <https://www.justice.gov/storage/120919-examination.pdf>; U.S. Dep't of Justice, Off. of Inspector Gen., *Audit of the Federal Bureau of Investigation's Execution of its Wood Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (2021), available at <https://oig.justice.gov/sites/default/files/reports/21-129.pdf> (Non-compliance identified in all 29 FISA applications reviewed by the OIG. DOJ later discovered 209 errors in those applications, 4 of which DOJ deemed material. Further audit work identified over 200 additional instances of Woods Procedures noncompliance—where Woods Files did not contain adequate supporting documentation for statements in the 29 applications); and U.S. Dep't of Justice, Off. of Inspector Gen., *Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters* (2022), available at <https://oig.justice.gov/sites/default/files/reports/22-116.pdf> (DOJ's National Security Division (NSD) and FBI's Office of General Counsel (OGC) had differing interpretations of the query standard under the FBI's Section 702 Querying Procedures, which resulted in numerous compliance incidents and disputes between the FBI's OGC and DOJ's NSD attorneys).

¹² *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them*: Hearing Before the Subcomm. on Crime and Government Surveillance, 116 Cong. (2019), available at <https://www.govinfo.gov/content/pkg/CHRG-116hhrg44884/html/CHRG-116hhrg44884.htm>.

safeguarding civil liberties.¹³ In particular, DOJ's Inspector General testified before this Committee and highlighted three important issues in light of the Committee's consideration of re-authorization of Section 702: (1) the need for effective supervisory review that occurs in real time and can prevent compliance errors from occurring; (2) the need for effective, routine, and regular internal oversight to identify and correct any errors or program weaknesses close in time to their occurrence; and (3) the role of the OIG and other independent oversight entities in conducting periodic, big picture external reviews.¹⁴

In this context, the FISA world of foreign intelligence has changed significantly since 2001 and the aftermath of 9-11. Over the last 20 years, Congress at one point or another has faced the difficult question of whether to re-authorize powerful foreign intelligence authorizations against the backdrop of a disturbing record of non-compliance. We have seen this before.

Without belaboring this point or rehashing the evidence over the last 20 years, suffice it to say, the Committee needs to implement meaningful reforms to prevent potential problems before they occur. All too often, the Committee and the public have learned about compliance failures after the fact, and then relied on law enforcement and the intelligence community to institute remedial solutions. This "after-the-fact" approach is not sustainable, and a new proactive approach is needed. Specifically, I would urge the Committee to examine proactive solutions that mandate procedural and substantive reforms to the internal processes and procedures used by law enforcement and the intelligence community, which would be subject to oversight in real time and

¹³ See *Id.* (Statement of Michael E. Horowitz, Appendix *Prior OIG Reports on FISA and National Security Authorities*), available at <https://oig.justice.gov/sites/default/files/2023-04/4-27-2023.pdf>

¹⁴ See *Id.* (Statement of Michael E. Horowitz).

not on a yearly or more basis after the damage has been done. We can no longer rely on DOJ's, the FBI's, and intelligence community's promises of reform to existing procedures and processes.

A new solution must be found, and the Committee must find a way forward to continue Section 702 collection while implementing real and significant reforms to protect our constitutional rights. Just like our original mission in 2001 in the aftermath of the attack against our country, the basic principles remain the same: we must protect our country from future terrorist attacks, and we must do so without harming our civil liberties.

There is no doubt that Section 702 has been a valuable tool and we should be careful about allowing it to expire. FISA was created in 1978 as a restraint against government and as a protection to Americans, however it is clear it needs to be updated. I would urge the Committee to undertake serious reforms, beyond those we have ever considered or enacted before, to ensure that the FBI and the intelligence community will not be permitted to threaten our fundamental civil liberties.

The Committee has before it a difficult task that requires a delicate balancing act. There are some who advocate that Congress should let Section 702 authority expire; and there are others who argue that if 702 is allowed to expire, the Executive branch will fall back on its inherent authority in the national security arena and executive orders and would probably be happy to do so without the pesky interference of Congressional oversight. If Section 702 is re-authorized, implementation of proactive monitoring programs, real and significant changes to law enforcement and intelligence community processes, and an increase of overall transparency of this powerful tool could serve as important checks. There must be consequences for abusing FISA as a deterrent to bad behavior.

We need to put teeth in FISA, so people think twice about doing inappropriate things. The trust can be rebuilt, but only if there is more accountability by the intelligence and law enforcement community. Congress and the FISC can exercise appropriate oversight and protection of our cherished liberties while ensuring the protection of our safety from foreign enemies. In the past, beginning with the creation of FISA, Congress has had to be reactive; now there is an opportunity to be proactive.

Apart from Section 702, it needs to be noted there has been a constant chipping away at the protections of the 4th Amendment. Data brokers regularly sell large quantities of personal data about United States citizens to law enforcement agencies and do so without notifying any United States citizen that such practice is occurring. Further, warrantless access is given to all kinds of information without any knowledge of the person who submitted it. Why is this data not protected? I am sure the individuals affected did not expect their data to be sold and accessed without their knowledge. The constant chipping away of 4th Amendment protections needs to be addressed.

When Chairman Sensenbrenner and I visited the horrific scene of the Twin Towers days after the 9-11 attack, we both knew at that time that our country's future would depend on our work with everyone in Congress, the Executive Branch, law enforcement, and the intelligence community to make sure the words "Never Again" would become a reality. I am convinced that today we can reaffirm this solemn promise to the American people by reforming FISA and by taking a broader look at how data is gathered on Americans without their knowledge by law enforcement agencies. Protections need to be, and should be, reviewed by Congress and addressed.

Mr. BIGGS. Thank you.

The Chair is not recognizes, Mr. Schaerr for your five minutes.

STATEMENT OF GENE SCHAERR

Mr. SCHAERR. Thank you, Chair Biggs. Thank you, Chair Biggs, Ranking Member Raskin, my own Congressman, and Chair Jordan, and the other Members of the Subcommittee.

I commend my fellow panelists for their insights and their hard work on the issues that we're discussing today.

I served as Chair and General Counsel to the nonpartisan, proprivacy organization called the Project for Privacy and Surveillance Accountability, which is blessed to have your former Chair, Bob Goodlatte, as our Senior Advisor.

Over the last 25 years, the administrations of both parties, our Nation has seen an expansion of privacy-destroying technologies and practices—key elements of a panopticon-style surveillance State coming together before our eyes.

One such element, of course, is FISA Section 702, mentioned repeatedly previously, in which the NSA's global trawl routinely catches the communication of innocent Americans. That program, of course, was the subject of the Reforming Intelligence and Securing America Act, RISAA, which passed the Congress last year and some have falsely claimed closed Section 702's loopholes. As useful as RISAA was, it left important work undone.

To see why, recall that RISAA primarily codified 702-related rules and procedures that the FBI itself adopted by early 2022, but the FBI failed, even by its own standards, when it conducted 204,000 warrantless searches for Americans' communications later in 2022. A DOJ audit recorded a noncompliance rate—that is, a noncompliance with the procedures rate—of at least 3,400 civil rights violations a year, almost 10 per day. Those included warrantless surveillance of a U.S. Senator, a State Senator, and a State judge.

Since RISAA's passage in April 2024, the Director of National Intelligence has revealed additional improper searches, including the communications of a congressional candidate, a congressional Chief of Staff, numerous Federal employees, and even the spouse of an applicant for a security clearance.

Beyond 702, routine searches of sensitive data purchased from data brokers are at least as serious a threat to privacy, but is currently shrouded in even greater secrecy than 702 searches. As abuses continue, the legal foundation for the FBI's warrantless searches under both of those programs is collapsing.

As Mr. Hamadanchy noted earlier, in December, building on a landmark Second Circuit ruling that held that a search of the Section 702 database constitutes a search for Fourth Amendment purposes, a Federal District Court ruled that the government had violated the Fourth Amendment when it failed to obtain a warrant before conducting such a backdoor search of the 702 databases.

Absent an explicit warrant requirement written into statute for searching both 702 data and purchased data, we can expect that such abuses will continue. Unfortunately, in the last Congress, this Committee demonstrated that it's possible to erect useful guardrails to protect Americans' civil rights against such abuses.

There's wide bipartisan support for reform, and although the two warrant requirements that we discussed earlier for 702 data and for purchased data ultimately did not become law, advancing them as far as you did was a tremendous legislative accomplishment.

With a YouGov poll showing that at least 70 percent of Americans support these kinds of warrant requirements, you can now move forward with confidence. Yes, you can expect whispered opposition from some elements of the intelligence community or the IC, but your proposals last year, as Chair Jordan mentioned, already answered their main objections.

An additional objection that we've heard frequently is that the IC will sometimes claim that a warrant requirement would require an additional army of FBI attorneys and FISA judges, but again, your proposals have a ready answer to that.

Using the FBI's own numbers, spelled out in the exhibit that's attached to my written testimony, the Bureau would, at most, have to handle an average of three additional queries per day requiring a warrant. That's not an overwhelming burden, as former prosecutors like Mr. Knott can confirm. It's a small price to pay for increasing public confidence in the entire FISA system, not to mention complying with the Fourth Amendment.

In short, this Committee has already proven that you can protect both the constitutional rights of your constituents and keep them safe. We urge the Committee to uphold the Constitution by, once again, boldly advancing, and then, persuading your colleagues to adopt these two important warrant requirements.

I thank you again for the opportunity to testify and look forward to your questions.

[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
Subcommittee on Crime and Federal Government Surveillance
Hearing on:
“A Continued Pattern of Government Surveillance of U.S. Citizens”**

April 8, 2025

Chairman Jordan, Ranking Member Raskin, Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee, I thank you for examining the massive growth of government surveillance of Americans, and what can be done about it.

The Problem

We have seen under administrations of both parties the expansion of myriad forms of privacy-destroying technologies and practices—elements of an emerging American surveillance state being knitted together before our eyes.

Like the proverbial frog unaware that it is slowly being boiled alive, Americans are being progressively trapped in a system of national surveillance. This is not happening because federal agencies are run by tyrants. The men and women in the intelligence community are passionate about their mission to protect the American people and our homeland. But in their zeal to execute their important mission, they are rapidly creating the elements of a pervasive American surveillance state. And astonishingly fast changes in technology are helping build this surveillance state before our laws can catch up to keep it within the constraints of our Constitution.

At airports, at malls, on the streets, we are identified and tracked by our faces. Cellsite simulators in geofenced areas ping our phones to follow our movements. Our automobiles keep a record of every place we drive. Our digital devices at international terminals are subject to having all their contents downloaded and inspected without a warrant. Moreover, thanks to purchases of Americans' digital information from data brokers, federal agencies ranging from the FBI to the IRS, Department of Homeland Security, and the Department of Defense, routinely access, without a warrant, digital information far more personal than what can be gathered by hand or found in a diary. To top it off, we also face the routine collection of Americans' communications “incidentally” caught up in the global data trawl of programs authorized by Section 702, and in the past few years alone the FBI has conducted hundreds of thousands of warrantless searches of the Section 702 database specifically looking for Americans' communications.

The end result is that the government is now able to collect and search through vast amounts of Americans' communications and other personal data with ineffective statutory limits and limited congressional oversight. The personal data thus obtained reveals much about our health, mental health, and personal relations. Worse, all this

data generated from myriad sources can then be woven together by the instant 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.

This is as about as far from the Founders' vision of the Fourth Amendment as one can imagine. 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 a secret political document, but they couldn't access anything close to the wealth of private information contained 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. How does that principle apply today to surveillance reform?

The Importance of Warrants

Of course, there is a legitimate need in a dangerous world for the government, in some rare situations, to seize Americans' papers and other assets to search for threats to life and liberty. But the Founders recognized that this authority was in itself a great danger, perhaps one as great as any external threat. So they placed a boundary around this power with the Fourth Amendment's requirement for a warrant.

Warrants force government agents to justify their snooping with statements of probable cause. After the fact, warrants provide a paper trail that helps deter the government from invading Americans' privacy when there is no good reason to do so—that is, when there is no "probable cause" to believe any harm is being or is about to be inflicted on the Nation or one of its citizens. And that probable cause requirement should apply, not just to direct surveillance like tapping someone's phone or following them from place to place. It should also apply to more indirect forms of surveillance like searching a database of purchased information, or searching the massive trove of information compiled under Section 702 of FISA.

Yes, surveillance under Section 702 is in theory limited to foreigners' communications. But because Americans are often in communication 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. As the FBI admits, it sometimes conducts warrantless "backdoor searches" of those communications and other data in ordinary domestic criminal cases, and believes it has the right to do so routinely.

Further, according to several FISA Court opinions, the FBI frequently conducts those backdoor searches in politically sensitive cases. For example, in violation of its own rules, in just the last few years the FBI has searched for communications of Black Lives Matter and January 6 protesters, of 19,000 donors to a congressional campaign, of multiple U.S. government officials (including at least one member of this House), of journalists, political commentators, and a local political party, not to mention people who came to the FBI to perform repairs; victims who approached the FBI to report crimes; business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy"; college students participating in a "Collegiate Academy"; police officer candidates; and colleagues and relatives of FBI agents.

Defenders of the status quo will claim that last year's passage of the Reforming Intelligence and Securing America Act (RISAA) in April 2023 closed the loopholes that allowed such abuses. As useful as RISAA was, that is far from the truth. What Congress did there was mainly to strengthen oversight and codify 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.

But the FBI failed even by its own procedural standards when it conducted over 204,000 warrantless searches for Americans' communications in the FISA database in 2022. A DOJ National Security audit recorded a "noncompliance" rate of 1.7 to 4 percent for such queries for that year alone. Even at the low-end estimate, that failure rate equals about 3,400 civil rights violations a year according to the FBI's own standards, almost 10 violations per day. Not to mention that all 204,000 of those searches sidestepped the Fourth Amendment and invaded Americans' privacy without probable cause or a warrant.

Some of the most egregious improper queries also occurred after the FBI's new rules were implemented. Even then, the FBI managed to dip 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. Moreover, since the passage of RISAA in April 2024, the Office of the Director of National Intelligence has revealed further improper searches of the communications of a congressional candidate, a chief of staff of a Member of Congress, U.S. government employees, and the spouse of an applicant for a security clearance.

As abuses continue, the legal foundation for warrantless searches is collapsing. In December, a federal district court 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.¹ That decision was based on an earlier decision by the influential Second Circuit holding that a government search of the Section 702 database is in fact a "search" for Fourth Amendment purposes.

As we have seen repeatedly, however, a judicial ruling here or there has proven insufficient to deter warrantless searches. Absent an explicit law mandating a warrant

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

requirement, such abuses will inevitably continue. We should be very concerned about any framework that allows the FBI to routinely search through Americans' communications without a warrant.

The Road Ahead

So where do we go from here? In the last Congress, you proved on a strong bipartisan basis that we do not have to meekly accept this status quo. You demonstrated that it is possible to erect useful guardrails to protect Americans' civil rights against surveillance abuses, 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.
- You shortened the reauthorization of Section 702 from five to two years.
- And on the House floor, you came within one 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.

As you do so, moreover, you can rest assured that the American people are behind you. For example, a YouGov poll shows that 76 percent of Americans support a warrant requirement for government inspection of Americans' international communications. As the debate on the reauthorization of Section 702 begins, you can speak and act with confidence, knowing that your constituents are strongly on your side.

Resisting Intelligence Community Misinformation

That is not to say the road will be easy. Last Congress, reform proponents lost the warrant votes because the Intelligence Community (IC) whispered to Members that they would be held responsible for a parade of horrors if those measures passed. That was and is nonsense. You took great care to make sure the intelligence community would retain the authorities it needs to track and counter dangers from here and abroad.

Indeed, the Intelligence Community's own testimony offered only a few scenarios in which U.S. person queries—the warrantless searching of Americans' communications in the Section 702 database—had any value in significant cases. And your proposed warrant rule included reasonable exceptions that allow the government to act effectively in every exceptional circumstance. Let me detail some of the whisperings of the Intelligence Community and the sound policy responses this Committee included in your proposed warrant requirements.

- For example, the IC whispered to Members that a warrant requirement for Section 702 would leave the country wide open to cyberattacks. But your proposed warrant requirement made it clear: Queries focused on cyberthreat signatures were explicitly exempt and usually involve metadata queries, not content. Otherwise, any U.S. company or critical infrastructure target can simply consent to a query.
- The IC also whispered that a warrant requirement for Section 702 would curb the ability to foil foreign plots. You had an answer: Any American targeted for assassination or kidnapping in a foreign plot will obviously give grateful consent for a query designed to protect them.
- The IC further asserted that a warrant requirement would expose us to foreign spying. Your answer was that, because metadata queries are exempt, a warrant rule would not inhibit the government's ability to identify contacts. The government *has never shown one instance* in which queries of actual message *content*—as opposed to identifying metadata—were critical to an investigation of a foreign agent. Besides, isn't reading the private communications of American citizens exactly why the Constitution mandates a warrant?
- Then there was the IC's trump card: What about the scenario of a ticking time bomb? This is perhaps their most hackneyed charge—that we risk lives by allowing for due process and court approval. The fact is that, if such a time-sensitive emergency ever did occur, your warrant rule explicitly accounted for it by including an exception precisely for such exigent circumstances.
- Finally, the IC alleged that a warrant requirement would require an army of additional FBI attorneys and FISA judges. But such a phantom army would never be needed. Attached is an analysis the Project for Privacy and Surveillance Accountability developed together with the Center for Democracy and Technology. In it, we show that the Bureau would at most have to deal with an average of three queries per day requiring a warrant. That may require a very

modest increase in agency and judicial resources, but it's a small price to pay for ensuring Americans' privacy—and compliance with the Fourth Amendment.

The excessive numbers are, in fact, on the other side of the ledger. The Privacy and Civil Liberties Oversight Board (PCLOB) reports that the government has given “little justification” for the value of almost 5 million U.S. person queries conducted from 2019 to 2022. The government could report only a handful of instances in which these searches were useful. And in each of those cases, the government could have easily obtained a warrant or invoked one of your proposed exceptions.

Conclusion

In the face of this well-organized campaign against reform, this Committee has advanced and can continue to advance sensible bipartisan, well-reasoned and thoughtful reforms. In the face of a surveillance state growing at breakneck speed, this Committee has shown leadership and a sense of urgency that matches the moment. We don't have to supinely accept the erosion of all privacy. We don't have to trust that government agents and future administrations will always use these awesome powers solely for national security. These technologies simply offer too much power to trust that future guardians will not be tempted to misuse them, as they have done in the past.

In short, you have shown that you can protect both the constitutional rights of your constituents and also keep them safe from foreign and domestic threats. I urge you to uphold the Constitution by once again advancing—and persuading your fellow Members to adopt—a warrant requirement for both government-purchased data and data collected under Section 702.

Thank you for the opportunity to testify.

Gene Schaerr





Debunking Myths on the National Security Impact of Warrants for U.S. Person Queries

Warrantless queries of Americans' communications obtained via Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") are antagonistic to the basic principle of the Fourth Amendment. Deliberately seeking to read Americans' private communications – but without ever showing evidence of wrongdoing or obtaining independent approval from a judge – violates the Constitution, disrespects American values, and opens the door to abuse.

Opponents of FISA reform nonetheless oppose requiring a warrant for U.S. person queries by claiming these queries provide huge value that would be disrupted by a warrant requirement. ***These claims are false – in reality a [warrant rule](#) has been carefully designed to account for the limited value that such queries provide.***

MYTH #1: U.S. person queries are immensely important in a broad array of situations, making it dangerous to place restrictions on this important tool.

REALITY: Queries only provide value in a limited set of situations, and the warrant rule proposed in 2024 during the 119th Congress provides exceptions to account for all of them.

Opponents of reform frame U.S. person queries as frequently valuable across a wide set of national security goals and investigations, but the 2023-2024 debate over FISA 702 proved this was false: The [Intelligence Community testimony](#), [the President's Intelligence Advisory Board](#), and [the Privacy and Civil Liberties Oversight Board](#) (PCLOB) uncovered only a few distinct scenarios in which U.S. person queries provided value.¹ And the [proposed warrant rule](#) includes exceptions that account for all of them.

Under the 2024 proposal, a warrant would not be required 1) when there is consent, 2) to track malware, or 3) for metadata queries:

- **Cyber Attacks:** Queries were most useful in the cybersecurity context, helping the government detect warning signs of future attacks and trace attacks back to their sources. But queries focused on cyberthreat signatures are explicitly exempt. Much of the cybersecurity value of queries focused on network traffic patterns; this involves metadata rather than content, and metadata queries are also exempt from the warrant rule. Most importantly, any U.S. company or critical infrastructure entity targeted for a cyberattack can simply consent to a query.

¹ For additional details, see [The Government's Objections to FISA 702 Reform Are Paper Thin | Lawfare](#); see also [Unpacking the President's Intelligence Advisory Board FISA 702 Report | Lawfare](#).

- *Foreign Plots*: Queries were also described as useful in detecting and responding to foreign assassination and kidnapping plots. But once again, the consent exception directly accounts for this need. A targeted American will obviously gratefully accept such a query to enable government protection.²
- *Foreign Recruitment*: Defenders of the status quo cited limited cases in which queries helped the government discover suspicious foreign contacts, assisting the government in investigating whether the U.S. person was a foreign target or foreign agent. But because metadata queries are exempt, a warrant rule would not inhibit the government's ability to identify these contacts. The government *has never shown one instance* in which content queries were critical to advancing an investigation against a foreign agent.³ Besides, reading the private emails of an American being criminally investigated is exactly what warrants are required for.

MYTH #2: U.S. person queries need to be done quickly and efficiently, and a warrant rule would slow the process down in a manner that endangers Americans' lives.

REALITY: The government has never shown queries provide time-sensitive responses, and the warrant rule's exceptions account for such a scenario if it ever did emerge.

A common argument against surveillance reform is the "ticking time bomb" hypothetical in which there simply isn't time to abide by due process and obtain court approval. But the government has never shown a situation in which query results were needed so quickly that obtaining a warrant would be infeasible.⁴

- If a time-sensitive emergency ever did occur, the warrant rule explicitly accounts for it by including an exception for exigent circumstances. Contrary to this complaint's framing, the government has indicated that query results are used primarily during the *early* stages of investigations, or with queries run on targeted victims--in which cases the consent exception makes a warrant unnecessary.

² In addition to the consent exception addressing this issue, the warrant rule can be satisfied by a probable cause showing that the query *would produce evidence of a crime*; so long as that standard is satisfied it is not necessary to prove that the query subject is a suspected criminal or foreign agent. Therefore, so long as the government can demonstrate probable cause that a query focused on the target of a foreign plot will uncover details of that plot, such a query would receive necessary judicial sign off. The government has regularly obtained warrants for digital searches focused on victims, and there is no reason to expect they could not do so in the context of queries as well. For more information, see [Issue Brief: A Warrant Rule for US Person Queries Would Not Prevent Victim-Focused Queries | CDT](#).

³ Notably the two independent reviews of FISA 702 only cite *one instance* when a queried individual was later discovered to be a nefarious actor, and this discovery was the product of an "independent investigation" for which the government successfully obtained a warrant. See [PIAB FISA 702 Report](#), p. 36; see also, [PCLOB FISA 702 Report](#).

⁴ Intelligence officials sometimes reference the significant length of FISA Title I warrant applications and time spent developing them as the basis to claim that US person query warrants would be equally slow and onerous. But this is not an apt comparison because the warrant proposal allows the government to conduct queries by obtaining either a standard Title III criminal wiretap order or a FISA Title I warrant.

In short, the exigent circumstances, consent and metadata exceptions to the proposed warrant requirement almost certainly address and legitimate concerns about the government's ability to respond to threats quickly.

MYTH #3: *Warrants are not feasible given the scale of U.S. person queries conducted; adding this rule would overwhelm intelligence agencies and the courts.*

REALITY: By permitting warrantless metadata queries, the warrant rule ensures the government will not need to go to court frequently.

In 2023, the most recent year for which data is available, [the FBI conducted queries for over 57,000 unique U.S. person terms](#), reflecting unacceptable government overreach and fishing efforts. However, most of these queries do not produce responsive results. Because the proposed warrant requirement would apply only when the government sought to access a communication's content, it would weed out impropriety without straining intelligence agencies or the courts.

- Only 1.58 percent of the FBI's U.S. person queries resulted in personnel accessing content, according to the FBI.⁵ Thus, even if queries continued to be conducted at the prior rate of 57,000 annually – an unlikely prospect, given that many of these queries were improper or broad fishing efforts – a warrant would be potentially applicable to less than 1,000 queries a year, less than 3 per day on average. And because the proposed warrant rule would permit warrantless metadata queries (and only require court approval to *access content*), agencies would be able to confirm when a query will yield a "hit" before devoting any time and effort to seeking a warrant.

And even as to these 2-3 queries per day, most would fall under one of the exceptions to the warrant requirement described above. The FBI usually wouldn't need 2-3 warrants each day; more likely it would need to obtain consent of 2-3 entities to help prevent a future cyberattack or foreign plot. And if adding a warrant requirement on this limited level would be too onerous for intelligence agencies or the courts, the solution would be to add personnel to cover that need, not to reject an important constitutional safeguard against abuse.

Americans' basic rights should not be secondary to bureaucratic hurdles and staffing limits. The exceptions and exemptions built into the 2024 warrant proposal would allow the government to remain within the boundaries of the Constitution while also having the means to protect national security.

For additional information, please contact Gene Schaerr (gschaerr@schaerr-jaffe.com), General Counsel at the Project on Privacy and Surveillance Accountability, and Jake Laperruque (jlaperruque@cdt.org), Deputy Director of the Security and Surveillance Project at the Center for Democracy & Technology.

⁵ See [PCLOB FISA 702 Report](#), fn. 35.

Mr. BIGGS. Thank you so much.

We will now proceed under the five-minute rule with questions. I now recognize the gentleman from Wisconsin, Mr. Tiffany.

Mr. TIFFANY. Thank you, Mr. Chair.

Mr. Czerniawski, in your testimony—I'm going to read from it,

RISAA did little in the form of reforms while simultaneously dangerously expanding the scope of surveillance by changing the definition of what was considered an electronic communications service provider.

Could you expand on that a little bit? What are you talking about there, that RISAA actually did not solve the problem and may have made it worse?

Mr. CZERNIAWSKI. Thank you for the question, Representative.

When we were looking at RISAA last year, as part of the reforms, they included a provision that would expand the definition of an electronic communications service provider. Now, this used to be a more narrowly tailored thing to capture data from these particular companies. The way that they extended the definition would capture a wider array of companies, so virtually including everybody, right?

So, what you ended up seeing was, from the Department of Justice, they made a promise that they were going to keep their searches for this kind of data a lot more limited, but again, it is still problematic enough that even the Chair of the Senate Intel Committee, Senator Warner, committed to trying to get a fix to that.

Unfortunately, that still has not gotten done to date, but this is a real serious threat. It's now virtually any, anybody that has data on Americans could be subjected to being considered an electronic communications service provider.

Mr. TIFFANY. So, we think the new leadership at the FBI is going to be better in terms of respecting people's constitutional rights. Should Congress just move on from this issue or should it act?

Mr. CZERNIAWSKI. Thank you for the question, Representative.

I think that, in light of the fact that administrations can change, I would not want to leave it up for interpretation for a potential abuse underneath a future administration. So, I do think that Congress should act to go and fix this overly broad definition of an electronic communications service provider.

Mr. TIFFANY. Mr. Schaerr, could you comment on the amendment that Mr. Biggs had in his bill that allowed for limited exceptions? Yet, we were being browbeaten saying that, "No, you cannot do this. You cannot pass the Biggs bill because there will be no way out to be able to get a perhaps bad actor."

Would you care to comment on that?

Mr. SCHAERR. Sure. Well, and a number of reasons were offered for that. My analysis is that it was all just fearmongering. Every single objection that I heard was just based on a misunderstanding of Mr. Biggs' amendment.

For example, as Chair Jordan mentioned earlier, the amendment had an exigent circumstances exception. If there were a ticking time bomb, the agency could act without getting a warrant.

Of course, the amendment allowed for people to consent to searches. So, if the FBI thought that somebody was being the subject of a cyberattack, for example, they could go to that person and

say, “We think you may be the subject of a cyberattack. Could we search your communications, so that we can find out who it is and try to forestall it?” That person could then consent. That’s also a well-recognized exception under the Fourth Amendment.

So, the Committee very carefully, and Chair Biggs very carefully, built in the protections that the FBI might legitimately need to be able to conduct searches without a warrant.

Mr. TIFFANY. So, the long and short of it, the Biggs amendment dealt with what you term “the exigent circumstances”?

Mr. SCHAERR. Yes.

Mr. TIFFANY. Is that correct?

Mr. SCHAERR. It had an express exception for that, and it also, it also exempted metadata searches. So, the FBI could actually look to see who was communicating with whom under Chair Biggs’ amendment. It just couldn’t actually search the communications themselves.

Mr. TIFFANY. I want to ask you another question and I’m not sure if you are going—you let me know if you can answer it or not.

In 2021, the FBI lawyer Kevin Clinesmith was sentenced to 12 months’ probation versus a typical five years. Why was that?

Mr. SCHAERR. Yes. Well, it was an unfortunate slap on the wrist. I’m separately representing Carter Page in his litigation against the Department. I thought it was an outrage that Clinesmith got such a low sentence for such an egregious act of dishonesty before the FISA Court.

Mr. TIFFANY. Who was the judge in that FISA Court case?

Mr. SCHAERR. I believe it was Judge Boasberg.

Mr. TIFFANY. Yes. So, Mr. Chair, this is the same Judge Boasberg that we see regularly in the news these days. The ultimate insider judge here in Washington, DC, gives a slap on the wrist to Kevin Clinesmith, who misrepresented the information out there, to the detriment of, it sounds like, your client, now is doing everything he can to keep foreign alien criminals in the United States rather than sending them back home.

I yield.

Mr. BIGGS. The gentleman yields.

The Chair recognizes the Ranking of the entire Committee, Mr. Raskin.

Mr. RASKIN. Thank you, Mr. Chair.

A lot of people were willing to give 702 a chance because of the various exceptions and amendments that were added to try to protect and insulate constitutional values, and specifically there, the Fourth Amendment requirement of a search warrant.

What has happened in the meantime has taught me, anyway, that we should never condition respect for constitutional values on an expectation of the goodwill of political actors in the Executive Branch of government.

Mr. Hamadanchy, a week after he took office, President Trump fired all the Democrats on the Privacy and Civil Liberties Oversight Board, which we had created, leaving it without the quorum necessary to do business.

Can you tell us what the Privacy and Civil Liberties Oversight Board does or what it is supposed to do, and why it is a basic defeat of the legislative design that it is no longer functioning?

Mr. HAMADANCHY. Yes. So, the Privacy and Civil Liberties Oversight Board is designed to report on the privacy and civil liberty implications of the surveillance and counterterrorism programs of the Federal Government.

These Members that have been fired, they actually had demonstrated independence from the Biden Administration in putting out a report that the Biden Administration, on 702, very much disagreed with.

It's not a good thing for the President to be able to fire these independent Board members who are meant to provide independent oversight, because it chills their ability to provide that oversight if you think the President can fire you if you say something he doesn't like. That is why Congress actually removed from the statute language that said the President could fire these Board members.

Mr. RASKIN. Then, that is not a partisan thing, as you just pointed out. The Framers of the Constitution expected anybody who got in as President to push the boundaries of his or her own power, to the detriment of the other branches, but, essentially, to the detriment of the citizens, right?

So, that is something we saw in the Biden Administration, as you point out, and something that we are seeing right now with huge red flags in the Trump Administration. So, we have got to write laws that insulate constitutional values against anybody who gets into the Executive Branch.

Does this Board issue reports and recommendations?

Mr. HAMADANCHY. Yes. When they have a quorum, they regularly issue reports. Last year, they did a report on 702. They recently, before the firings, did a report on watchlisting programs, and they regularly would issue reports when they are able, when they have a quorum. When they haven't had a quorum, it's the PCLOB has been much less effective.

Mr. RASKIN. All right. So, there's no quorum. There are no reports. There are no recommendations. Congress is not getting the information we need to determine whether or not in this difficult terrain constitutional values are being protected against government overreach.

So, I take it you agree with me that it was bad for civil liberties and constitutional rights that the President fired the Democrats on the Board?

Mr. HAMADANCHY. Yes, I do.

Mr. RASKIN. Mr. Schaerr, do you agree with that?

Mr. SCHAERR. We would like to see PCLOB reconstituted as quickly as possible.

Mr. RASKIN. OK. Mr. Kiko, the same question to you.

Mr. KIKO. Yes, the same, we would like to have it reconstituted with the same kind of people that were there.

Mr. RASKIN. Mr. Czerniawski?

Mr. CZERNIAWSKI. The same.

Mr. RASKIN. Yes.

Mr. CZERNIAWSKI. Similar to them, yes, we would like to see PCLOB reconstituted with the full membership.

Mr. RASKIN. OK. Mr. Schaerr, I want to ask about the reforms that Congress did make to Section 702 last year when we reauthor-

ized FISA. The bill mandated the FBI's National Security Division report to Congress the number of U.S. persons' so-called "backdoor searches" conducted each month.

That is, as Chair Jordan explained it, the data is mocked-up from all the surveillance of foreign persons, but, then, since the theory is we are in lawful possession of the data, backdoor searches can exist for Americans.

Why is it important for us to know the number of backdoor searches that the FBI is conducting on a monthly basis?

Mr. SCHAERR. Well, for one thing, so that you can know the extent of the issue. You can, with the number, you can understand better the risk to Americans' privacy of the whole 702 system.

It also enables you to evaluate claims that are made by the IC about the effect of additional reforms. I don't know how you can, how you can act and respond, respond to their arguments without knowing exactly how many people—

Mr. RASKIN. What was the FBI sending us before the new reporting requirements were put in?

Mr. SCHAERR. My understanding is that it was pretty spotty.

Mr. RASKIN. Yes. The additional reporting is going to require more staff and more support. I had previously learned from the National Security Division that they wanted 14 more people to comply with Congress' requirements. Not only have they frozen hiring, but they have also removed the person who was responsible for managing of the compliance and audits. So, what does that mean—

Mr. BIGGS. The gentleman's time has expired.

Mr. RASKIN. Yes, but if I could just finish this sentence? What does that mean for the new statutory language that we put in?

Mr. SCHAERR. Well, we would certainly support staffing that very important function at NSD.

Mr. BIGGS. The gentleman's time has expired.

Mr. BIGGS. Without objection, Mr. Cline will be permitted to participate in today's hearing for the purpose of questioning the witnesses, if a Member yields time for that purpose.

The Chair now recognizes the Chair of the Full Committee, Mr. Jordan.

Chair JORDAN. Thank you, Mr. Chair.

Mr. Hamadanchy, what is the main argument the other side uses on the warrant requirement? We think there should be a warrant. They have an argument. Can you tell the Committee what that argument is?

Mr. HAMADANCHY. They will, typically, say, "We have lawfully collected this information already. So, we should be able to search through it."

The Second Circuit has recognized that the search of a U.S. person's data is a separate Fourth Amendment event that requires a separate Fourth Amendment analysis.

Chair JORDAN. Yes, that is their argument, "Oh, we followed the law. We were searching foreigners overseas for intel." Right? That is what the law says they can do. They said, "We followed the law. So, now, we can search the data for Americans." That is the problem.

The court in New York just last year said, "No, no, no, you can't do that." The court said this—here's a fundamental question. Tell

me if you agree. Should the government be allowed to do warrantless searches of the same information Section 702 says it is not allowed to collect?

Mr. HAMADANCHY. The court was very clear that they should not be able to do that.

Chair JORDAN. Right, and the law says it. You are supposed to collect information on foreigners overseas, foreign intelligence. Now, there are people who say, "No, you don't need a warrant because we're going to do searches for Americans using their identifiers, their email, their phone number, their name." Well, that is not supposed to be in there. The court said you can't have it both ways.

That is what the other side wants. They want to have it both ways. They can call it "incidental." They can say, "We're doing a query, not really a search." That doesn't fly.

Again, don't take our word for it. The court in New York said so December of last year, is that right?

Mr. HAMADANCHY. Yes, and the court said, like citing the Second Circuit, that simply storage is not enough. It said it in, I believe, *Riley v. California*, which gave the example of a case where they lawful possession of a cell phone. They still needed a warrant to be able to search the contents of that cell phone.

Chair JORDAN. Yes. This is, the Chair knows we spent a year debating this within our conference and with our friends on the other side last Congress. Then, we are about ready to go back into the same darn fight for the next year.

This court decision, we didn't have that last year. I like the way they say it. They said:

It would be paradoxical to permit warrantless searches of the same information that Section 702 is specifically designed to avoid collecting.

You are not supposed to collect information on Americans, but, "Oh, we did this search of foreigners and we got some. So now, we can search Americans." No, that makes no sense, but that has been the argument year after year, Congress after Congress. Hopefully, we can get to commonsense and what the court said this Congress and say, "Time out. You can't do it anymore."

We will still put the exceptions in, for goodness' sake. So, to answer their other argument, "Oh, there could be an emergency situation, imminent threat." OK, fine. We don't want bad things to happen to America. Fine, you can do that.

If we can't get this passed, it is—I don't know; I was so frustrated because winning beats losing every time and a tie is a loss. That is what we had last time. We have got to make sure we win this time, Mr. Raskin.

[Laughter.]

We need to make sure we win this time.

I will yield my time either to the Chair or to Mr. Cline. I have a minute and 40 seconds left.

Mr. Cline?

Mr. BIGGS. Mr. Cline?

Mr. CLINE. Thank you.

Mr. Kiko, if the government can't articulate how many Americans care being surveilled under Section 702, how can it claim the program is narrowly tailored to national security threats?

Mr. KIKO. If they can't articulate it, then they—I won't say what they're doing. It's certainly not telling the truth.

Mr. CLINE. Is it really a national security risk to require a warrant to search the communications of Americans, especially if there is probable cause?

Mr. KIKO. No, it's not a national security risk. Everybody—it's we collect all this incidental information, and you should have a, you should have a warrant to search it. That's not why it was collected. It was incidental.

As other witnesses said, "there's other ways to check on this information without like metadata and stuff like that." So, that's my opinion.

Mr. CLINE. Mr. Czerniawski, you have spoken about government overreach and tech policy. So, how do we justify allowing the government to query vast databases of Americans' private communications without a warrant, especially when those queries are increasingly used in routine criminal investigations?

Mr. CZERNIAWSKI. Yes, thank you for the question, Representative.

I don't think you can justify it. At the end of the day, when people discover that the government has violated their trust by violating their Fourth Amendment rights to search for these vast databases for their communications, that undermines their faith and trust in a key institution that they believe is supposed to be protecting them. It's quite chilling for them to realize that that weapon is being turned inward and being leveraged against them to spy on them, when they have not necessarily done anything wrong.

Mr. CLINE. I'm going to ask the ACLU witness, whose name I can't read on that.

Can you give us an update on the status of the decision? Was it appealed from the Second Circuit?

Mr. HAMADANCHY. So, the decision was a District Court decision. The defendant lost on separate grounds. So, it would actually be the defendant who has to appeal it, not the government. The government can't actually appeal that. I'm not sure what the defendant plans on doing.

Mr. BIGGS. The gentleman's time has expired.

Mr. CLINE. Thank you.

Mr. BIGGS. The Chair recognizes the gentleman from New York, Mr. Goldman.

Mr. GOLDMAN. Thank you, Mr. Chair.

I do look forward to having this debate. As someone who spent 10 years writing, drafting, and getting warrants through courts, and recognizing, also, the exigent circumstances that often exist with the 702 information, it is not as simple as my friend, the Chair at the end, would have you believe. I probably disagree with some of the witnesses here today as well.

The problem I have with this hearing is, this is an important argument, but it pales in comparison to what is going on right now with Americans' privacy, with Americans' national security. We are talking about whether there should be a warrant to search a certain amount of information lawfully collected from foreigners. It's not a broad set of information.

Yet, some nongovernment employee, Elon Musk, is getting access to every single American's personal identification information. His employees, some of whom have already been found to have stolen information from one company to bring to another competitor, are getting access to Americans' personal identification information, whether it be through the Social Security Administration, it be through the Department of Treasury.

So, it feels like this hearing, while important, is somewhat misguided at this time, when the privacy considerations of every American are at risk, rather than a very narrowly tailored set of Americans who are communicating with foreigners who are suspected, or potentially suspected, of being involved in adversarial actions against the United States.

The other thing that I want to bring up with our friends here is the threat to national security. We are talking a lot about that in this hearing. Obviously, 702 is designed to protect our national security.

As many of you know, I'm sure, last week I believe it was, the NSA Director General Timothy Haugh, widely, widely respected, a career national security official overseeing the NSA, which is principally responsible for using Section 702 materials and gathering Section 702 materials, he was fired. Do you know why he was fired, Mr. Hamadanchy?

Mr. HAMADANCHY. The reporting is that there were certain people commenting to the President, specifically, Laura Loomer, that he should be fired.

Mr. GOLDMAN. Laura Loomer. Yes, Laura Loomer went in and had a meeting with the President and urged that General Haugh should be fired because he was handpicked by General Mark Milley, who was the Chair of the Joint Chiefs of Staff in 2023, when Haugh was nominated to lead both the Cyber Command and the NSA.

Now, this is the same Laura Loomer who says 9/11 was an inside job; who has openly advocated at a White nationalist conference that she is a White advocate; who said during the campaign that, if Kamala Harris, who is half-Indian, won, that, quote, "The White House would smell like curry and White House speeches will be facilitated via a call center"; who has said that numerous mass shootings are all hoaxes and conspiracies; who calls herself a proud Islamophobe, and perpetuated the completely bogus conspiracy theory about Haitian immigrants in Ohio. Yet, she is given access to the President of the United States to make a national security recommendation that, coincidentally or not, the next day happened.

How does this affect our national security, Mr. Hamadanchy, when a conspiracy theorist who is denounced by numerous Republicans is effectively making decisions about who oversees our most sensitive collection agency?

Mr. HAMADANCHY. So, I think the first question is whether or not the NSA Director was refusing to follow any illegal orders. The reporting does not indicate that.

The second question is, have there been any policy changes at the NSA since President Trump took office? That's something that this Committee should look at.

The third question is, who is the President going to replace the NSA Director with? If that person is unqualified, if that person has the potential for abuse, to abuse the authority of NSA? That's something that Congress should weigh-in on, if that's the case.

Mr. GOLDMAN. I agree—

Mr. BIGGS. The gentleman's time has expired.

Mr. GOLDMAN. Mr. Chair, I will. I will, if I could just have one second?

Mr. BIGGS. No, you can't.

Mr. GOLDMAN. I agree that—

Mr. BIGGS. Your time has expired.

Mr. GOLDMAN. —I hope we do look into all that because that's far more important than Section 702 right at this minute.

Mr. BIGGS. Thank you, Mr. Goldman.

The Chair now recognizes the gentleman from Alabama, Mr. Moore.

Mr. MOORE. Thank you, Mr. Chair.

Mr. Chair, a quick question.

The Crossfire Hurricane investigation and subsequent surveillance of Carter Page, a real dysfunction and political bias, obviously, on the part of the FBI leadership, but also real problems with FISC, is that correct?

Mr. SCHAERR. It did. It illustrated that FISC does not always examine the warrant applications under Title I with sufficient care, and that's one of the reasons that our organization, working with Senator Lee and many others, has been pushing for reforms at the FISC that would allow amici, friends of the Court, to participate in important FISC proceedings to ensure that privacy is protected.

Mr. MOORE. One of the reforms—are there other reforms, as you recommend, to help as we work through this process of reauthorizing 702 that we could put into the law that would help eliminate some of these abuses? Lord, there have been a number of them.

Mr. SCHAERR. Well, the amicus requirements were strengthened somewhat in RISA. I think they can be strengthened still further. RISA did contain a very useful provision in that it allowed the Chair and the Ranking Member of this Committee, for example, to sit in on FISC proceedings so that there's more of a window of transparency there.

Certainly, FISC needs additional staff. They need to have additional people who are cleared, so that they can process their business more expeditiously, but—

Mr. MOORE. Also, RISA—and I think we put in the—require the same judge to renew the application process.

Mr. SCHAERR. Yes.

Mr. MOORE. There were some other things, too. One of the things that—the reason I was a no-vote is I thought there should be a warrant requirement. Would you agree with that?

Mr. SCHAERR. Absolutely.

Mr. MOORE. That was stripped out at the end. That was a tough vote for many of us. We wanted to do what we could to renew this thing, but when you got—when I came to D.C., they wanted to issue me another government phone. I said, “I think you just need to put everything on one phone.” They were like, “Well, sir, if we

do that, we're going to know everything that is on your phone." I thought to myself, "Like you don't already." Right?

So, as we are going through these hearings, we understand they are spying on U.S. citizens without warrants. That was one of the things that I thought we absolutely needed to do. What are improvements that Congress can consider to—for FISC on how it operates, some other improvements as we're going through this process?

Mr. SCHAEFFER. None beyond those I have just mentioned.

Mr. MOORE. OK. So very good.

Mr. Czerniawski, will you explain how the government has abused nondisclosure orders relating to the use of information obtained under FISA?

Mr. CZERNIAWSKI. Yes. Thank you for the question, Representative. The government has utilized the information gathered under the FISA in numerous of instances to spy on Americans, whether that was spying on protestors during the Black Lives Matter riots or looking at the communications of 19,000 donors to a political campaign. The list goes on and on.

Really, when people see that revelation coming up after the fact, it does undermine their trust because they feel that the government now is starting to snoop at them. That has a real chilling effect if now, simply because you want to support a candidate, now you could be subjected to government surveillance. That is a pretty unnerving outcome for people to see this carried out.

Even in this most recent iteration of the FISA reauthorization fight, to see that those surveillance authorities had been abused to spy on a sitting Member of Congress, a sitting Member of the Senate, it showed to me that the intelligence community seemingly had no self-restraint on what they were willing to do to get access to whatever information they thought was necessary. That is really alarming.

Mr. MOORE. Extremely alarming. For those of us that—one of the top issues was always the weaponization of the government, and certainly, certain Members were spied on and, like you said, Members of Congress.

With that, Mr. Chair, I yield my remaining time to our friend Mr. Cline if he wants to take it. If not, I will yield back to you.

Mr. CLINE. I appreciate the yielding.

Mr. Kiko, do you think you would support an independent audit of these queries conducted under 702?

Mr. KIKO. Yes, I would support that.

Mr. CLINE. How else can we ensure meaningful congressional oversight when most of the relevant details are classified and shielded from public scrutiny?

Mr. KIKO. Well, I just think there are a lot of requirements that are already in the law. I just would hope that the requirements are adhered to in a very quick manner, the audits are done in a very quick manner, and the audits and requirements are audited in the next year, so if they are not complied with, then you can deal with that through the next reauthorization.

I do think that the IG was very good in coming up with all the problems and everything, and Congress responded to 15 or 20 re-

quirements. It is, basically, oversight is—you have to bring the intelligence community to heel.

Mr. CLINE. Thank you.

Mr. BIGGS. The gentleman's time has expired. I now recognize the gentleman from California, Mr. Kiley, for five minutes.

Mr. KILEY. Thank you, Mr. Chair.

I think it is important to note at the outset the successes that we did have in the last Congress in reauthorizing FISA for the protection of America and American national security while instituting some truly significant reforms, which were developed through the painstaking work of this Committee and in a bipartisan way in a Committee that is not always known for its spirit of kumbaya bipartisanship. We were able to find a lot of common ground in protecting civil liberties without burdening the ability of our national security officials to protect Americans.

However, there is, as Chair Jordan noted, more work to do. I do think it is important to look at what was done in the bill that was signed into law in the last Congress. We had reforms that included new and heightened civil and criminal penalties for those who violate the terms of the FISA authorities and that required reporting on FBI disciplinary investigations. It requires the FBI to establish minimum accountability standards for violations of the querying process. The bill significantly reduced the number of FBI personnel authorized to approve queries, required audits of U.S. person queries, and included increased transparency measures, among other important reforms.

There is a broader question here, though, when it comes to the pace at which we are seeing technology develop and the newfound opportunities that this opens up for very problematic violations of privacy or uses of surveillance, but then at the same time, the opportunities to perhaps use that technology not only to advance national security and public safety, but to do so in a more narrowly tailored way.

Advances in AI are an example of that where there are obviously a host, an unlimited variety, of potentially problematic uses by those who are entrusted with the power to investigate American citizens, but then there are also already a number of very positive proven use cases.

So, my thought—and I will maybe direct this at you, Mr. Hamadanchy—is on how we can harness this technology in the right way going forward. You gave an example of how there was one police agency in Florida that—or maybe this was you, but—so either of you can weigh in on it, but that used an algorithm to try to predict where crimes were more likely to occur. That seems like it actually could be helpful if it allows us to allocate police resources in the right way, but may be unhelpful if it leads to people being targeted prematurely or in a way that violates their civil liberty.

I guess I will give either of you an opportunity to opine on that. Maybe we will start with Mr. Hamadanchy, and then since I misremembered who actually gave this example, I will give you the opportunity as well.

Mr. HAMADANCHY. I would say we are definitely concerned about the use of AI in surveillance. More than four years ago, we had a

report where intelligence agencies were saying they want to embed AI in every stage of the intelligence cycle. The NSA stands out in this context because it just described itself as a leader in integrating AI into intelligence-gathering.

There are real concerns that AI is being used to automate target selection and potentially initiating surveillance without adequate human review. That is something the Committee should look into as it considers these issues.

Mr. CZERNIAWSKI. Thank you for the question, Representative. I think that it is incredibly important. As you rightly note, artificial intelligence is a tool. It is a pretty neutral values/neutral kind of thing. It depends on who is using it as to whether or not that can be used for good or for bad.

It is really unfortunate when we see instances like what happened in Florida where they were using AI to develop this algorithm to identify prolific offenders and then give them community visits. One such person ended up in the hospital with symptoms of an anxiety attack because of the presence of law enforcement coming up and showing on their door. You can imagine that this is a very frightening experience for some people.

That it just reinforces the need—I don't want to go and take away a tool from law enforcement from being able to leverage a tool like artificial intelligence or other technologies that are out there, but I do think that it is important to make sure that if they are going to be using it, that we have proper rules and guidelines and procedures in place to minimize the potential downside here because when the State does leverage these technologies and they get it wrong, the costs are really high both for the city that ultimately bears the responsibility of the legal action that follows and for the victims in that case.

There is a really good conversation to be had about what we can do to go and better set guardrails around this so that law enforcement doesn't lose access to critical tools that can help them with their public safety functions while simultaneously protecting people's Fourth Amendment rights.

Mr. KILEY. Yes, and I will add to that this—getting this right is really important, not just for protecting civil liberties in the first instance, but also because there are so many truly beneficial applications of AI in this and other contexts, and that if we don't—

Mr. BIGGS. The gentleman's time has expired.

Mr. KILEY. —get these threshold questions right for protections, then it could lead to a backlash that undoes those possibilities. With that, I yield back to the Chair.

Mr. BIGGS. I thank the gentleman.

The Chair recognizes now the gentlelady from Florida, Ms. Lee.

Ms. LEE. Thank you, Mr. Chair, for convening this important hearing.

Thank you to our witnesses who have joined us today to provide testimony. This Committee remains committed to restoring public trust in our Federal law enforcement agencies, and a critical part of that involves holding open, informed conversations with experts like yourself to identify areas of proposed reform and change that we can then use to inform our work and collaboration with the intelligence community.

Last Congress, I was proud to lead the RISA bill that we have been discussing here today, which made significant reforms to how our Federal law enforcement agencies handle, collect, and retain critical intelligence. This legislation was an important first step in our broader effort to rebuild confidence in the intelligence community and to keep America secure.

There is no question that the abuses that we have seen, particularly in the FBI's handling of Section 702 information, are deeply troubling, and the surveillance unauthorized or unlawful of American citizens must be stopped. It should not have happened, and it must not happen going forward, which is why accountability and transparency and the things that we are discussing here today are so important.

It is also important that any discussion that we have about 702 include a recognition of why we have it and why it exists and that this is a vital part of our country's intelligence-gathering capabilities. It is an essential component of what we do, and it is necessary that this conversation center on how we make it better, how we ensure accountability and transparency without dismantling it.

With that in mind, I appreciate your efforts to help us strike that balance and identify where we can further improve and strengthen FISA overall and Section 702 in particular.

Mr. Schaerr, I would like to start with you and in particular return to the discussion you were just having about the FISC and some of the reforms that we implemented in the FISC to ensure a greater level of accountability and prevention of some of the abuses that we've seen in the past.

In particular, as you know, the RISA bill implemented inclusion of a more adversarial process for FISC proceedings. You just mentioned you thought we could do more there with amici. I would love to hear more about your thoughts about how that program could be further enhanced.

Mr. SCHAERR. My recollection of RISA is that—and I agree with you, Congresswoman Lee, that there were some very useful reforms in RISA, and we should look to build on those rather than tear them down.

With respect to amici and the FISA court, I think that one limitation is that, currently, amici are only appointed if the judge decides that an amicus would be helpful. That obviously leaves the FISC judge with lots of discretion as to whether to appoint an amicus.

We would prefer to see that expanded somewhat so that there is a category of cases where the judges are expected to appoint amici, for example, cases that obviously involve sensitive political issues or religious issues, like the FBI's investigation of the traditionalist Catholics down in Richmond last year or a couple of years ago.

Those kinds of situations—and you can identify categories of situations where an amicus, at least presumptively, should be appointed. If an amicus is not going to be appointed, then the judge should have to explain why not.

Ms. LEE. I would note a couple of additional reforms we made specifically in the FISC that were targeted to prevent some of the past abuses we have seen—first, a requirement that exculpatory evidence be included in an application before the FISC; and second,

also that opposition research could not be the basis for granting of a warrant by the FISC.

Are there other things that you think—first, do you find those reforms to be something that was productive and useful? Second, are there other things you think we should get at or address there with the FISC?

Mr. SCHAERR. Absolutely. Those were important reforms, for sure. One additional thing that would be very useful is to create a system whereby people whose rights are abused in the FISC court—for example, like the Kevin Clinesmith situation—make clear in the law that people who are victims of that are entitled to compensation when that happens. That will not only be fair to those people, but also will provide an added deterrent to abuse.

Ms. LEE. Thank you.

Mr. Chair, my time is expired.

Mr. BIGGS. I thank the gentlelady.

The Chair now recognizes the gentleman from North Carolina, Mr. Knott.

Mr. KNOTT. Thank you, Mr. Chair. Thank you for having this hearing. To all the Members and the guests, thank you for your participation.

I come at this line of questions from my own experience as a Federal prosecutor. I have actually engaged in surveillance of American citizens through a process called the Title III wiretap. The level of protections that are required to get to the actual flipping of the switch—it is fairly astounding. Obviously, it is one of the more intrusive investigative techniques, so you have to demonstrate necessity. You have to demonstrate why other techniques are futile.

Candidly, once we would go to trial or once we would charge the case, the rigor that we had to exercise was very important for a number of reasons. Obviously, it kept the internal investigators accountable. It kept the process—once we were—the investigation was ongoing, it kept it open and honest. They knew that their actions were going to be subject to pen and paper. They were going to be subject to judicial review, and then obviously, with opposing counsel, they would review it. Also, when we would go to court, if there was a jury trial, the jury themselves would know these actions; this evidence, was collected with sufficient predication.

I do find it somewhat—I don't want to say troubling yet, but it is amazing to me that there is so much resistance to the warrant requirement alone. In that vein, with the Title III wiretap on one side, I am very familiar with how the evidence is collected, how it is stored, how it is accessed.

Mr. Czerniawski, if you could explain, with the 702 program and the FISA court, how is the data that is collected under that subsection—how is it, again, collected, stored, and then accessed? Does that make sense? Just tactically and in a physical server, how is it collected and stored and accessed?

Mr. CZERNIAWSKI. Yes, so it is stored on a secure server. The backdoor search loophole really is why this is so important, right? Because this is basically allowing the government's ability to search the communications that they have incidentally collected or, as Chair Jordan has referred to it, incidental collection of Ameri-

cans' information during the surveillance of foreign targets, all without a warrant, right?

Mr. KNOTT. Right.

Mr. CZERNIAWSKI. This warrant requirement that we have been advocating for adds that necessary layer of protection because, as you pointed out, as we are—we are using warrants, basically, as a procedure matter of demonstrating why we got to where we got. That is really important that—when we are talking about foreigners that is fine if we are going to go and engage in surveillance, but once those surveillance powers turn inward and we are trying to tap into that data that we have collected, that we have that warrant process carried out, so that way we have due process.

Mr. KNOTT. When that much information is readily available, the natural trend throughout history, regardless of who is in power—obviously, people on my side of the aisle are very distrustful given what happened with President Trump. There have been conservative abuses when we are in power, without question.

Mr. CZERNIAWSKI. Absolutely.

Mr. KNOTT. In regard to that information, how easy is it to access once it is collected?

Mr. CZERNIAWSKI. It is fairly easy for people to go and access that, and that is why we have seen the litany of abuses as to why that information needs to have a better, tightened control. Now, admittedly, as Representative Lee was talking about, they have done some limited changes in RISA to go and talk about what kinds of members of the FBI can go and query that data.

We believe that this is still not sufficient. This is why we want that warrant requirement, so that way we can have that procedural accountability of who is tapping into it, and be able to have the necessary—

Mr. KNOTT. Is there any way, with the current technology infrastructure, to determine how often that material is accessed and by whom?

Mr. CZERNIAWSKI. Right now, I think that it is a challenge in its own right because we don't have full transparency into who is querying it.

Mr. KNOTT. That is a huge problem.

Mr. CZERNIAWSKI. It is a massive problem.

Mr. KNOTT. That is a huge problem.

Mr. CZERNIAWSKI. Yes. Absolutely, Representative.

Mr. KNOTT. Mr. Chair, let me talk to you really quickly. In regards to you mentioned earlier that you worked with Carter Page. That obviously highlights a lot of abuse, again, for political purposes, right? Which is what the Fourth Amendment is designed in part to protect against.

What type of penalties, what type of deterrents, are there for the law enforcement community if they abuse the 702 access to information currently?

Mr. BIGGS. Well, currently, there is—for one thing, there is no personal liability if somebody abuses that system. There is only the potential for liability against the government itself if you can jump through the necessary hoops.

Mr. KNOTT. Given how opaque this process is, that is very hard to build a case against.

Mr. BIGGS. It is very difficult.

Mr. KNOTT. Yes. In the Title III wiretap affidavit, if you lie, if you submit false information, you will be charged. You could lose your law license, et cetera.

Mr. BIGGS. Right. Right. We don't yet have those kinds of protections in the 702 area. We moved a lot closer to them with RISA, but—

Mr. KNOTT. Yes. Well, I could go a lot longer, but, Mr. Chair, five minutes goes very fast.

Mr. BIGGS. Thanks. The gentleman's time has expired.

I now yield to myself for five minutes. I, like all you—I want to see PCLOB back up and running.

I will ask you, Mr. Hamadanchy, is this the first time that we have been without a quorum on PCLOB?

Mr. HAMADANCHY. It is not.

Mr. BIGGS. Yes. It is not. We need to get it up and run as quickly as possible, but it is not—this isn't necessarily unique. It needs to get fixed, though. I wanted to ask you a question because you responded, and I am going to tell you how I interpreted your answer why the firing took place. You said it was reported that Laura Loomer recommended that. I interpret that as meaning that you are like me. I don't know why he was fired.

Mr. HAMADANCHY. Yes, I only know the reports that I read.

Mr. BIGGS. Yes.

Mr. HAMADANCHY. I will say there is a difference, also, between a job like the NSA where the President has the authority to fire someone, where with PCLOB, it is an independent oversight board, and the President should not be able to fire those board members.

Mr. BIGGS. He currently has the authority now, but maybe some reform there is what you are suggesting.

Mr. HAMADANCHY. Yes. Well, we would argue that he did not have the authority to fire the board members.

Mr. BIGGS. OK. All right. Fair enough.

I am going to go on here. Mr. Schaerr, you reported that there was—you indicated that there was some reported abuse, even perhaps post-RISA. Can you give us an idea?

Mr. SCHAERR. Yes.

Mr. BIGGS. Right.

Mr. SCHAERR. That is from an ODNI report from after RISA was passed that described a number of additional abuses, including congressional staffers and a number of Federal employees and even the spouse of somebody who had requested a security clearance.

Mr. BIGGS. It is remarkable because RISA was supposed to take care of probably that very kind of thing and failed to do so, which is indicative that we need to do more.

Mr. SCHAERR. Right.

Mr. BIGGS. Mr. Kiko, I would venture to say, the Chair is gone, but the Ranker is still here. RISA allowed for the Chair and the Ranker to attend FISC hearings. My guess is that they haven't been able—actually, we have got a busy schedule, so probably did not get to do that. We actually were trying to get that expanded, those of you who are participating with us, so there would be more Members of Congress who could actually get there.

Do you know if the Chair or the Ranker have been able to actually attend a FISC hearing?

Mr. KIKO. No, I do not.

Mr. BIGGS. You have indicated there should be some more oversight. How do we get more vigorous oversight, and in a shortened answer, how would you say we do that?

Mr. KIKO. I would just—

Mr. BIGGS. You need your microphone, please.

Mr. KIKO. Yes, I see that. I would just have meetings all the time. I would have somebody, whoever is your oversight person, call these people up and say, “Where are you on this? Give a report,” because there are 15 or 20 requirements that are new requirements in RISA. You should hold their feet to the fire and get in coordination with the Inspector Generals and have a whole bunch of stuff done that way.

I did mention in my testimony, though, there was a requirement that—for one of the intelligence agencies to use—I think it was the FBI—AI to make sure that there is compliance.

Mr. BIGGS. Right.

Mr. KIKO. I don’t know why this body, your Committee, shouldn’t be able to real-time make sure that there is compliance, and what does that compliance look like? Just make sure that they are complying with everything because you are going to be reauthorizing the bill in a year.

Mr. BIGGS. I agree with you. We need to be more vigorous in oversight, definitely and for sure.

Mr. Czerniawski, the warrant requirement—and Mr. Knott alluded to this. A lot of people think that is just too onerous to get. With a recent court ruling, but beyond that, if there are exigencies in there—did we miss any exigencies, any sections, when we put together the amendment to the proposed bill last year?

Mr. CZERNIAWSKI. Thank you for the question, Mr. Chair. I believe that the warrant—the sections to the warrant amendments that you put together during the last Congress were quite robust in terms of providing the needed flexibility for the agencies to conduct their surveillance without necessarily needing to worry about that. You did a very good job with that, sir.

Mr. BIGGS. Thank you. I would say that I am where Chair Jordan is. I thought we actually opened the door up too wide, broader than you would have in a normal Fourth Amendment exigency circumstance.

Needless to say, we are going to work on this. I appreciate all of you being here today. I appreciate your testimony, and I think more reforms ahead, to be frank with you. So, with that, thank you all, and we are adjourned.

[Whereupon, at 11:35 a.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Crime and Federal Government Surveillance can be found at: <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118101>.