AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 118–575

# OVERSIGHT OF SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND RELATED SURVEILLANCE AUTHORITIES

## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

JUNE 13, 2023

**Serial No. J–118–20**

Printed for the use of the Committee on the Judiciary

*www.judiciary.senate.gov*
*www.govinfo.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
58–969 WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

DIANNE FEINSTEIN, California
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
CORY A. BOOKER, New Jersey
ALEX PADILLA, California
JON OSSOFF, Georgia
PETER WELCH, Vermont

LINDSEY O. GRAHAM, South Carolina, *Ranking Member*
CHARLES E. GRASSLEY, Iowa
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TED CRUZ, Texas
JOSH HAWLEY, Missouri
TOM COTTON, Arkansas
JOHN KENNEDY, Louisiana
THOM TILLIS, North Carolina
MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, *Chief Counsel and Staff Director*
KATHERINE NIKAS, *Republican Chief Counsel and Staff Director*

# CONTENTS

## OPENING STATEMENTS


| | Page |
|---|---|
| Durbin, Hon. Richard J. | 1 |
| Graham, Hon. Lindsey O. | 12 |


## WITNESSES


| | |
|---|---|
| Abbate, Paul | 9 |
| Prepared joint statement | 46 |
| Responses to written questions contain classified information and are not included in the appendix. | |
| Barnes, George C. | 5 |
| Prepared joint statement | 46 |
| Responses to written questions contain classified information and are not included in the appendix. | |
| Cohen, David S. | 7 |
| Prepared joint statement | 46 |
| Responses to written questions contain classified information and are not included in the appendix. | |
| Fonzone, Chris | 3 |
| Prepared joint statement | 46 |
| Responses to written questions contain classified information and are not included in the appendix. | |
| Olsen, Matthew G. | 11 |
| Prepared joint statement | 46 |
| Responses to written questions | 60 |


## APPENDIX


| | |
|---|---|
| Items submitted for the record | 45 |

# OVERSIGHT OF SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND RELATED SURVEILLANCE AUTHORITIES

**TUESDAY, JUNE 13, 2023**

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:04 a.m., in Room 216, Hart Senate Office Building, Hon. Richard J. Durbin, Chair of the Committee, presiding.

Present: Senators Durbin [presiding], Whitehouse, Klobuchar, Blumenthal, Hirono, Booker, Padilla, Ossoff, Welch, Graham, Grassley, Cornyn, Lee, Cruz, Hawley, Kennedy, Tillis, and Blackburn.

## OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Chair DURBIN. This meeting of the Senate Judiciary Committee will come to order. Senator Graham is on his way and sent word that we should start before he arrives.

Today, the Judiciary Committee will focus on two of our most critical responsibilities to the American people: protecting our national security and our Constitution.

At the end of this year, an important and controversial surveillance authority known as Section 702 of the Foreign Intelligence Surveillance Act, or FISA, is set to expire. It is worth taking a moment to recall the history of this program.

After 9/11/2001, the Bush administration launched a warrantless surveillance program without authorization from the courts or Congress. Years later, the Committee heard dramatic testimony about White House officials pressuring Attorney General John Ashcroft from his hospital bed to reauthorize this surveillance program. He refused.

After this surveillance program came to light, Congress retroactively authorized it in the FISA Amendments Act of 2008 as a temporary—temporary emergency tool to combat terrorism. That is what became Section 702.

Today, nearly two decades later, Section 702 is touted as critical for a range of purposes, including countering China, tracking Russian atrocities in Ukraine, and even monitoring the distribution of fentanyl in the United States.

There is no doubt that Section 702 is a valuable tool for collecting foreign intelligence. But, as I have said for years, Section

702 also raises serious constitutional concerns. Only foreigners abroad may be targeted under Section 702. Let me repeat that. Only foreigners abroad may be targeted under Section 702. But in the course of gathering intelligence on foreigners, our Government also collects the private communications of Americans who communicate with these individuals abroad.

How many American communications are collected under Section 702? The Government cannot and will not say. What we know is that hundreds of thousands of foreigners are targeted each year, and likely, billions of communications are collected and stored on Government databases. The Government can then search these databases for Americans email, phone calls, and text messages. All without a warrant.

Just as a reminder, the Fourth Amendment to the Constitution says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

It was my view when this program was first established—first authorized by Congress in 2008, and it's my view now that Section 702 does not sufficiently protect the privacy and civil liberties of Americans.

That's why I joined with Senator Lee in a bipartisan 2012 effort to offer an amendment to require a warrant for any backdoor search of American communications.

The Government can then search these databases for emails and phone calls, as I mentioned earlier, in what is known as a backdoor search. The FBI alone conducted more than 200,000 warrantless searches of Americans in 2022.

Since Senator Lee and I offered our amendment in 2012, the problems with Section 702 have continued. The court charged with overseeing this program has found, quote, "persistent and widespread," closed quote, violations of the rules governing Section 702.

In just the latest example, it was recently revealed that the FBI has used Section 702 to conduct backdoor searches on the communications of Americans who were arrested in the racial justice protests following the murder of George Floyd, as well as individuals who participated in the January 6 insurrection.

I understand that recently implemented remedial measures have already begun to reduce these egregious violations. I understand additional compliance measures are under consideration. These are good steps. But Congress also has a constitutional responsibility.

So at the outset of today's hearing, let me say this. I will only support the reauthorization of Section 702 if there are significant—significant reforms. And that means, first and foremost, addressing the warrantless surveillance of Americans in violation of the Fourth Amendment.

Moreover, the reforms must also include safeguards to prevent future abuses and ensure effective oversight by Congress and the courts.

Some of our colleagues believe it will be best to let this authority expire. Others argue that Congress should reauthorize Section 702 with minimal reform.

As Chair of this Committee, I will work on a bipartisan basis to bridge this divide over the coming months. I understand the seriousness of this challenge. We can protect America's national security and the constitutional rights of the American people at the same time.

Senator Graham has not arrived. I will start with the introduction of the witnesses. He may be coming in shortly.

Today, we welcome five senior officials from the administration. Chris Fonzone—I hope I pronounce the name correctly—general counsel of the Office of Director of National Intelligence. Next, we will hear from George Barnes, deputy director of the National Security Agency. We will then hear from the deputy director of the CIA, David Cohen. Following Mr. Cohen, we will hear from Paul Abbate, the deputy director of the FBI. And last, we will hear testimony from the Assistant Attorney General for National Security at the Department of Justice, Matt Olsen.

After we swear in the witnesses, each witness will have 5 minutes to provide an opening statement. Then each Senator 5 minutes to ask.

I urge my colleagues to focus their questions on today's hearing. In particular, I'd like to emphasize that everyone on both sides of the aisle has a responsibility not to interfere in the Special Counsel's ongoing criminal investigation of the former President.

Mr. Trump is entitled to the presumption of innocence. Attempting to litigate the indictment against him has no place in today's hearings. Now, I'd ask the witnesses to stand and be sworn. Please raise your right hand.

[Witnesses are sworn in.]

Let the record reflect that all of the witnesses answered in the affirmative. We'll begin with opening statements from ODNI General Counsel Chris Fonzone. Mr. Fonzone, you may proceed.

**STATEMENT OF CHRIS FONZONE, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

Mr. FONZONE. Chairman Durbin, distinguished Members of the Committee, thank you for the opportunity to speak to you today about Section 702 of the Foreign Intelligence Surveillance Act, an important intelligence authority set to expire at the end of the year.

Section 702 is an authority that enables the United States to collect critical foreign intelligence on non-U.S. persons located outside the United States with the assistance of U.S. communications service providers. It provides the United States with indispensable insight into a diverse range of issues, from the conventional and cyber threats posed by China, Russia, Iran, and North Korea to cybersecurity and terrorism threats, to the proliferation of weapons of mass destruction, to numerous other high priority national security challenges.

And it provides these insights while simultaneously requiring the Government to comply with robust safeguards designed to protect the privacy and civil liberties of Americans. That's why, in a nut-

shell, my intelligence community, and DOJ colleagues, and I believe the reauthorization of Section 702 is so vital.

Section 702's origins lie in the rapid changes of the threat in communications landscape that occurred early in the 21st century when Congress recognized that the then-existing legal framework for collecting intelligence—often referred to as traditional FISA—had not kept pace with technology.

Specifically, when FISA was first enacted in 1978, it was primarily designed to regulate activities inside the United States. Over time, however, the advent of the internet and other technological changes meant that terrorists, hackers, spies, and other adversaries operating overseas, but using U.S. communication services, were increasingly subject to traditional FISA's requirements. Requirements which included that the Government must obtain a court order based on probable cause to collect those adversaries' communications.

The operational burden of obtaining those individual court orders was unworkable, however, and also legally unnecessary as foreign adversaries located overseas are not entitled to Fourth Amendment protections.

Section 702 was Congress' elegant solution to the problem. Rather than requiring individual judicial approval to collect intelligence on these non-U.S. persons located overseas, Congress decided to create an approach that a court would approve on a programmatic basis, and that all three branches of our Government would help oversee.

Specifically, for the Government to collect intelligence using Section 702, the Foreign Intelligence Surveillance Court, an Article III court, must annually review and approve certifications submitted by the Attorney General and Director of National Intelligence that describe the categories of foreign intelligence that the Government plans to acquire.

Alongside these certifications, the court also reviews the detailed procedures containing privacy and civil liberty safeguards the Government proposes to follow in collecting and using in foreign intelligence under Section 702. And the court will only approve these certifications procedures if it concludes that they are consistent with both the Fourth Amendment and FISA, including statutory protections that require the program to be properly aimed at non-U.S. persons located outside the United States.

Even after the court approves the program, the Government still cannot collect information on any specific target until it complies with detailed rules that require, among other things, a documented basis for concluding that the target is a non-U.S. person located overseas, and that there is an appropriate foreign intelligence purpose for the collection.

Furthermore, even after the Government starts collecting under Section 702, all three branches of our Government engage in rigorous oversight of the program. This includes oversight from internal components at each agency, DOJ's review of the documentation for every targeting decision, programmatic oversight from DOJ and ODNI, regular reporting to the FISC, and regular reporting and briefings to the congressional Intelligence and Judiciary Committees.

I think it is safe to say that my colleagues and I unanimously believe that this program, enacted by Congress in 2008 and subsequently improved over time, is an essential authority. In particular, while I will leave it to my colleagues to provide more detail on Section 702's intelligence value, I will just note that I think the Attorney General and DNI pretty much summed it up in a letter they sent to congressional leadership earlier this year: "Section 702 has proven invaluable again and again in protecting American lives and U.S. national security," they wrote, "such that there is no way to replicate Section 702's speed, reliability, specificity, and insight."

Likewise, I believe the other half of Section 702's equation, its privacy and civil reduced safeguards, have also proven their efficacy. To be sure, this does not mean the intelligence community has been perfect. To the contrary, like any human endeavor, we have made mistakes, including some important ones.

But Section 702 has required us to identify and confront those mistakes, disclose them to our overseers and the public, and take remedial actions that make us better. This process also identifies areas for potential statutory improvement, and we are therefore committed to working with Congress on reforms so long as they fully preserve the critical intelligence Section 702 provides.

I look forward to answering your questions today and working with you to renew this essential authority. With that, I will turn it over to my colleague from the National Security Agency.

[The prepared statement of Mr. Fonzone appears as a submission for the record.]

Chair DURBIN. Thank you, Mr. Fonzone. We have next NSA Deputy Director Barnes. You may proceed.

**STATEMENT OF GEORGE C. BARNES, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY**

Mr. BARNES. Chairman Durbin, Ranking Member Graham, and distinguished Committee Members. I'm honored to represent the National Security Agency here today, and I'm grateful for the opportunity to speak with you about FISA, Section 702. This authority is essential to NSA's foreign intelligence mission. Without it, our ability to preserve the Nation's security would be significantly impaired.

The United States is the leader in internet technology and U.S. communication services are globally distributed, including by use by a myriad high priority intelligence targets. When the intelligence community compels the assistance of electronic communication service providers under 702 authority, we quickly get access to reliable, detailed information that addresses key national security information gaps affecting the safety and security of our Nation.

The importance of this authority to our mission cannot be overstated. Data from FISA Section 702 helps us every day to understand the strategic intentions of foreign governments and certain non-state actors who pose threats to our interests. This source of intelligence is a big part of what keeps our leaders well informed about the threats we face. Fifty-nine percent of the Presidential Daily Brief articles include intelligence acquired by NSA under 702 authority, and the PDB plays a key role in keeping the leadership across our Government cited on key threats.

Countless intelligence community successes would not have been possible without 702. We have spoken publicly many times about how 702 has supported our counterterrorism mission from preventing an attack on New York City's subway in 2009, to supporting the operation that took down Ayman al-Zawahiri just last year. But 702 has likewise become indispensable across NSA's other vital mission areas.

Let me offer some specifics.

702 collection identified an Iranian ransomware attack against an American nonprofit, and the data we acquired provided the U.S. Government with information needed to mitigate the damage and recover the victim organization's data without resorting to ransom payments.

Information acquired under 702 authority was essential to the recovery of the cryptocurrency ransom paid by Colonial Pipeline to the foreign hacker who perpetrated the attack in 2021.

Section 702 was vital in warning the international community, the private sector, and the public about DPRK efforts to commit widespread fraud, including against U.S. businesses aimed at generating revenue for their nuclear weapons program.

702 regularly provides intelligence community counterparts with critical insights into the fentanyl supply chain, from Chinese origins of key precursor chemicals to the efforts of foreign narcotic traffickers to smuggle fentanyl and other drugs toward the United States.

702 has also helped us to uncover despicable atrocities committed by Russia in Ukraine, including the heinous murder of noncombatants, and the forced relocation of Ukrainian children to Russia.

In every facet of our foreign intelligence mission, 702 is critical. And that's not just an exaggeration.

Last year, nearly every item in the President's Intelligence Priorities list was addressed in some way, shape, or form by 702. It's not replaceable. NSA could not replicate intelligence from 702 using other authorities. It's agile, specific, and efficient.

The compelled assistance of U.S. electronic communication service providers means that for certain key requirements, we can avoid sending our officers into overseas hostile areas to mount risky collection operations.

It means that we can rapidly acquire information about targets in remote and denied areas of the world where the intelligence community has little or no accessibility.

It means that when we see a target changing their behavior, we can adapt quickly, ensuring that we do not miss critical leads and details.

And importantly, it means that we get narrowly tailored information, the data of specific foreign targets located overseas communicating information of foreign intelligence significance and value. All in a manner defined by the law guided by the National Intelligence Priorities Framework and scoped by the specific certifications approved annually by the FISC.

Finally, I'll talk a bit about compliance. NSA has a deep culture of compliance. I'm proud that our workforce is so dedicated to compliance with all the laws and policies that we follow, and those that govern our sacred mission, including 702.

The DOJ's review and assessment determined that NSA's 702 targeting decisions have been over 99 percent compliant since the last reauthorization. In large part, because we have a robust compliance program, including hundreds of dedicated compliance professionals working hand in hand with analysts.

Our compliance team is part of each stage of the analytic process, from the initial targeting decision to the review of the responsive content supporting the mission and ensuring that our culture of compliance is maintained day in and day out.

Thank you for the opportunity to discuss 702, and what it means to NSA. And I'd like to turn next to my colleague, David Cohen, from CIA.

[The prepared statement of Mr. Barnes appears as a submission for the record.]

Chair DURBIN. The CIA Deputy Director, Mr. Cohen, you may proceed.

**STATEMENT OF DAVID S. COHEN, DEPUTY DIRECTOR, CENTRAL INTELLIGENCE AGENCY**

Mr. COHEN. Good morning, and thank you, Chairman Durbin, Ranking Member Graham, and Members of the Committee for inviting me to discuss this important topic, and to represent the men and women of the Central Intelligence Agency.

The information the CIA derives from FISA 702 collection is, quite simply, indispensable for CIA to perform its mission. It allows us with precision and with care for the rights of the American public that we serve to gain authoritative, timely, and actionable insights into the full range of national security threats and foreign policy issues confronting our Nation.

I thought it would be most useful for the Committee to focus my opening remarks on some of the ways that CIA uses FISA 702 collection every day to do our job. I'll focus in particular on how we use 702 in our overseas clandestine collection and counterintelligence operations, in preparing all-source analysis for policymakers here in Congress and in the administration, and as part of a Governmentwide response to the fentanyl crisis.

First starting with our operations. As I'm sure you know, one of CIA's core missions is to operate clandestinely overseas to collect intelligence from individuals we've recruited. These individuals, our assets, often risk their lives and the lives of their families to provide information to CIA officers to help the United States. And my officers who spot, assess, develop, recruit, and meet with these individuals often put their lives, their safety, and their well-being at risk to do their job.

Because human intelligence operations carry a great deal of risk, we often think about human intelligence, or humans, as the collection of last resort. The means of collection we turn to when no other source of collection can deliver the information we need to keep this country safe. Once we've reached that point, once we know a human source is necessary, we have to find exactly the right person among hundreds, maybe thousands of potential candidates.

FISA Section 702 helps us find many of these individuals, these potential sources. And it allows CIA officers to do their jobs faster

and with less risk. Once we have an operation underway, 702 collection helps us keep those operations secure by allowing us to identify threats early, and to provide real-time monitoring during our most dangerous operations.

CIA officers face unique challenges and threats from all sorts of nefarious actors, from hostile intelligence services trying to identify our officers and our sources, to terrorist groups who seek to harm, or even kill them.

We take very seriously our responsibility to protect our officers and the people who put their lives on the line to work with us as sources. 702 is quite simply a key tool in our arsenal to help keep both our officers and our assets safe.

Section 702 collection plays a critical role in our analytic mission, ensuring we can provide the best possible all-source analysis to policymakers in the administration and in Congress. CIA analysts leverage intelligence from every source available: open source information, humans, imagery, signals intelligence, and 702 to prepare this analysis.

Information collected under 702 is a key piece of that all-source puzzle, and a particularly important one because of its timeliness and precision. The statistics bear this out.

As I'm sure you know, one of our primary analytic publications is the World Intelligence Review, known by its acronym, the WIRe. It is provided across the executive branch and to Congress.

In the last year, nearly 40 percent of our daily WIRe articles contain at least one intelligence report derived from 702 collection.

In our other analytic products for Congress and the administration, including the Presidential Daily Brief, the numbers are similar.

Section 702 is, put simply, a critical component of much of CIA's analytic product across the gamut of national security and foreign policy issues.

The third way we leverage 702 is to support broader U.S. Government efforts against foreign-based drug trafficking organizations. 702 collection illuminates the networks and global supply chains used by foreign-based drug trafficking organizations. This includes how they manufacture and transport everything, from precursor chemicals to their foreign labs, to their distribution of their product into the United States. As we gain this insight, we're able to support and partner with foreign governments to take action.

Most recently, 702 has proven critical in helping us counter the fentanyl threat, which, as I'm sure this Committee is aware, is responsible for the deaths of nearly 100,000 Americans every year.

Without 702, we would be missing essential information on the dangerous groups and individuals behind overseas fentanyl production and distribution. And CIA's ability working with and through our partners to stem the flow of fentanyl into our communities would be greatly diminished.

I hope these three examples illustrate some of the ways that we at CIA rely on FISA 702 collection every day. It is, as I said at the outset, indispensable for our work. I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Cohen appears as a submission for the record.]

Chair DURBIN. Thank you, Mr. Cohen. Next we have FBI Deputy Director, Mr. Abbate. I hope I pronounced your name correctly.

Mr. ABBATE. Yes, Senator.

Chair DURBIN. Please proceed.

**STATEMENT OF PAUL ABBATE, DEPUTY DIRECTOR, FEDERAL BUREAU OF INVESTIGATION**

Mr. ABBATE. Thank you, Chair Durbin, Ranking Member Graham, and Members of the Committee. It is a privilege to be here because of the immense importance of this topic, and the discussion to follow, and for the opportunity to have it in this public setting as this distinguished panel of colleagues has already done a thorough job of covering so much of what is vitally important about the collective FISA Section 702 authority.

I will try to provide insight into the FBI's use of the tool, how we act based on the critical intelligence gleaned from it, and the actions we have taken, and continue to take, to ensure strict compliance with its use.

With respect to the threats we face, as you are all aware, Section 702 is invaluable within our cyber program as it counters malicious activity from adversaries such as China, Russia, Iran, North Korea, among others. It is also a critical authority for the counterintelligence program which relies on it to thwart the work of hostile foreign intelligence services, including each of the lawless authoritarian regimes just mentioned.

And our counterterrorism operators depend on it to stop foreign terrorists, those who detest American values, freedom, and our way of life. And who seek to attack our country, take lives, and cause harm. As we've learned from the past, if the 702 tool is lost, and we have to rely on traditional FISA moving forward, it would be next to impossible to keep pace with the foreign threats we face today.

With that, we know many very real and legitimate concerns have been raised about the Bureau's use of 702, particularly as it relates to querying the limited subset of 702 data relating to the FBI's national security investigations.

I want to be clear about my own views on the compliance incidents that were cited in the FISA Court's opinion from last year, which was just recently declassified.

They are wholly and completely unacceptable, and they do not reflect the high standards that we seek to hold ourselves to in the FBI. I know Director Wray and the entire leadership team feel the same way.

It is important to keep in mind that all the incidents cited in that 2022 FISA Court opinion predated a set of major reforms that the FBI instituted in 2021 and 2022 that were designed to address the root causes and eliminate incidents like these, from changes in our IT systems to our internal approval processes, to training, and to accountability.

These reforms have already had significant positive impacts. We've seen a 94 percent drop in U.S. person queries overall, and our Office of Internal Auditing found a 14 percentage point increase in our compliance rate from before the reforms to after. It is now at approximately 96 percent.

What is vital to remember is that there are incredibly important national security and public safety reasons for the FBI to query U.S. persons in FISA holdings. This was a fundamental lesson derived by both the 9/11 Commission and the Fort Hood Commission.

We must share information across the intelligence community so that we can connect the dots, and then we must be able to find the relevant pieces of information in our databases in time to be able to take action to neutralize the threat.

U.S. person queries are used to identify those who are actively working with foreign terrorist organizations or hostile intelligence services with intent to harm U.S. national security and threaten the lives of those who we serve. And we also use these queries to determine if those U.S. persons are current or potential victims targeted by those foreign powers. And if they are victims, we use U.S. person queries to investigate the extent of that targeting and can use that information to protect and warn the U.S. person or organization.

But it's not enough to say that queries like these are valuable to our mission to protect the homeland. The American people and Congress also need to have trust and confidence that these queries are being done lawfully and in a fully compliant manner. It is our obligation to rebuild and to earn that trust.

As the FBI official responsible for personally approving some of the most sensitive queries, I take these compliance errors very seriously, and find them entirely unacceptable. It is difficult to express strongly enough in words how disappointed I am in these failures.

And so, in response to these and other incidents, I'm announcing today two additional new measures we will be taking to hold personnel accountable for FISA-related compliance incidents.

First, I have issued new accountability procedures which establish a three-strike policy, four-query compliance incidents deemed to be unintentional, with a range of rapidly escalating consequences. And even stronger disciplinary action for those incidents deemed deliberate, reckless, or particularly egregious. Penalties based on the facts range up to dismissal from the agency.

Second, the FBI has developed a new business health measure to hold our leadership accountable for monitoring FISA compliance within their field offices and divisions. This is one of the measures our leaders will be evaluated on when it comes time for performance ratings, awards, and promotions. Because it is not enough to simply hold the line-level employees accountable. We strive to ensure that we have accountability at every level throughout the organization.

You have an absolute and complete commitment from Director Wray and I that we will continue this progress and work within the bounds of legislative authority. Because as crucial as 702 authority is now, it will only become more important over the next 5 years as foreign cyberattacks continue to escalate in sophistication and frequency, as foreign terrorist organizations continue to reconstitute and pose resurgent threats to the homeland, and as we venture further into an era of heightened global strategic competition.

So thank you again for inviting us to this important hearing, and for your continued support of the FBI and our close partners represented here. Thank you.

[The prepared statement of Mr. Abbate appears as a submission for the record.]

Chair DURBIN. Thank you very much, Mr. Abbate. Mr. Olsen.

**STATEMENT OF MATTHEW G. OLSEN, ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE**

Mr. OLSEN. Thank you, Chair Durbin, Ranking Member Graham, Members of the Committee. As you've just heard, Section 702 is invaluable. The reauthorization of 702 is perhaps the single most consequential national security decision that this Congress will make. The stakes could not be higher.

Congress enacted Section 702 as part of a number of fundamental legal reforms following 9/11. Those attacks demonstrated that we must, one, share intelligence, and two, that we must eliminate walls between foreign intelligence collection and domestic law enforcement. I was part of the team at the Department of Justice in 2008 that worked with Congress to pass Section 702.

Congress, then, recognized that FISA, as written, created a dangerous intelligence gap, and enacted 702 on a bipartisan basis. And when Congress passed 702, it also included a number of critical safeguards for Americans.

The law, for example, prohibits targeting anyone inside the United States or a U.S. person anywhere in the world. The FISA Court reviews Section 702 procedures every year to ensure that they comply with the Constitution and with FISA. And the National Security Division, which I lead, reviews every single targeting decision that's made.

In my experience, Section 702 is a model piece of legislation, an authority that both protects national security and safeguards civil liberties. So let me address one area of particular concern, and that's the FBI's use of Section 702 information.

To use the intelligence that the IC collects lawfully, agents and analysts, quote, "query the database of FBI information." This is the small subset of 702 data that is relevant to open FBI national security investigations.

A query simply means using a term to retrieve specific information that already is in the FBI's possession. It's like searching for something in your email inbox. You don't read every single email. You probably enter a keyword to find what you're looking for quickly within what's already stored in your inbox.

And the FBI's ability to do this, to conduct these queries, is absolutely essential to its mission. For example, if the FBI learns that a spy working for the PRC has a list of U.S. phone numbers on their phone, FBI investigators may query FBI 702 data with those phone numbers—some of them may be U.S. phone numbers—to help identify others working for the PRC, or even potential victims of PRC espionage.

And this is not just hypothetical. The FBI, in fact, was able to disrupt—able to disrupt ongoing assassination and kidnapping plots, in part, because FBI investigators searched their 702 data

with U.S. person identifiers. And they were able to therefore quickly discover the nature and extent of the plotting.

In another case, the FBI was investigating a cyberattack against a critical infrastructure company here in the United States. The FBI queried its Section 702 data with U.S. person identifiers. And they found out that it was Chinese hackers that were behind the attack, and that they had compromised the network. And they figured out how they did it. It was this information that the FBI got from querying its data that allowed the FBI to alert the network operators and to mitigate the attack.

Ultimately, the FBI is the single organization represented here with the responsibility and the authority to take action inside the United States to protect our national security, whether that's to identify and disrupt terrorism attacks, espionage, or cyber threats. And the FBI's ability to quickly review its Section 702 data is an essential tool for that mission.

The FBI, however, must safeguard the rights of Americans. In recent years, we have identified and reported serious compliance issues with FBI's U.S. person queries.

And let me be clear, I join with Deputy Director Abbate. These compliance problems are not acceptable. They have eroded public trust, and I am not here to defend them.

Indeed, when we identified these problems, the Attorney General directed the FBI to make significant changes to their systems, and their policies, and their training. Changes that have already proven effective in improving compliance. But this is an ongoing process, and as the deputy director testified, the FBI is imposing new measures for compliance, and new measures for accountability. And we are continuing to review the FBI's performance for ways to improve.

We are committed to working with you and with the rest of Congress on potential reforms. As we work with you on this effort, we must ensure that any changes we make also preserve Section 702's essential effectiveness as a national security tool.

In the end, we must not forget the lessons of 9/11. Unduly limiting the FBI's ability to access lawfully collected information, and imposing artificial barriers between foreign intelligence and criminal investigations will set us back decades. It will put our Nation at grave risk.

Section 702 has proven to be an irreplaceable authority that enables our entire intelligence community to work together, to collect, and to share, and to use the information that's necessary to protect our country. Thank you.

[The prepared statement of Mr. Olsen appears as a submission for the record.]

Chair DURBIN. Thank you, Mr. Olsen. Before I start the questioning, I'll recognize Senator Graham for an opening statement.

**OPENING STATEMENT OF HON. LINDSEY O. GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA**

Senator GRAHAM. Thank you, Mr. Chairman. I'll be very brief.

The Committee has heard pretty jarring testimony from people in the intelligence and law enforcement space that if Congress fails to reauthorize 702, that the country would be much at risk. And

this program has been used to identify some pretty bad actors and take action on behalf of the United States.

The abuses that you talked about—I'll talk to you about in a minute.

But I guess what I'm trying to tell my constituents back home, the threats to the country are growing. They're not lessening. The ISIS–al-Qaeda footprint is coming back. China's up to no good at every front. The Iranians are threatening to kill former members of the Trump administration, and many of us have been briefed by the FBI based on pickups you've had regarding threats against us. And I would imagine that came from 702.

That's the need for it. The downside is that it's been abused, and there's a warrant requirement to investigate an American citizen for potential wrongdoing. And we don't want this to be used to get around a warrant requirement. So bottom line is let's reauthorize this program and build in some safeguards.

Chair DURBIN. Thank you, Senator Graham.

Before I begin my questions, I want to remind my colleagues that following this open session, we'll have a closed session—SVC 217 at 12 p.m. today—where you can pose questions that may not be able to be answered in open session.

I'd like to start with questioning by just noting the following. I listened to how this program was described by our witnesses. Mr. Fonzone described it as an elegant program. Mr. Barnes described it as agile and specific. Mr. Cohen referred to precision. Mr. Olsen, that it was irreplaceable, and invaluable, and so forth.

But since the last reauthorization of Section 702 in 2017, many violations of the constitutional, statutory, and court-imposed restrictions on Section 702 have come to light.

Last month, an unsealed Foreign Intelligence Surveillance Court, or FISC, opinion revealed that the FBI conducted improper searches of 702 databases for American communications 278,000 times—278,000 times. These searches have affected all manner of Americans such as individuals listed in police and homicide reports, including victims, next of kin, and witnesses to the crime.

One hundred thirty-three people were arrested during the 2020 Black Lives Matter protest when, as Justice Department itself concluded, quote, "there was no specific factual basis to think the searches would turn up foreign intelligence."

And 19,000 donors to congressional campaigns when, quote, "the only 8 identifiers used in the query had sufficient ties to foreign influence activities to allow such a search"—8 out of 19,000.

Mr. Abbate and Mr. Olsen, you both testified regarding the remedial measures that have been implemented or are underway. But why should Congress or the American people trust the Executive to comply with the law this time in light of this track record?

Mr. OLSEN. Thank you, Chair Durbin. I'll first take the question, and then pass it off to the deputy director.

As we both said, the problems that you've cited, and that we've identified in our reviews of the FBI queries are not acceptable. And I don't defend them. I'm not here to do that. What I can tell you is that those problems predate the critical remedial measures that were put in place in 2021 and 2022.

In particular, the FBI made a simple change to its system at the Attorney General's direction. Instead of—by default, when there was a query conducted by an FBI analyst or agent searching all of its data, including FISA, raw FISA, and 702 data, it simply switched that to a default opt-in.

So that from that point forward, starting in 2021, the FBI agent or analyst had to actually affirmatively take the step of saying I'm going to conduct a search using a U.S. person identifier. And then, say why that was reasonably likely to return foreign intelligence information.

And it was that single change that has resulted primarily in the reduction of the number of U.S. person queries by 93 percent from 2021 to 2022.

So, it was at—it wasn't—again, these changes, or these problems, these mistakes were not intentional. They were inadvertent. They're not defensible. But they were addressed largely by just simply requiring an affirmative step to search that data because most of those searches were inadvertent.

You know, and if I made one other point on the 278,000 number within the court opinion that you cited. Obviously, that's a huge number.

The one thing to put that in some context—the one response to put that number in context, that doesn't represent a single—each one of those a single wrongful query. Many of those queries were batch queries. In other words, multiple queries by one mistake. One agent making a mistake. In fact, one of those errors accounts for over 100,000 of the 278,000. So I think it's important to put that number, again, in context. Again, not to defend or to excuse that mistake.

Chair DURBIN. It's been a source of frustration since the creation of this program to get adequate accountability for the numbers, either on the positive side or the negative side. And you have to, I hope, understand why some of us are skeptical at this point that 278,000 doesn't mean 278,000. I'm not sure where you're going with that.

Let me just ask the basic fundamental question in the few seconds I have left. Is the skill of our adversaries and the potential destruction that they could bring to us by their malicious acts really made the Fourth Amendment something that we have to question whether we can follow it in the 21st century?

Mr. OLSEN. Again, I—the FBI is committed, the Department of Justice is committed to ensuring the safeguards are followed with regard to 702. There is no diminution of the Fourth Amendment when we're talking about U.S. person queries.

In other words, the answer to your question is, we do not need to dispense with the Fourth Amendment. The Fourth Amendment applies fully to everything we do. In fact, it's the hallmark of the work that we do when we investigate and prosecute cases, is to follow the Fourth Amendment along with the rest of the Constitution.

The courts that have looked at this—have looked at FISA 702 and FBI queries, no judge has said that there is a Fourth Amendment requirement for the FBI to query the data that's already lawfully collected. In fact, the courts that have looked at it have said there is no Fourth Amendment violation or requirement. There cer-

tainly are privacy implications here, and that's why we've adopted the changes that we've talked about. And that's why the FBI has today announced additional compliance measures which, again, are already proving to be effective.

Chair DURBIN. I can't go any further because I've run out of time. But I will tell you that if the reforms that you've mentioned in 2021 and 2022 are the only reforms that you're bringing to this Committee as we discuss the future of 702, I've got to see more. I hope there is more that you can present. Senator Graham.

Senator GRAHAM. Thank you, Mr. Chairman. I'll just ask the panel to raise your hand if you agree with the following: The United States is an undeclared state of war against ISIS and al-Qaeda. You agree with that or not?

[Laughter.]

[All of the witnesses raised their hands.]

Senator GRAHAM. Okay. All right. I think you raised your hands.

[Poster is displayed.]

Senator GRAHAM. That the Communist Chinese Party is hell bent on infiltrating as many systems in America as possible? Okay.

So let's talk about—I don't know if there's anybody named John Doe out there, but I don't know why you would name your kid John Doe. So let's talk about John Doe. If John Doe is suspected of working with the Chinese or some terrorist organization, do we all agree you'd have to get a warrant against John Doe if they were an American citizen?

Everybody nods their head. Right?

If you think some American is colluding or working with some foreign power that would be a crime, then you'd have to get a warrant to investigate them. Do we all agree with that? Okay.

702. This is about foreign persons outside the country. Is that correct? We're surveilling foreign people outside the United States not to solve a crime but to find out if they're up to no good in terms of intelligence-gathering threats to the country. Is that correct?

Here's the rub. You pick up a phone on the battlefield somewhere, and there's a bunch of names in that phone or numbers in that phone. I think you talked about this, Mr. Abbate. But let's just say you capture a terrorist somewhere overseas, and you have a mobile device, and on that device there are names of Americans or numbers of Americans. What happens next?

Mr. ABBATE. We're going to quickly take those numbers, Senator. We're going to run them against the holdings——

Senator GRAHAM. Without a warrant?

Mr. ABBATE. If we're talking about FISA 702?

Senator GRAHAM. Yes.

Mr. ABBATE. Yes. If it's obtained from a foreign terrorist——

Senator GRAHAM. Yes.

Mr. ABBATE [continuing]. Absolutely.

Senator GRAHAM. So the idea of not looking at those numbers is absurd. Why wouldn't you want to look at those numbers? Doing it in a constitutionally sound manner is what we're talking about. So what would you do? You would ask the system what?

Mr. ABBATE. We would be looking connections around the world and specifically in the United States. We would want to know if that terrorist is working with someone——

Senator GRAHAM. So if he called——

Mr. ABBATE [continuing]. In the United States.

Senator GRAHAM [continuing]. John Doe in Cleveland, Ohio, and you pinged the system, and there is communications between the terrorist's device and John Doe in Cleveland, Ohio, what would you do next?

Mr. ABBATE. We would do all the investigative steps that you would expect. Physical surveillance——

Senator GRAHAM. Would you have to get a warrant?

Mr. ABBATE. If we were going to seek technical surveillance on the U.S. person, absolutely we would.

Senator GRAHAM. Okay. So if a terrorist is talking to someone inside the United States, and we pick it up from 702, if you want to follow the American on the other end of the phone, you'd potentially have to get a warrant. Is that correct?

Mr. ABBATE. Yes, Senator.

Senator GRAHAM. Okay. But just asking the question about whether or not there was a contact does not require a warrant? Does that make sense?

Mr. ABBATE. Yes.

Senator GRAHAM. Okay. So if an American is involved with a foreign person overseas, and there's evidence of an American being involved—we don't know what the nature of the involvement is, we'd like to know more—you can ask the system. But if you're really focusing on the American as being up to no good, you have to get a warrant. Is that fair to say?

Mr. ABBATE. That is correct, Senator. Once the focus turns to the U.S. person, the person inside the United States.

Senator GRAHAM. The only reason I mention this is that 702 is not designed to avoid a warrant requirement against people you have to get warrants for. Is that correct? The goal of 702 is to find out about what bad guys or bad girls may be up to overseas regarding us here at home, our interests throughout the world, and do something about it before it's too late. Is that the general nature of 702?

Mr. ABBATE. Yes, Senator.

Senator GRAHAM. Okay. Now, you're going to have to prove to this Committee that when you query about American citizens in that system, that you're not just being lazy getting around the law, and these abuses need to stop.

So count me in with Senator Durbin. I want to know more about how to have guardrails. But to the Members of this Committee, if we lose this tool, we will pay a heavy price.

Chair DURBIN. Senator Whitehouse.

Senator WHITEHOUSE. Thank you very much. Thank you all for being here. Mr. Olsen, you and I were both engaged in that 2008 initial process back when I was on the Intelligence Committee as well as the Judiciary Committee. So let me just join Mr. Abbate in his feelings of dismay that these errors have been allowed to take place. I've been a constant supporter of 702, and it's very frustrating, years into the process, to have these errors continue.

You've mentioned, the panel has mentioned the role of 702 in finding out about atrocities committed by Russia in Ukraine. Can

you tell me if that information has yet been shared with the International Criminal Court?

Mr. OLSEN. I'm not sure. I defer to my colleagues about whether it has or not. Yes.

Senator WHITEHOUSE. The reason I'd like an answer to that is that this Committee, Senator Graham, Chairman Durbin, saw to it that a law was passed lifting the ban on cooperation with the International Criminal Court as it regards, specifically, Russian atrocities in Ukraine.

And our understanding from the last conversation we had was that the Department of Defense was stopping the executive branch from complying with that law passed by Congress.

And if that is still the case, then we'd like an answer to that. So can we get an answer to that in a timely fashion for the Committee?

Mr. OLSEN. Yes.

Senator WHITEHOUSE. It's the law of the country for the executive branch to cooperate with the International Criminal Court as regards the investigation into Russian crimes. The failure of the executive branch to abide by that law, I believe, because of the recalcitrance of one agency, just isn't consistent with the way things are supposed to work in our democracy. So I hope that we've put an end to that problem or solved it. But if not, we're going to continue to press on that question.

Mr. Olsen, there are three areas that we've talked about with regards to 702 that are not presently in the 702 statute.

One is its use to pursue the international organizations that are responsible for bringing fentanyl into the country and for thousands of American deaths. You are currently using the program to target those organizations. Correct?

Mr. OLSEN. The program is being used, Senator, for the purpose of gaining intelligence on fentanyl distribution focusing on individuals and groups outside the United States who are not U.S. persons.

Senator WHITEHOUSE. So let me make a recommendation that you add to 702 a specific authorization for that purpose. I think that would be welcome.

Second, you've announced a considerable number of repairs and reforms, including the FBI unclassified congressional notice that we received today. Those are all being accomplished administratively. Correct?

Mr. OLSEN. That's correct, at this point.

Senator WHITEHOUSE. I would strongly recommend that you take as many of those as you feasibly can and bake them into the law. So work on an amendment that incorporates those reforms so that it now is part of the 702 law that we will be voting on.

The third is that you have mentioned the role of 702 in supporting American victims of foreign intelligence breaches. Very often it's a company that is having information stolen out of it. Often, by PRC-related entities. And the way you find out about it is that through 702, you pick up the contact with the American company. Now you have the ability to go to the American company and say, "Hey, you have a problem," and help them defend themselves. Is that an accurate description of the way that transpires?

Mr. OLSEN. Absolutely. Both through direct means as well as cyber means is the way we've seen those types of intrusions occur.

Senator WHITEHOUSE. Yes. So I would also recommend that you add to 702 specific authority related to the support for American victims. There's no reason that should hide that aspect of the program under a bushel. And once it's part of the program, there's no doubt that that's a legitimate way for the executive branch to proceed. With that, my time is up. I thank you, all, for your service and yield back to the Chairman.

Chair DURBIN. Thanks, Senator Whitehouse. Senator Grassley.

Senator GRASSLEY. Mr. Fonzone, you can't have meaningful discussions about reauthorizing 702 when Government reports and court opinions are heavily redacted and hidden from the public. Will you commit to declassifying information about the FISA abuses and procedures before the 702 reauthorization deadline? And if you can't say yes to that, why not?

Mr. FONZONE. Yes, Senator. Thank you. I think we—we have recently released a FISC opinion that released—that declassified a bunch of information. And the law already requires us to review FISC opinions for declassification and release them to the public. And we're committed to making more information public about Section 702 to assist Congress and the public in its consideration of renewing this authority.

Senator GRASSLEY. Mr. Olsen, I heard you say in your opening statement about processes you're taking to make sure that people that abuse this process are going to be held accountable. You heard about the 278,000 times that it was violated. What is the Justice Department doing to punish folks who have already abused FISA?

Mr. OLSEN. Senator, thank you for that question. And, again, compliance includes rules and procedures. But it only works if you have accountability.

And that's why the FBI has instituted a comprehensive approach to accountability for the agents and analysts who use FISA but abuse the rules. It's on a spectrum for intentional misuse. Agents and analysts can be fired. In fact, one person was fired for wrongfully violating the rules intentionally with respect to FISA.

But the vast majority of the mistakes we've seen are not intentional. And the FBI has announced today—Deputy Director Abbate talked about a three-strikes approach of escalating penalties that include notes in a personnel file, loss of access to FISA data, and other measures, including retraining to ensure that individuals are tracked over time if they're repeat offenders. So there's, again, a range of repercussions and discipline. And I know the deputy director and the director of the FBI take this very seriously.

Senator GRASSLEY. Okay. Mr. Abbate, I'd like to have you describe for me the process and procedure that the FBI should normally follow when receiving criminal allegations from a trusted FBI source that an office holder engaged in bribery. For example, if the allegations include reference to evidence that would prove or disprove the bribery scheme, would standard operating procedure require the FBI to seek out that evidence?

Mr. ABBATE. Senator, in any instance where we receive information, an allegation, or a complaint, you know, we apply the standards and the Attorney General guidelines, and our DIOG, and de-

termine whether the information received, the allegation, or the complaint meets the threshold for the opening of an investigation.

We consult appropriately with our field office, with our program management elements at headquarters, with our Office of General Counsel, and then we take it from there based on the information whether it meets the standard.

Senator GRASSLEY. So that's the investigation process that should have been followed with respect to the 1023. Apparently, that process wasn't followed. For the sake of restoring credibility, the FBI must explain itself sooner rather than later.

Mr. Olsen, this is my last question. The Washington Post reported your involvement in Mar-a-Lago raid. It wrote that, quote, "FBI agents on the case worried that prosecutors were being overly aggressive," and further, quote, "Olsen appealed to senior officials in FBI headquarters to push their agents to conduct the raid." Did you communicate with senior officials at FBI headquarters to push their agents to search Mar-a-Lago?

Mr. OLSEN. Senator, our solemn responsibility in every case is to follow the facts, and the law, and to do so without fear or favor. We are absolutely committed to the impartial administration of justice, and to upholding the rule of law, which includes applying the law equally to everybody. As I'm sure you can appreciate, that matter is under the auspices of the Office of the Special Counsel——

Senator GRASSLEY. Is The Washington——

Mr. OLSEN [continuing]. And I'm not going to comment further on it.

Senator GRASSLEY. Is The Washington Post right or wrong?

Mr. OLSEN. That's a matter that's pending, and it's an ongoing matter, and it's being handled by the Office of the Special Counsel. So I'm sure you can understand that I'm not going to comment further.

Senator GRASSLEY. Thank you. I yield.

Chair DURBIN. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you, all of you, for your good work.

I'll start with you, Deputy Director Cohen. I know Senator Whitehouse asked you—asked Mr. Olsen about the use of 702 when it comes to drug trafficking. And I wanted to kind of dig down on that just because we're seeing more and more fentanyl kill people, and also more available on the internet. Sometimes, many times, unknowingly, when people are purchasing other pills that shouldn't be on those platforms.

Without getting into specifics, how is data collected under Section 702 been used to disrupt trafficking networks, and prevent fentanyl and its precursor chemicals from entering our communities? What work is being done?

Mr. COHEN. Thank you for that question, Senator Klobuchar. So we use Section 702 collection on foreign persons overseas, query the database to identify individuals tied to organizations that are involved in drug trafficking and fentanyl production in particular.

It helps us illuminate where the precursor chemicals are coming from. Often from China. How those chemicals get to overseas. Oftentimes to Mexico. Not invariably, but oftentimes to Mexico. As well as how some of the pill presses that are used to manufacture

fentanyl are acquired. Again, overseas, and brought into Mexico for use including by, you know, organizations such as the Sinaloa Cartel.

Senator KLOBUCHAR. I think that's really——

Mr. COHEN. That really helps us——

Senator KLOBUCHAR [continuing]. Important to know for those just talking to families of lost kids who purchasing drugs on the internet, that the platforms are being used——

Mr. COHEN. Yes.

Senator KLOBUCHAR [continuing]. By these cartels. You don't have to go into that. But these cartels are actually involved in this. So it's not like they can get all their justice in the U.S. And in order to stop this, we're going to have to stop it from coming in—the ingredients and some of the other substances. Is that correct?

Mr. COHEN. That's correct, Senator.

Senator KLOBUCHAR. Okay. Deputy Director Abbate, I appreciated Senator Durbin's words about making sure that these reforms continue, and that they are. I appreciated what you announced today, and that there'll be changes to the existing 702 authority.

Could you talk about how the reforms the FBI implemented resulted in measurable improvements in the FBI's compliance? Number one. And then number two, is there a lag in the publicly available data such that the most recent FISC Section 702 certification does not accurately inform the public?

Mr. ABBATE. Thank you, Senator. Yes. With respect to the reforms that we've already put in place—as the Assistant Attorney General noted—we've seen significant progress. Just the one that Mr. Olsen cited on having our personnel opt in year over year resulted in a 90-something percent decrease in overall U.S. person queries.

So we've seen significant progress there along with the other reforms that we've implemented on batch queries which are anything more than one. We had put in place a requirement that for any batch queries over 100, it would require attorney review from our Office of General Counsel. I've taken that even further now because I saw some recent examples, again, where I was disappointed in the compliance error. So we've actually cut that down now so that any batch query of any number is going to require attorney review from our Office of General Counsel going forward.

We're also requiring written justifications for our personnel when they're endeavoring to make a U.S. person query. And we're going to continue to iterate on that. We view it as an ongoing process, and we're open to any and all further reforms in working with the Committee and Members here. And we're not going to stop until we've achieved 100 percent compliance.

Senator KLOBUCHAR. Okay. I was going to ask Mr. Olsen if you wanted to add anything. But before that, quick, how has the FBI used Section 702 to critical infrastructure and businesses to protect them from ransomware and other cyber threats? Because we certainly have been seeing a surge in those.

Mr. ABBATE. Yes, Senator, as we said, it's a vital tool. Some examples have already been provided with regularity that we see that. It's helped us literally identify potential victims, and victims

in the United States—both individuals and companies who are either being targeted for cyberattack, or in the midst of an attack, or already have been.

It's allowed us to get in front of that, particularly with regard to our critical infrastructure to warn victim companies before they're hit and prevent the harm from occurring from adversaries like China, Russia, Iran, North Korea. And it's been—without it, we would not have been able to have achieved that goal——

Senator KLOBUCHAR. Okay, because you've——

Mr. ABBATE [continuing]. And to protect our country's——

Senator KLOBUCHAR [continuing]. Had some major prosecutions. Could I just ask Mr. Olsen? It appeared he had something you wanted to add on the reform front.

Mr. OLSEN. If I may, just two quick points, Senator. One on your cyber question. One example is the notorious Colonial Pipeline attack where 702 collection helped us both identify the hacker, and it enabled us to recover most of the ransom money that had been paid.

Senator KLOBUCHAR. Mm-hmm.

Mr. OLSEN. Second, your question about the certification and the FISC opinions.

Senator KLOBUCHAR. Yes.

Mr. OLSEN. There is a 2023 opinion that is now going through the declassification process that will come out shortly, and which does identify some additional improvements in FBI compliance. Not 100 percent. There are still problems and things that we're still working on. That's part of the deal. But it does identify that the FBI has continued to improve its compliance over the past year.

Senator KLOBUCHAR. Okay. Thank you very much.

Chair DURBIN. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman. I haven't heard anyone say that 702 is not essential to our national security, and I believe that it is essential to our national security. So I'm delighted to hear that people are saying that—not claiming that we can do away with it.

But what you're also hearing is, is a lot of skepticism, even distrust of the intelligence community based on abuses that have been well documented. And, as you know, once that trust is lost, it's hard to earn it back.

So we're at a little bit of a crossroads here. I'll remind you that it was just a few years ago where we tried to reauthorize Section 215 of the Foreign Intelligence Surveillance Act and were unable to build a political consensus to do that.

So I do believe your testimony that this is important to our national security. So the question is, how do we work together to regain the public's trust, and the confidence of Members of Congress who'll be asked to vote in favor of some reforms?

Mr. Abbate, just—you've talked about the work that's been done at the FBI. And I had the opportunity to go look at how the FBI's reforms—not the ones you mentioned today, but the others in terms of querying FISA information—how those work. Would you have, or the FBI Director have any objection if those reforms that you've announced, that the FBI has announced, were codified and written into the law, as opposed to just policies of the agency?

Mr. ABBATE. Thank you, Senator, first for visiting with us at FBI headquarters, and taking the time. We would not have any objection at all from the FBI standpoint to codifying any and all of the reforms that we put in place, and future ones, as well.

Senator CORNYN. And Mr. Abbate, I was struck by the fact that when the FBI is doing an investigation, an agent's not just sitting down and doing a query of foreign intelligence information lawfully collected. You're actually engaged in querying more than 100 different databases. Is that correct?

Mr. ABBATE. Yes, Senator. I don't know the exact number of databases, but we do have quite a few.

Senator CORNYN. And so this is not agents sitting down and just looking at foreign intelligence surveillance. They're looking for all the data points to be able to put together an investigation into potential intelligence vulnerabilities or to pursue perhaps crimes.

So there has been some suggestion—and I'll throw this open maybe to Mr. Olsen. There's something known as Executive Order 12333, which, again, by definition is something that the President of the United States has done without congressional input or interaction.

But there's been a question raised as whether—if 702 were to go away, does Executive Order 12333 provide the tools necessary to protect our country?

Mr. OLSEN. I'll answer, and maybe Mr. Fonzone might have an answer to this, as well, in his role as General Counsel for the DNI. But the short answer, Senator, is no. And the reason the answer is no, and flatly no, is that Executive Order 12333 does not allow for the critical piece that 702 does. And that is compelling the support and compliance of private electronic communication service providers.

In other words, the real genius behind Section 702 was, yes, it's focused outside the United States on non-U.S. persons. But it also allows the Government to compel the assistance of a provider inside the United States, which are often the ones that are providing support or, you know, communication support to the individuals that we're targeting outside the U.S.

Senator CORNYN. Mr. Cohen, obviously, Congress is very much engaged on a bipartisan basis in supporting the Ukrainian people from—on the basis—in light of the Russian invasion of their country. And the other sort of major issue that seems to enjoy broad bipartisan consensus is defending our country against the aggression of the People's Republic of China. Could you speak to how 702 is important in terms of both of those matters?

Mr. COHEN. Senator Cornyn, I will say for both of those efforts, 702 is involved. I can go into more detail when we go into closed session.

But we, and with our colleagues in the intelligence community, rely on 702 to identify foreign intelligence information that is useful for our analytic work in providing products to Congress and to the administration in the Ukraine context to understanding what's happening there, as well as a whole host of products that we write with respect to the challenge that we're facing from the People's Republic of China. But I'm happy to go into more detail in the closed session.

Senator CORNYN. Thank you. Thank you.

Chair DURBIN. Thank you, Senator Cornyn. Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman. I will be interested in hearing how 702 has been useful with respect to both Ukraine and China. I can certainly understand as to China. I wonder if you could give us a little bit more, even in this public setting, about how it's been important to our assistance to Ukraine and its fight against Russia's criminal murderous aggression.

Mr. COHEN. Senator, let me—let me take a shot at that. But mindful that I do think that some of the real substance would be better discussed in closed session. So, what I will say—and picking up a little bit on the answer to the prior question—is that our adversaries, whether they're Russians, Chinese, Iranians, North Koreans, terrorist organizations, make use of U.S. communications service providers.

And if there is a reason for believing that we have a, you know, some foreigner operating overseas who is using a communication service that is provided by a U.S. service provider, we are more likely—the NSA will target that foreign person overseas to collect the intelligence that's—collect those communications.

We can then query the database of information that is collected on those foreign persons overseas. We run queries, NSA runs queries, obviously the FBI runs queries against this database of information that is collected when it is reasonably likely to retrieve foreign intelligence information.

And we do that in the Ukraine context. We do that in the context of the People's Republic of China, and in other contexts where we have national security concerns.

Senator BLUMENTHAL. And in the Ukraine context, we can play a part in supporting Ukraine through sharing our intelligence. Correct?

Mr. COHEN. There's a whole host of ways in which we're supporting the Ukrainian government with intelligence sharing, and, you know, it involves, you know, the full swath of collection that the United States is involved in.

Senator BLUMENTHAL. Let me ask you, as you may know, and I think we've talked about it in our conversations in my office. I've been a longtime advocate of some more robust adversarial process within the Section 702 FISA procedure.

In 2015, Congress took an important step in codifying the amicus responsibility. My numbers are from 2015 to 2020. There were 1,200 FISA applications, but just 19 amicus appointments. And in 2017, the only amicus at the time with significant criminal defense experience in the FISA context resigned because he hadn't been assigned to a single case.

Those numbers tell me that the present amicus process is not providing really robust or sufficient adversarial procedure, when we all know as lawyers that our justice system thrives on the adversarial procedure.

This area is the one part of our justice system where we have no such adversarial process because the subjects of 702 collection likely will never learn that they've been the subject of this process. So what is your position on this issue? I think I know what it is, but I'd like you to state it for the record, if you would, sir.

Mr. COHEN. Senator, is that a question for Mr. Olsen or for me?

Senator BLUMENTHAL. Whoever would like to answer it.

Mr. COHEN. Why don't, why don't I turn it over to Mr. Olsen, who——

Mr. OLSEN. I'm happy to answer that question, Senator. I represent—I lead the National Security Division and we represent the Government before the Foreign Intelligence Surveillance Court. So we're directly involved in the process that you describe.

First, we are open to reforms, as I said at the beginning, that preserve the essential effectiveness of Section 702. So if there are reforms, for example, to the FISA Court process, we're happy to engage with you and other Members of Congress as we think through how those would work.

When it comes to the amicus process, the FISA Court can ask for an amicus to be appointed in any case. And they do so in any case involving a novel or complex interpretation of FISA. And that's the cases that are the hard cases where they do have an adversarial process through the amicus appointment.

The vast majority of FISA applications are basically the same as the ex parte process that occurs in a Title III criminal application, which is not an adversarial process, but rather criminal matter.

Senator BLUMENTHAL. It's not, but eventually there is likely to be a challenge.

Mr. OLSEN. That's correct.

Senator BLUMENTHAL. And in this instance, there's likely to be no challenge. And so the privacy interests arise not only where there's some new major novel interpretation of law. But as you well know—you know a lot more than I do, at least—the case-by-case decisions often turn on interpretations of law that are challengeable. And that's why an adversarial process would provide a lot of reassurance, I think, to this Committee and the American people.

Mr. OLSEN. Again, we're open to having this conversation and engaging with you on this. I do—it is my view that the vast majority of FISA applications are basically facts against the probable cause standard. They don't involve novel interpretations of the law, and they are done on a level of—with a degree of urgency, you know, multiple times a week that would—that does not lend itself to the sort of adversarial back and forth process that an amicus would introduce. And it would—so there is some serious risk to having, for example, an amicus in every case.

Senator BLUMENTHAL. Thank you. Thank you, Mr. Chairman.

Chair DURBIN. Thank you, Senator Blumenthal. Senator Lee.

Senator LEE. Over the past 12½ years, I've raised significant concerns in hearing, after hearing, after hearing about FISA, and the FBI's shocking disregard for Americans' constitutional rights and civil liberties.

I've been given basically the same answer by FBI Directors, and Attorneys General, and other officials during three Presidential administrations involving both major political parties.

The answer every time is a variation, more or less, of the following: "Just trust us. Don't worry. We've got good people, law abiding people running this. And we've got lots and lots of procedural safeguards in place to prevent this type of abuse that you're

facing here." "These aren't the droids you're looking for"—that's what we're told.

Here again today [holds up document], just the last 24 hours, we got a new policy. This one's finally going to fix it, you tell us. This one—this one's going to do it.

Meanwhile, what's happened? Well, in 2019, Inspector General Horowitz issued a shocking report confirming a lot of what I had feared over the years but had found it difficult to prove. A report regarding Crossfire Hurricane, the FBI's secret surveillance of Donald Trump's 2016 Presidential campaign, and then a subsequent memorandum dealing with the FBI's failure to maintain the so-called "Woods files," which a Woods file is basically the evidentiary record underlying a FISA order request in violation of FBI policy.

Year after year, in hearing after hearing, we hear of instances of noncompliance. Including the disclosure just last month that the FBI illegally surveilled 19,000 donors to a congressional campaign, Americans participating in protests in the summer of 2020, Americans who were in Washington, DC, on January 6th, 2021, and even a sitting Member of Congress.

Hundreds of thousands of searches of Americans' private communications and information are conducted each and every year without a probable cause warrant. Frankly, without any warrant if conducted under Section 702.

Now, let me be very clear. That number should not just be going down. That number should be zero. Every, quote, unquote, "noncompliant search" involving U.S. persons violates an American citizen's constitutional rights.

And yet every year the FBI claims that we should just trust the FBI to fix the problems internally. Well, first they tell us there are no problems. Then they tell us we will fix them because we've got good people, and we've got new policies, and this time it's going to be different.

Only later we find out that the FBI conducted more and more illegal searches in violation of Americans' constitutional rights than the last time we addressed the issue.

So it's hard not to conclude that the only thing the FBI wishes it could fix here is the possibility of getting caught. This is what I find so insufferable. This is what I find so incredibly insulting.

Look, I want to echo Senator Blumenthal's point a minute ago, and I hope every American can take note of this feature of this. This is unlike other court proceedings. We call it a court, and yet it doesn't have any of the trappings of an ordinary court. There is no adversarial process.

We're told a moment ago by Mr. Olsen that it's okay. It's okay because the FISA Court has the ability to appoint an amicus anytime it feels necessary to do so. Well, why not in every case? And even if there is an amicus, what interest does the amicus have that's on par with the individuals affected?

The bottom line is you collect all this data. And then after you store all that data, some of it involving communications, the content of individual phone calls, emails, text messages, whatever it is—the content. Not just the metadata, but the content. You can do a backdoor search on that without a warrant predicated on probable cause.

That is itself an affront to the Constitution. That is itself something that is always going to lead to constitutional violations, and it must stop. We've got an opportunity this year to make necessary reforms, and we must do it.

But while we've got you here, Mr. Olsen and Mr. Abbate, why should we ever trust the FBI and the DOJ when it comes to this issue, whether under the current administration or under future leadership? Why should we ever trust the FBI and the DOJ again to police themselves under FISA when they've shown us repeatedly for more than a decade that they cannot be trusted to do so?

Mr. OLSEN. Senator, thank you for the question. Obviously, Section 702 is an invaluable intelligence tool. That's beyond dispute. It's also one that's very powerful, and it must be used responsibly. And I share the frustration that you express with the lack of compliance that we've seen in past years from the FBI. I'm not here to defend those compliance problems.

What I can tell you is that those compliance problems predate some of the very significant changes that the FBI has put in place. I will not say that compliance problems will be zero next year. We are not saying, as I think you mentioned, that we'd say we're done. This is an ongoing process. We will continue to try to improve. We will work with you, and your staff, and other Members of Congress to make sure that we're implementing procedures and policies, training, and other measures to continue to drive down these errors and compliance problems.

But in the end, the tool itself is so incredibly important to our national security that I believe that its essential effectiveness must be preserved.

Senator LEE. Mr. Abbate.

Mr. ABBATE. Senator, thank you. I share your concerns as well, and I take this seriously. And with regard to the FISA 702, since I've been in this role and under the leadership of Director Wray, we've made significant changes. Ones that have never been made before, and there has been a lot of progress. But we're not going to rest on our laurels. We're going to keep driving ahead, continue to implement reforms as required, taking guidance and counsel from the Committee and other Members.

With regard to Crossfire Hurricane, what happened there was wholly unacceptable. We agree with the findings set forth by Inspector General Horowitz and Special Counsel Durham.

We've acknowledged that in the past, and going—that's 2017 and earlier, that conduct occurred—not under Director Wray's leadership or when I was in this position.

We have an entirely new leadership team. We've implemented very strong corrective actions. The poor decision-making, the grave errors of judgment, the misconduct, the——

[Gavel is tapped.]

Mr. ABBATE [continuing]. Lack of rigor, investigatively, that occurred there, totally unacceptable. We reject it.

We hold people accountable for that now. And everything that we've done on the work, on the mission since that time, we've worked to avoid those mistakes, and apply the lessons learned of the past. And anyone we find who goes against that, they are not

going to work in the FBI and they will be held accountable for that period.

Senator LEE. Great to know. Congress has got to fix this problem and stop trusting the surveillance state to fix it. It can't. It won't. We know that because it hasn't.

Chair DURBIN. Thank you, Senator Lee. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman. Mr. Chairman, I share your concerns about the—regarding U.S. person queries without warrants, and the concerns expressed by a number of my other colleagues.

So this is one of the reasons that I have not been able to vote for reauthorizing 702. And when I am thinking about a warrant in this context, I am thinking about something much less involved than a typical FISC order, and much more like the search warrants that are issued in countless courthouses in our country every day.

Last year, Federal magistrate judges considered over 140,000 search warrants. Probable cause is not a high bar, and magistrate judges are used to evaluating it. Different provisions of FISA already allow Federal magistrate judges to issue certain FISA orders, and I would support discussion about expanding that authority to this context.

For Mr. Olsen, so you've had a chance to—we have met to talk about why can't we have a warrant requirement. The Department opposes a warrant requirement because you argue that many of the queries are done before the FBI has probable cause.

Which says to me that if you had to meet a probable cause requirement, that would already decrease the number of applications. So do you have any reaction to the idea of using Federal magistrate judges in a warrant requirement process?

Mr. OLSEN. Thank you, Senator, and I appreciate the opportunity to meet with you, and your staff, and to discuss these important issues. The warrants requirement that has been discussed when it comes to Section 702, I think, is not workable, and not legally required. And let me explain why.

First, every judge that's looked at this issue, every Federal judge, including judges on the FISA Court, have concluded that a warrant is not required under the Fourth Amendment for searching the lawfully collected data that is in the FBI holding. So there's no legal requirement.

But putting that aside, because there are indeed privacy and civil liberties implications to the FBI searching with the U.S. person identifier. The fundamental problem is that such an approach would be unworkable.

And I go back to the hypothetical that Senator Graham described. Which is, assume the military, our military, obtains a cell phone in Syria. And that cell phone has 100 phone numbers on it, 30 of them are, you know, U.S. phone numbers. And the person that they get it from is a suspected ISIS member who's plotting against the United States.

There may not be, in fact, likely wouldn't be probable cause to search those phone numbers in the FBI database. But with time being of the essence, it's absolutely critical that the FBI, along with other components within the intelligence community, take those

phone numbers and determine whether or not we have an ISIS operator inside the United States who's plotting an attack.

So we would not have probable cause. We wouldn't be able to take that step. It's not legally required. And if we were required, the sheer number of such requests would simply overwhelm the system. There's no number of FISA Court judges or even magistrates who would have the clearances, for example, who could possibly manage the number of queries. So it's both not legally required, and it's not workable, and it wouldn't protect us.

Senator HIRONO. You mentioned that all of the courts that have addressed the issue of Fourth Amendment issues, that they have all found that Section 702 does not require such warrants. But I have information that that is actually not the case. I don't know what specific questions were before particular courts, but several judges, including a unanimous panel of the Second Circuit Court of Appeals, have raised constitutional concerns.

And you note that you would want a U.S. person inquiry in the instance where there is a definite connection with the terrorists, for example. But how do you justify the querying of American protesters, for example, or people who have made contributions? I think that the 702 is way too broad. It does raise constitutional questions.

And I'm just searching for some way that is not going to stop the legitimate reasons for why we need 702, but also to address the constitutional questions. And it occurs to me that maybe having magistrate judges who are very used to determining probable cause can be utilized in this regard so that we don't have the situation of protesters' information being accessed, or political contributors, that has no connection to terrorists, for example.

So, you know, I am hopeful that we can figure out a way to find some way. I think I heard you say that you're okay with some reforms. And I know that the FBI recently put in a new procedure called—well, where you record the justification for all U.S. person queries. I would be interested to know what kind of recordation is it, and who determines whether justification was there. So perhaps maybe you can give me a little bit of enlightenment as to what this record the justification is?

Mr. ABBATE. Yes, Senator——

Senator HIRONO. Mr. Abbate.

Mr. ABBATE. Yes. Within our system, the automated system, when the FBI employee who's seeking to do the query, the written justification has to be input into the system. And it's retained there in the records, and recoverable forever with respect to that query.

And we're making the system adaptations right now to fully put that into place, ensure that those records are retained, and that they're reviewable, and auditable.

Senator HIRONO. My time is up, but I would have a concern as to whether there is any kind of a third party—independent third-party person who reviews whether there was justification. Thank you——

Mr. OLSEN. If I may——

Senator HIRONO [continuing]. Mr. Chairman.

Mr. OLSEN [continuing]. Just very briefly, Senator, that's in fact, what the lawyers in the National Security Division do. The lawyers

who work for me do exactly those audits of the FBI queries—about half the field offices each year. We review all of the queries that were done, and we review those justifications—those written justifications to ensure that they meet the legal standard for searching the data. So, again, I appreciate your interest, and I look forward to working with you further on this.

Senator OSSOFF [presiding]. Senator Kennedy is recognized for 5 minutes.

Senator KENNEDY. Thank you, Mr. Chairman. I guess my comments will be directed to Mr. Abbate. Am I saying that right?

Mr. ABBATE. Yes, Senator.

Senator KENNEDY. And Mr. Olsen. Perhaps to all of you. No fair-minded person can doubt the efficacy of Section 702. But here's the problem you've got. Just when the FBI—which I think—which I think is the most effective law enforcement agency in all of human history.

Just when the—but people are people, and just when the FBI has rebuilt itself after former Director Hoover, along comes Mr. Wray's predecessor who clearly did not understand how to exercise power, either intelligently or maturely.

He decides to investigate in a public way, not only one, but both candidates for President of the United States. And to do it publicly, and to leak like the Titanic. He investigates the Republican nominee with the flimsiest of evidence that has been manufactured that he—the FBI Director at that time—didn't even bother to examine. And then he turns to the Democratic nominee with respect to her email servers, investigates her, calls a press conference, says, well, I—I, not we, I am not going to prosecute her, but—but she needs to clean up her act. She's been negligent.

And then a little time goes by, and he opens up the investigation again in a public way on the Democratic nominee. And says, I'm opening this up. And a few days later, he closes it down. Might have cost her the election.

And then we start having reports predictably come out after that. The Durham report, the Mueller report, the Horowitz report. And it did extraordinary damage to the FBI, and frankly, to the Department of Justice.

Now, Mr. Wray, who I supported to replace Mr. Comey, has said he has reformed the FBI. We just don't know how. We have no idea. I don't have any idea. I do know stuff keeps happening.

I mean, one of your agents that was involved in the Mr. Hunter Biden's investigation goes on social media, apparently for a long period of time, and trashes all Republicans. He got fired only because Senator Grassley caught him.

And all this hurts you. And it makes a fair-minded American look at this and go, "Whoa, you know, this is enormous power you have, and it can be used for the greater good, but it also can hurt people." And we've got to come up with a way to make sure that the right people are using this law enforcement tool. And that's—that's the problem you've got, gentlemen.

If I were you—I'm not. I don't have your expertise, and I thank you all for your service. But if I were you, I'd try to be coming up with a way to suggest to Congress how you can check this power that you have so that the FBI, and the Department of Justice, and

the other agencies can regain their reputation, and tell us what you think.

That doesn't mean we won't come with our own ideas. You know, Senators don't take orders. Most of them barely take suggestions, but it would be helpful to me if you would come up with your own ideas to address these concerns. Not just our concerns, but the concerns of the American people.

I don't want to live in a country where if the FBI knocks on your door, the first thing you have to do is wonder whether the agent is a Republican or a Democrat. And thanks to Mr. Wray's predecessor, that's where we are, folks. I know that's a cold issue truth, but I think that's the truth.

So I'm going to read your testimony. I need to learn more about this, but help us figure out this problem. Thank you, gentlemen.

Senator OSSOFF. Chair Durbin has stepped out and left me to chair in his stead. And I'm also going to spend my——

Senator KENNEDY. I like you better. You're doing a hell of a job.

Senator OSSOFF. Not in public, Senator Kennedy, please.

[Laughter.]

Senator KENNEDY. You're doing a hell of a job.

Senator OSSOFF. Okay. So I have the privilege of sitting on both the Judiciary and Intelligence Committees. And let me just start by saying I think there's no serious doubt about the collection value of this overarching authority. And the most important question that we need to be focused on at this hearing is U.S. person queries. That is the principal source of concern for me, and I think for many of my colleagues.

And Mr. Olsen, it's the case, is it not, that the FBI can query this database for U.S. person communications simply seeking evidence of a crime? It does not have to be a national security investigation. Correct?

Mr. OLSEN. It is correct, Senator. Thank you for the question that the FBI can search using a U.S. person identifier for either foreign intelligence or evidence of a crime. But there must be a reasonable basis to believe that there is information in the Section 702 data that would be responsive to such a query.

Senator OSSOFF. Yes. Why should there not be a warrant requirement for these searches, which are known as crime only searches, whereby FBI agents are seeking the communications of Americans either considering opening a criminal investigation or in the midst of a predicated criminal investigation? Why should there not be a warrant requirement for such a U.S. person query?

Mr. OLSEN. So stepping back for a moment, if I may, just to provide——

Senator OSSOFF. Just for a moment.

Mr. OLSEN [continuing]. Very quickly. Section 702 is a foreign intelligence tool.

Senator OSSOFF. Yes.

Mr. OLSEN. It's not a law enforcement——

Senator OSSOFF. Right.

Mr. OLSEN [continuing]. Tool.

Senator OSSOFF. So why is it used for domestic law enforcement purposes?

Mr. OLSEN. It has been used exceedingly rarely where a query using a U.S. person identifier would have identified information that did not have a foreign intelligence purpose. So outside of the national security realm, not involving a terrorism, or espionage, or cyber charge or investigation——

Senator OSSOFF. So it can be used for this purpose, and it has been used for this purpose.

Mr. OLSEN. In 2022, it was 16 different times—14 of those times where it was used for evidence of a crime only were where the U.S. Government had an affirmative discovery obligation to search.

Senator OSSOFF. Well, we'll get into those numbers in a second.

Mr. OLSEN. Yes.

Senator OSSOFF. But it begs the question, if it's so rare, as you state, why not go get a warrant?

Mr. OLSEN. I think the initial idea was that there would be occasions, perhaps, where an agent or an analyst would find evidence of a crime only—not national security information—in the 702 data and would want to be able to use that.

And it has happened that an agent found evidence of child abuse while looking at Section 702 data. So pure evidence of a crime that they were then able to follow——

Senator OSSOFF. Different things. We are talking about seeking evidence of a crime only. We're not talking about encountering evidence of other crimes in the course of querying foreign intelligence information.

Mr. OLSEN. Okay.

Senator OSSOFF. We're talking about U.S. person queries whose sole purpose is investigating domestic crime. Why should that not require a warrant?

Mr. OLSEN. The reason for not requiring a warrant is that this is lawfully collected information that is in the FBI holdings. And to simply wall off the FBI, for example, in the child abuse context from seeing that information and using it would prevent them from——

Senator OSSOFF. Yes.

Mr. OLSEN [continuing]. Being able to follow up——

Senator OSSOFF. That's a different fact pattern. That's encountering evidence of a crime in the course of conducting foreign intelligence investigations. This is a question I think that the Committee needs to look into.

I want to talk about this question of justification. We got a document last night about 12 hours before this hearing announcing some new reforms. I want to read back something that you said to Chair Durbin in this hearing. You said, "Starting in 2021, the FBI agent or analyst had to actually affirmatively take the step that I'm going to conduct a search using a U.S. person identifier. And then say why that was reasonably likely to return foreign intelligence information." This is the justification for the query, but has to be entered into the system.

But it's the case, isn't it, that until 12 hours ago, when we received this, they only had to enter that justification if they actually looked at the results. They did not have to enter that justification to enter the query. Correct?

Mr. OLSEN. That's correct. It was only if there was responsive information from the query. At that point there would be the obligation to——

Senator OSSOFF. Right.

Mr. OLSEN [continuing]. Justify it.

Senator OSSOFF. So they can—they can enter the query and they're going to see substantive information before they view the full results. Aren't they going to see a number of results? They may see some metadata. They may even see some preview content. Correct?

Mr. OLSEN. I don't believe that there would be any opportunity to review any content of what was produced in response to the query before entering the justification.

Senator OSSOFF. No metadata?

Mr. OLSEN. I'm not sure about that. It—I'm not——

Senator OSSOFF. Well, it's metadata either way. Isn't it? Because it reveals whether or not the U.S. person being investigated has had contact with anyone in the FBI's portion of the underlying 702 database. Correct?

Mr. OLSEN. It may simply be sent. I don't know the exact answer, but——

Senator OSSOFF. So I'm out of time, but I——

Mr. OLSEN [continuing]. It may simply be a response that there is responsive information in the data, but nothing further.

Senator OSSOFF. I'm out of time. But, let me just—so as I said at the beginning, I don't have any doubt about the foreign intelligence value of this. But the U.S. person query aspect of this is really concerning to the Congress. I don't think you've effectively made the case that there shouldn't be a warrant requirement whether or not it is constitutionally required for a U.S. person search that is crime only.

And it just—it undermines the feeling about transparency. When you and your colleagues making the rounds for the last few months about, you know, touting the reforms you've implemented, have been explaining to us that, well, ever since the reforms were made, we have to state a justification for the query——

[Gavel is tapped.]

Senator OSSOFF [continuing]. When it turns out that you only had to state the justification for the query if you actually decided to look at what the search revealed.

So U.S. person queries is an area ripe for statutory changes, Mr. Chairman. Thank you.

Chair DURBIN [presiding]. Thanks, Senator Ossoff. Senator Cruz.

Senator CRUZ. Thank you, Mr. Chairman. Gentlemen, every day when I'm home in Texas, I hear from Texans who are deeply dismayed about the growing politicization and weaponization of the Department of Justice and the FBI. If you are not, every one of you should be deeply concerned about the damage being done to the integrity of the institutions in which you operate.

My office hears regularly from FBI agents and from assistant U.S. attorneys who are likewise concerned about the politicization and weaponization of the Department of Justice and the FBI. And this is profoundly damaging to the rule of law in our Nation.

Last month, a whistleblower brought to light the existence in the FBI of a report in FD–1023 in which the informant alleges that President Biden and his family members engaged in a $5 million bribery scheme during his time as Vice President. Deputy Director Abbate, is it true that the FBI has a report making those allegations?

Mr. ABBATE. I'm not going to comment on that, Senator.

Senator CRUZ. And why is that?

Mr. ABBATE. I'm just not going to comment on information we received, investigations——

Senator CRUZ. You owe an——

Mr. ABBATE [continuing]. On ongoing matters.

Senator CRUZ [continuing]. Obligation to the American people to be candid about evidence of corruption by the President of the United States.

Mr. ABBATE. This is an area that I'm not going to get into with you, Senator.

Senator CRUZ. Well, I understand you don't want to. And that's why people are mad at the FBI. Because you're stonewalling and covering up serious allegations of evidence of corruption from the President.

Yesterday, Senator Chuck Grassley stood on the Senate floor and alleged that there are 17 recordings of this informant from Burisma, Ukrainian natural gas company, 15 of them are recordings—voice recordings of him talking to Hunter Biden. Two of them are voice recordings of him talking to Joe Biden. Deputy Director Abbate, does the FBI have 17 voice recordings laying out evidence of a bribery scheme?

Mr. ABBATE. Senator, I would add also that we've worked with the House Oversight Committee——

Senator CRUZ. Yes, this is the Senate. We're the other——

Mr. ABBATE [continuing]. To provide the documents that you are——

Senator CRUZ [continuing]. Side of the Capitol. This is the Senate. Do you have those 17 recordings?

Mr. ABBATE. I'm not going to comment on any investigative matter, Senator——

Senator CRUZ. See, that's——

Mr. ABBATE [continuing]. Period.

Senator CRUZ [continuing]. The problem. The FBI—and I've had this conversation with Chris Wray, too, this is why you are damaging the institution. The American people have a right to know whether there is serious, credible evidence that the President of the United States took a $5 million bribe. And by the way, if it's false—Chairman Durbin just rolled his eyes.

Chair DURBIN. He watches me pretty closely.

Senator CRUZ. If Chairman Durbin were interested in the rule of law, we would have a hearing on these allegations. But of course, the Democrats don't want a hearing on these allegations. And to be clear, if the allegations are false, you know who could disprove them? Joe Biden. He could call for this to be released publicly. But the FBI is stonewalling. Would you——

Mr. ABBATE. Two things——

Senator CRUZ [continuing]. Agree——

Mr. ABBATE [continuing]. Senator.
Senator CRUZ. Sure.
Mr. ABBATE. No one's stonewalling. The 1023——
Senator CRUZ. You just said you refused——
Mr. ABBATE [continuing]. Was provided in response——
Senator CRUZ [continuing]. To answer the question.
Mr. ABBATE [continuing]. To a subpoena by the Oversight Committee.
Senator CRUZ. Okay. Then why did you refuse to answer my question?
Mr. ABBATE. The pertinent information is there, and I reject your assertion that——
Senator CRUZ. Why did you refuse——
Mr. ABBATE [continuing]. The FBI is politicized.
Senator CRUZ [continuing]. To answer my question?
Mr. ABBATE. I just answered your question.
Senator CRUZ. Okay. So, yes, you have a 1023. Do you have the 17 recordings, yes or no?
Mr. ABBATE. I'm not going to get further into that, Senator.
Senator CRUZ. So you're stonewalling. You can't say, I'm not refusing to answer your question, but I won't answer your question.
Mr. ABBATE. I'm going to answer within the parameters that we operate in, sir.
Senator CRUZ. That's the problem. The FBI has right now an unlimited hubris that you believe you are unaccountable. You don't believe you're accountable to the United States Congress, and you don't believe you're accountable to the American people. And you are doing damage.
The FBI is a great institution. When I go home to Texas, people ask me, should we abolish the FBI? Now, I tell them, no, because you have heroes and patriots working for you that are catching child predators, that are catching terrorists. But you're sitting there happily erecting a wall to protect Joe Biden.
Will you provide to this Committee—not the House, the Senate Judiciary Committee, will you provide the FD–1023? And will you provide the 17 recordings so we can assess what is the evidence—the specific, credible evidence that Joe Biden personally took a $5 million bribe from a foreign national?
Mr. ABBATE. Senator, we will work with this Committee, you and other Members, to provide the information within the parameters of the process.
Senator CRUZ. Will you provide the FD–1023, yes or no?
Mr. ABBATE. I will take that back, and we will work with our team to——
Senator CRUZ. So you're not answering that. Will you provide the 17 recordings?
Mr. ABBATE. We will take that back, and we'll work with you and your staff——
Senator CRUZ. So you're not answering that, either. Did you investigate in any way, shape, or form these allegations?
Mr. ABBATE. Senator, once again, I'm not going to comment——
Senator CRUZ. So you're not going to say——
Mr. ABBATE [continuing]. On an ongoing investigation.
Senator CRUZ [continuing]. Whether you did your job?

Mr. ABBATE. We do our job to the very best of our ability——

Senator CRUZ. Well, not here. You're not answering a single question to the American people. And you may think this is esoteric. I promise you, millions of Americans are concerned.

You know who isn't concerned? Not a single Senate Democrat. We're going to go through this whole hearing. Not one Democrat will ask a question about this. You know who else isn't concerned? The corporate media who is joining with the Democrats in covering up this evidence.

If Joe Biden is innocent, the evidence should be made public and demonstrate that he's innocent. But if he is not, is it true this informant who alleged that he personally took a bribe was an informant the FBI had relied upon previously in other investigations, yes, or no?

Mr. ABBATE. Senator, in each and every investigation that we have, all the work that we do——

Senator CRUZ. I asked a yes or no question.

Mr. ABBATE [continuing]. The expectation is that every logical avenue——

[Gavel is tapped.]

Mr. ABBATE [continuing]. Of investigation be——

Senator CRUZ. I asked you——

Mr. ABBATE [continuing]. Pursued to its fullest——

Senator CRUZ [continuing]. A yes or no question. Are you going to answer it?

Mr. ABBATE. I'm answering your question.

Senator CRUZ. Was the informant one you had relied on previously in other investigations, yes or no?

Mr. ABBATE. Senator, we run down every piece of information——

Senator CRUZ. You're not answering it then?

Mr. ABBATE [continuing]. And review it——

Senator CRUZ. You're refusing to answer——

Mr. ABBATE [continuing]. Objectively——

Senator CRUZ. So you're refusing to answer the question?

Mr. ABBATE [continuing]. To the fullest extent possible——

Senator CRUZ. You're refusing——

Mr. ABBATE [continuing]. Relentlessly——

Senator CRUZ [continuing]. To answer the question.

Chair DURBIN. Senator, your time has expired.

Mr. ABBATE [continuing]. And in the correctly allowed instances.

Chair DURBIN. Senator, your time has expired.

Senator CRUZ. Disgraceful. It's disgraceful, Deputy Director Abbate. Disgraceful.

Chair DURBIN. Senator, your time has expired. Senator Tillis.

Senator TILLIS. Chairman, I think Senator Blackburn goes before me or Senator Welch. I appreciate the opportunity, but.

Chair DURBIN. Thank you, Senator Tillis. It's Senator Welch is next.

Senator WELCH. Thank you, Mr. Chairman. I want to thank all the witnesses. I'm sitting in a seat that was previously occupied by Senator Leahy, who was a champion of civil liberties, and a strong supporter of law enforcement, his own prosecution background.

But he, and with the great support of Vermonters, very much was concerned about the civil liberty questions that are raised. And I've heard from all of the witnesses you share that concern, and I certainly do. What Chairman Durbin said in his opening remarks in expressing his very serious concern about the extraordinary breaches, I share that.

So a couple of things. One, Senator Cornyn had asked about codifying in statute reforms that have been made. And my understanding—I think this goes to you, Mr. Olsen—is that you would be supportive of any of the reforms that have been made to date being codified in statute so it wasn't another episode of, "Trust me, and we'll try to get it right"?

Mr. OLSEN. I think that's exactly as the deputy director said. I mean, the fundamental point is we are open to engaging on reforms and implementing reforms that don't undermine the essential effectiveness of Section 702. Certainly——

Senator WELCH. But codifying them.

Mr. OLSEN. And among those would be, right, putting in statute where it makes sense to do so. Some of the changes or the changes that the FBI has implemented on its own to ensure compliance.

Senator WELCH. You know, I just want to make certain that we're on the same page here——

Mr. OLSEN. Yes.

Senator WELCH [continuing]. Because it's one thing to say trust us, we've learned, and will be good in the future. It's another thing to have the force of law behind it.

Second thing——

Mr. OLSEN. And if I may just say, the rule of—I'm being a little—I'm hesitating only because as the lawyer here next to Mr. Abbate, I just want to make sure that—we'd want to make sure that the language in any statute is——

Senator WELCH. Well, no——

Mr. OLSEN [continuing]. Appropriate, of course.

Senator WELCH [continuing]. That goes without saying.

Mr. OLSEN. Yes.

Senator WELCH. Now, another thing, I know Senator Leahy and Senator Lee worked on an amicus amendment, as I understand it. Senator Lee—and by the way, he very much appreciated working with you on that. He's told me. My understanding is you're resistant to that, you're saying for practical reasons.

But keep in mind, I think the motivation Senator Leahy had—I'll speak for my conversation with him, and I've heard Senator Lee express it—the interest of maintaining Fourth Amendment protections for citizens is constitutional and inviolate. So I would expect to advocate for that. Again, you answered the question, but I just want to bring that to your attention.

You know, the heart of this is this question of whether there is an exception on the warrant protection when a U.S. citizen gets swept into this. And I know Mr. Ossoff asked in my absence about the warrant protection, but I am wanting to go back on that. Why can't we have a warrant when it does involve a U.S. citizen?

And can you make distinctions between a situation where there's imminent urgency, and obviously that requires a different kind of action versus those situations where information comes up. My

telephone number is on a telephone that's been captured on the battlefield, but there's no urgent matter that has to proceed with action. What's the problem with providing a continuation of the warrant protection that is available to all U.S. citizens outside of FISA?

Mr. OLSEN. Maybe Mr. Fonzone might have more to add to this. But let me just say, stepping back, so it's really important for me to be clear that when it comes to the targeting decision, the initial decision to target, that is outside of the Fourth Amendment. Because the targeting decisions are focused on non-U.S. persons overseas. It's only when the FBI receives——

Senator WELCH. No, I understand that.

Mr. OLSEN [continuing]. A small—yes. It's only 3 percent of all of the 702 collection that FBI has access to where it's related to an open FBI investigation. So they have 3 percent of the lawfully collected information. And it's very common rather than rare that the need to search that data, whether it's an ongoing cyberattack, for example, or an espionage effort, that it is not a degree of urgency to quickly be able to say at the very earliest stage of an investigation: We need to understand, is this technical identifier associated with this cyberattack? Is this hitting other, you know, hospitals or energy companies?

Senator WELCH. Well, my time is coming up, and we'll have to—there's real practical questions here. But I go back to this absolutely astonishing situation where folks who showed up here in Washington that was totally domestic, or Black Lives Matter, totally domestic, were searched.

And, like, how in the world did that happen? Somebody just felt like doing it or what? I know my time is up. So I'm going to have to stop. But I just want to convey my ongoing concerns which I think many of the Committee Members share. Mr. Chairman, thank you very much.

Chair DURBIN. Thanks, Senator Welch. Senator Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman. Mr. Abbate, I want to come to you because Tennesseans are incredibly concerned about the politicization of the FBI. And they have watched the FBI target parents, people of faith, people with conservative values. And I am often asked what group is going to be next, and how did we get to this point?

Because they have watched the FBI, under your leadership, draw their guns on a pro-life advocate. That was stunning to them. That was done in front of his wife and children. They have labeled parents interested in education as domestic terrorists. And all parents should be interested and are interested in their children's education. They watched the raid on a former President and a political opponent on his home.

And these have confirmed their worst fears: that there are indeed two tiers of justice, and that there is a political cabal within the FBI that sees it that way. Because when Hillary Clinton mishandled information, and she wiped her email server with a tool called BleachBit, and then beat the mobile devices with a hammer and destroyed those SIM cards, you all basically said there's nothing to see here. There is nothing to question.

And when President Biden mishandled classified documents, there was no raid on his home or on his offices. But you see how President Trump has been handled with this. So it looks like the old playbook of distract and deflect. And the American people have a right to be concerned about this.

Now, I want to talk about Senator Grassley's information from yesterday. Because when the FBI produced the document that you referred to earlier relating to the Biden bribery allegations, and you gave that to House Oversight, you all redacted any reference to the fact that the foreign national who allegedly bribed Joe and Hunter Biden had those 17 audio voice recordings. So first of all, why did you redact that part of the information?

Mr. ABBATE. Senator, first, as I said before, your assertion, or anyone who makes the assertion that the FBI is politicized, I reject it wholeheartedly. It's wrong, and it is not true. The work we do——

Senator BLACKBURN. Okay, Mr. Abbate, then let me——

Mr. ABBATE [continuing]. And the people I see in the FBI——

Senator BLACKBURN [continuing]. Ask you this. You said in your response to Senator Cruz that you and the FBI do your job to the best of your ability. So why don't you tell me what your job is? Is it to defend and shield Joe Biden? Or is your job to protect this country and the Constitution of the United States? Which is it?

Mr. ABBATE. The job of the FBI is to protect the country, keep people safe, and uphold the Constitution of our great country——

Senator BLACKBURN. So why are——

Mr. ABBATE [continuing]. Period.

Senator BLACKBURN [continuing]. You using——

Mr. ABBATE. That's what we work to do every day objectively. There are not two standards of justice. There is only one. It's applied——

Senator BLACKBURN. Practically and by perception——

Mr. ABBATE [continuing]. Equally to each and every person——

Senator BLACKBURN [continuing]. There are two standards, very clear standards of justice in this country. We see it every single day. The American people see this every single day. They look at you and they see a politicized entity that is weaponizing an agency of the Federal Government against the American people.

Mr. ABBATE. That is not the FBI that——

Senator BLACKBURN. They see this play out.

Mr. ABBATE [continuing]. I see, Senator.

Senator BLACKBURN. That is not the FBI you see. There are a lot of good people that work for the FBI, but you have a political cabal there. So why did you decide to conceal the information in that revelation to the House Oversight Committee? Why did you redact all of that rep—pertaining to the phone calls?

Mr. ABBATE. We have exceptional people——

Senator BLACKBURN. You're not——

Mr. ABBATE [continuing]. In the FBI, the very best——

Senator BLACKBURN [continuing]. Answering the question. Why did you redact that information?

Mr. ABBATE [continuing]. And they work relentlessly every day to keep——

Senator BLACKBURN. You chose not to reveal——

Mr. ABBATE [continuing]. This country safe, and to protect people——

Senator BLACKBURN [continuing]. That the calls——

Mr. ABBATE [continuing]. Period.

Senator BLACKBURN [continuing]. Were there, and Senator Grassley found it out anyway. Is that accurate?

Mr. ABBATE. With regard to the document——

Senator BLACKBURN. You chose to redact it, yes or no?

Mr. ABBATE. We often redact documents to protect——

Senator BLACKBURN. So you chose——

Mr. ABBATE [continuing]. Sources and methods——

Senator BLACKBURN [continuing]. To redact the fact that there are 17 voice recordings, two of those with the now President. You chose to redact that and not to give that to House Oversight.

Mr. ABBATE. I have——

Senator BLACKBURN. Is that accurate?

Mr. ABBATE [continuing]. No idea if there are voice recordings or not. What I will tell you with respect——

Senator BLACKBURN. You have no——

Mr. ABBATE [continuing]. To the document, the document was redacted to protect the sources. Everyone knows.

Senator BLACKBURN. Well then, let——

Mr. ABBATE [continuing]. And this is a question of life——

Senator BLACKBURN [continuing]. My time potentially expired——

Mr. ABBATE [continuing]. And death, potentially.

Senator BLACKBURN [continuing]. But I think it would be helpful if when you came before us, if you were willing to answer the questions. It would help to remove the perception that the American people have because this is what they see. They see you do it every day. And that is politicizing the FBI and using it against the American people who don't happen to be named Biden, Clinton, or one of the elites. Thank you, Mr. Chairman.

Chair DURBIN. Senator Hawley.

Senator HAWLEY. Thank you, Mr. Chairman. Mr. Abbate, let me just stay with you. You just started to answer Senator Blackburn's question that not releasing the 1023 or talking about it as a matter of life and death. Question of life and death, you said. Explain.

Mr. ABBATE. It is potentially a question of life and death——

Senator HAWLEY. For whom?

Mr. ABBATE [continuing]. With regard to the source of the information.

Senator HAWLEY. So—okay. So now we've confirmed that the document exists. That's progress because the FBI Director initially denied that it exists.

Mr. ABBATE. No.

Senator HAWLEY. Why did he do that?

Mr. ABBATE. We have already and previously acknowledged the existence of the documents.

Senator HAWLEY. Yes. After you first denied it. Now, when a Member of this Committee read it. Right? The FBI Dir—let's just get the record straight. The FBI Director initially said it doesn't exist. Then Senator Grassley said, I've read it. Then he said, oh, okay, well, got you. I guess it does exist. Now, you're going back

and forth with Members of this Committee what's in it. Why don't you just release it? Is it classified?

Mr. ABBATE. The document is not classified.

Senator HAWLEY. Okay. Will you commit to releasing it?

Mr. ABBATE. Senator, we'll take that back, and we will work with you and this Committee——

Senator HAWLEY. How about just a yes or no? Will you commit to releasing this unclassified document that alleges that the President of the United States—the President of the United States has taken $5 million or more in bribes from a foreign nation?

Mr. ABBATE. The document has already been released pursuant to a subpoena to the House Oversight Committee. We will——

Senator HAWLEY. Has it been released to this Committee?

Mr. ABBATE [continuing]. Work with this Committee within the parameters that are established to meet——

Senator HAWLEY. Will you release——

Mr. ABBATE [continuing]. The request.

Senator HAWLEY [continuing]. The document to the public? It's unclassified. Don't you think the American people have a right to see it?

Mr. ABBATE. Senator, the document, as you know, contains sensitive information that has bearing on the life of the source of the information, potentially.

Senator HAWLEY. You can redact the source's name. We do this all the time.

Mr. ABBATE. In some instances, Senator, and I know you know this, that is not sufficient to protect people. And that's what we strive and work to do each and every day. And I hope you would take that seriously, too.

Senator HAWLEY. Oh, I take it very seriously. But I also take seriously the fact that your institution has repeatedly abused its authority, has repeatedly targeted political opponents.

Your institution is the one that went to the door of pro-life protesters with SWAT teams to try and intimidate people because of their speech.

Your institution is the one that treated parents as domestic terrorists because of their speech.

Your institution is the one that according to the court, the FISA Court, ran 278,000 unwarranted, probably illegal queries on Americans. Right? That was your institution. Correct?

Mr. ABBATE. There are—with respect to the compliance incidents, yes. Some of the other things you cited, we can take them one by one. They are not accurate.

Senator HAWLEY. Compliance. You would characterize the unlawful querying 278,000 times of American citizens as compliance issues?

Mr. ABBATE. We've said before, I've said, that they're totally unacceptable.

Senator HAWLEY. Who's been fired for it?

Mr. ABBATE. Individuals involved are handled through the disciplinary process.

Senator HAWLEY. Who's been fired for it?

Mr. ABBATE. We have in the case of the unintentional instance where something similar happened, we have fired people in the past.

Senator HAWLEY. I'm sorry, what does that word salad mean? The unintentional instance—what does that mean? Who's been fired for the 278,000 times that you improperly or illegally queried the database for American citizens?

Mr. ABBATE. When we find intentional incidents——

Senator HAWLEY. Were you saying that the 278,000 queries were unintentional?

Mr. ABBATE. I believe that's correct.

Senator HAWLEY. Wow, 278,000 times American citizens' information was queried by your agency unintentionally? That's your testimony?

Mr. ABBATE. I would want to go back and check that, Senator.

Senator HAWLEY. Well, that's what you just told me.

Mr. ABBATE. My understanding is that the vast majority of the——

Senator HAWLEY. Wait, that's different. You just said it was. You just said it was unintentional. Now it's the vast majority. Which is it? Do you know?

Mr. ABBATE. I would want to go back and check it.

Senator HAWLEY. So you don't know?

Mr. ABBATE. My understanding is that likely all are—were unintentional——

Senator HAWLEY. Likely all.

Mr. ABBATE [continuing]. In nature.

Senator HAWLEY. So first it was all of them. Then it was vast majority. Now, it's likely all. So you don't know, is the answer to the question.

Mr. ABBATE. I don't know the answer as we sit here today, but I——

Senator HAWLEY. You could have started with that, probably.

Mr. ABBATE [continuing]. Will find out and get back to you.

Senator HAWLEY. Who was fired for the lies to the FISA Court for the Carter Page warrant. Who was fired for that? Anybody? Has anybody been held accountable for your institution deliberately lying to a FISA Court to get a wiretap on an ongoing Presidential campaign?

Mr. ABBATE. There is an ongoing disciplinary process with respect to individuals involved in that.

Senator HAWLEY. Here's the deal. You're back in front of us asking for the reauthorization of extraordinary authorities. Multiple courts have uncovered extraordinary abuses perpetrated by your agency.

You are, at the same, time concealing information about serious allegations made against the President of the United States even as your institution also targets his chief political opponent in an unprecedented way. Why would we ever give you the blank check that you want to continue surveilling American citizens in an improper manner? Why would we ever do that?

Mr. ABBATE. Senator, we're here to talk about reforms. Today, I did get confirmation that the query instances——

Senator HAWLEY. No, we're not. We're here to talk about the reauthorization of Section 702. Why would we reauthorize it given your track record of abuse, and illegal improper surveillance, and political targeting? Why would we do that? Why would it be appropriate for this body to do that?

Mr. ABBATE. We've made significant reforms and implemented corrective measures. We've seen significant progress as a result of that, Senator. The——

Senator HAWLEY. So you say.

Mr. ABBATE [continuing]. Queries that you mentioned early were, in fact, unintentional. That's what I was just told by my counterpart.

Senator HAWLEY. That—that is an amazing——

Mr. ABBATE. That is to clarify your earlier question.

Senator HAWLEY. So your testimony is the 280,000 queries of American citizens was unintentional. That's your final answer?

Mr. ABBATE. That's how they were assessed by that team that did the review. I'm not satisfied with that. That's——

Senator HAWLEY. Yes. I don't believe that at all.

Mr. ABBATE [continuing]. Why we've implemented further measures as I announced earlier today.

Senator HAWLEY. Yes. I don't believe that at all. And frankly, we've heard from your agency a thousand times that you're going to do better. We'll do better. You promised after the abuses of Title I you'd do better. And then we find out that in the meantime, you're illegally querying 280,000——

[Gavel is tapped.]

Senator HAWLEY [continuing]. American citizens' data. It's just—it's unbelievable. Frankly, everything you say is unbelievable.

Chair DURBIN. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chair. Thank you all for being here, and thanks to all of the hardworking law and Federal law enforcement officers that I believe are overwhelmingly majority good patriots doing a great service and keeping our country safer.

I appreciate the documents that you all sent over. Particularly, we can talk about what it's doing.

A couple of months ago, I went over to the FBI. I saw a demonstration of many of the changes that you've implemented on the online query system. I think they're very promising. It also begs the question, why didn't we have it before? But we've corrected that mistake.

Senator Cornyn mentioned codification. I had that discussion with the Department of the changes, Mr. Abbate, that you all have made. I also would encourage every Member to see this in action and go through the demonstration that I did. I think it's positive progress.

But I had a question for you, Mr. Abbate, on the three strikes. I'm trying to figure out how we get to reauthorizing Section 702. It would be irresponsible of us to not figure out a way to do it. It's critically important. A very important tool.

The three-strikes thing, though, kind of struck me as why should anybody get past one strike? I mean, and to me, there are, "Oops, I just didn't know. I just finished training." Maybe that's a legitimate reason. But three strikes against the controls that you're put-

ting in place before what action occurs? What happens with strike three? I'm assuming they're out, but what are they out of?

Mr. ABBATE. It could include everything up to dismissal, Senator. And I think it's important to clarify here. This three-strikes applicability refers to those that are deemed to be—those compliance errors that are—or incidents that are deemed to be unintentional. And it's an escalating approach with respect to the three strikes.

If someone was to unintentionally commit an error like this three times, then they would be referred for greater discipline in addition to the things that come into play. Their FISA access would be removed upon the occurrence of the first incident. They would undergo full mandatory retraining. They would have to sit down and be counseled by one of the attorneys from our Office of General Counsel.

And it gives us the ability to, you know, evaluate the conduct and determine whether it is truly unintentional or whether it should be elevated to the category of reckless or even intentional, which would warrant more severe disciplinary action.

One of the things I've struggled with as I've looked at the compliance incidents—and this gets back to the other Senator's earlier question—those that are unintentional. Given the measures we've put in place now with the system adaptations, the prompts with regard to sensitive queries, the written justification, the parameters around batch queries and sensitive queries, and the opt-in, it's hard to imagine that it would be unintentional if someone pushes through all of those measures in order to run a query that is found to be noncompliant.

And that's part of the strength of the sort of regime of reforms that we've put in place now. Because prior, and this was not satisfactory to any of us, many of them were categorized as unintentional when they may not have otherwise been, and they may have risen to the level of recklessness or even intentionality.

Senator TILLIS. Could you talk a little bit about—I think that with Crossfire—I mean, people have raised some concerns, and, I think, rightfully so about Crossfire Hurricane. We all know it. That was mostly Title I as opposed to Section 702. Do you agree with that, and can you explain the differences?

Mr. ABBATE. I do agree with that, Senator. That was Title I FISA. That's the traditional FISA where we go to the FISA Court. It involves a U.S. person, and I'll defer to my colleague here to get into legalities. But we are—in those instances, we go to the FISA Court. We have to establish probable cause in order to get authorization to implement surveillance on the individual targeted.

Senator TILLIS. Mr. Olsen, in response to, I think, one of Senator Ossoff's questions about this information being used in an investigation. You—I think you stated a relatively small number of people who are actually swept into that category. Can you elaborate a little bit more? And over time, are we seeing fewer of those? Is that because we're getting trained better, or it's just because we're honing our investigations?

Mr. OLSEN. Sure. When we were talking about is the FBI's authority to conduct a query of the data it has access to for simply evidence of a crime that is not national security related. It's exceed-

ingly rare. And it's rare because there has to be a—we're talking about a database that is a foreign intelligence database.

So the odds of finding simply evidence of a non-national security crime—bank robbery, public corruption—in a foreign intelligence database is just so unlikely. In the last recording period, there were 16 instances. But actually, 14 of those 16 instances was where the FBI had an affirmative obligation to search for evidence of a crime because of discovery or Brady obligations in an ongoing case.

So it is not, obviously, the main purpose. It is—I would consider it sort of a backstop or failsafe if there is evidence, but a non-national security crime that the FBI would want to see or follow up on. But it's just so exceedingly rare. It's not the focus, certainly, of our efforts.

Senator TILLIS. My time has expired. But I would encourage, as I said after that demonstration of the changes that you've made, that we need to see a meaningful legislative proposal on the codification of all the measures that you put into place. And I think, probably based on the comments you have here, this is not an ideological dispute for the most part. You've got different people supportive, other people that want to go dark. We need the Department to fairly quickly get us some baseline text that those of us who want to get it reauthorized can begin to explain how we're addressing the problems that are legit problems. And every Member here who's frustrated has a reason to be. Thank you, all.

Mr. OLSEN. Thank you, Senator.

Chair DURBIN. Thanks, Senator Tillis. Pursuant to the procedures and traditions of the Committee when it comes to the debate of 702, we have a session reserved in the SCIF SVC 217 as soon as we adjourn today. And I don't know, we think several colleagues are going to come to that meeting to ask questions that couldn't be discussed in open session.

But I thank you for your cooperation, your attendance today, and I thank the Members for their participation. And the meeting of the Senate Judiciary Committee will stand in recess, subject to reconvening at SVC 217 upon arrival. Thank you.

[Whereupon, at 12:21 p.m., the Committee recessed.]

[Additional material submitted for the record follows.]

# A P P E N D I X

**Submitted by Chair Durbin:**


Advocacy For Principled Action In Government, et al., letter ..... 90
American Civil Liberties Union, et al., statement ..... 99
Center for Democracy & Technology (CDT), statement ..... 103
Goitein, Elizabeth, statement ..... 108



**SENATE JUDICIARY COMMITTEE**
**JOINT STATEMENT FOR THE RECORD**

***of***

**CHRIS FONZONE**
**GENERAL COUNSEL**
**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

**GEORGE BARNES**
**DEPUTY DIRECTOR**
**NATIONAL SECURITY AGENCY**

**DAVID COHEN**
**DEPUTY DIRECTOR**
**CENTRAL INTELLIGENCE AGENCY**

**PAUL ABBATE**
**DEPUTY DIRECTOR**
**FEDERAL BUREAU OF INVESTIGATION**

***and***

**MATTHEW OLSEN**
**ASSISTANT ATTORNEY GENERAL**
**NATIONAL SECURITY DIVISION**
**DEPARTMENT OF JUSTICE**

**JUNE 13, 2023**

**(U) I. Introduction**

(U) Chairman Durbin, Ranking Member Graham, distinguished members of the Committee, thank you for the opportunity to speak to you about Section 702 of the Foreign Intelligence Surveillance Act (FISA), the vital intelligence authority which, along with other FISA provisions, will expire at the end of this year unless Congress renews it.

(U) Section 702 authorizes the Intelligence Community to collect critical foreign intelligence information about foreign targets located outside the United States with the compelled assistance of U.S. communications service providers. In the fifteen years since its enactment, Section 702 has proven indispensable to U.S. national security. Every day it helps protect Americans from a host of new and emerging threats—such as terrorist plots, weapons of mass destruction, malicious cyber activity, and hostile state behavior from China and Russia.

(U) As described below, Section 702 is an elegant solution to an operational challenge created by the advent of the Internet and changes in the technology supporting international communications. It authorizes the Intelligence Community to collect vital intelligence overseas while requiring the Intelligence Community to comply with rigorous safeguards that protect the rights of Americans. It is a cornerstone of our Intelligence Community's efforts to identify and understand a broad range of challenges our country faces in an increasingly complex and dangerous world. And it remains a paradigmatic example of congressional leadership in national security. Without it, the United States and its allies and a partners would be less safe.

(U) Presidents of both parties have strongly supported it and attested to Section 702's importance to national security. Congress, recognizing Section 702's critical value and stringent protections, has three times voted on a bipartisan basis to authorize it, first in 2008, and then in 2012 and again in 2018. If Congress allows this authority to lapse, or renews it in a diminished form, the United States will lose access to critical intelligence about strategic national priorities and threats around the world.

(U) Section 702 is subject to robust privacy protections and oversight by all three branches of government. This structure enables the government to proactively identify, transparently disclose, and swiftly address compliance risks. For example, the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) recently imposed additional safeguards in response to compliance incidents related to procedures for accessing data lawfully collected through Section 702.

(U) This Committee plays an important role in overseeing this critical surveillance authority, and we stand ready to provide you with the information you need regarding the use of Section 702. The executive branch is committed to working with the Committee and the rest of the Congress on reforms to further enhance privacy protections while fully preserving the efficacy of this vital national security tool.

(U) Today we will illustrate the immense national security value of Section 702; describe its origin and legal structure; outline its compliance regime; and address concerns regarding privacy, particularly with respect to U.S. person queries of Section 702 data.

**(U) II. The Value of Section 702 Collection**

(U) Section 702 provides foreign intelligence information that is indispensable to protect the nation against national security threats. It has proved invaluable in protecting American lives and U.S. national security. There is no way to replicate Section 702's speed, reliability, specificity, and insight. In many cases, Section 702 is the sole source of our information about foreign threats to the United States and its people.

(U) Section 702 has been tremendously effective in combatting international terrorism, the dominant national security concern when Congress initially enacted the authority. In 2009, for example, Section 702 helped foil an active plot to bomb the New York City subway. National Security Agency (NSA) analysts relied on Section 702 to acquire the email communications of a suspected Al-Qa'ida courier in Pakistan and discovered a message sent by someone in the United States seeking advice about making explosives. The FBI identified that person as Najibullah Zazi and was able to disrupt his plot in time to save countless lives. Moreover, Section 702's value to the government's efforts to counter international terrorism continues to the present day. Just last year, in July 2022, Section 702 played an important role in the strike against Al-Qa'ida's leader, Ayman al-Zawahiri. Section 702 collection contributed significantly to our knowledge that al-Zawahiri was living in a safe house in downtown Kabul.

(U) Section 702's utility extends well beyond counterterrorism. It provides critical insights on some of the most urgent threats to U.S. national security.

- (U) Section 702 has been used to identify ransomware attacks on U.S. critical infrastructure, and multiple attacks have been identified and defended against because of Section 702 collection.

- (U) For example, Section 702 played an important role in the U.S. Government's response to the cyberattack on Colonial Pipeline attack in 2021. Using Section 702, the Intelligence Community acquired information that verified the identity of the hacker, as well as information that enabled U.S. Government efforts to recover the majority of the ransom.

- (U) Section 702–acquired information related to sanctioned foreign adversaries was used in U.S. government efforts to stop components for weapons of mass destruction from reaching foreign actors.

- (U) Section 702 information has identified key economic security risks, including strategic malign investment by foreign actors in certain U.S. companies.

- (U) Section 702 collection has helped identify when hostile foreign intelligence services are trying to send their operatives into the United States to recruit spies here in the United States.

- (U) Finally, Section 702–acquired information revealed:
    - insights that have informed the U.S. government's understanding of the Chinese origins of a chemical used to synthesize fentanyl;
    - foreign actors' illicit plans to smuggle methamphetamine across the U.S. border;
    - the quantities and potency of drugs, including fentanyl, destined for illegal transfer to the United States, as well as specific smuggling techniques used to avoid detection; and
    - a foreign narcotics trafficker's purchase of a vast quantity of pills for transfer to the United States.

(U) Today, Section 702 not only helps defend and protect the United States but also helps advance U.S. foreign policy priorities around the world. For example:

- (U) Section 702 has helped uncover gruesome atrocities committed by Russia in Ukraine—including the murder of non-combatants, the forced relocation of children from Russian-occupied Ukraine to the Russian Federation, and the detention of refugees fleeing violence by Russian personnel. This and other information have helped the U.S. government to galvanize accountability efforts related to Ukraine by confidently and accurately speaking to the international community about Russia's atrocities.
- (U) Section 702 data helped expose efforts by foreign powers, including China, to coerce nations to oppose international responses to human rights violations. This reporting enabled U.S. diplomats to assist countries in shielding themselves from coercion and influence.
- (U) In 2021, Section 702 data enabled U.S. diplomats to demarche a Middle Eastern country over its efforts to monitor and track dissidents abroad, as well as dissidents here in the United States.
- (U) In 2022, Section 702 data was vital in warning the international community, the private sector, and the public about efforts by North Korea to deploy information technology workers to commit fraud against a global industry, including against US businesses, to generate revenue for its nuclear program.

(U) Section 702 plays a key role in advancing the missions of each of our agencies.

- (U) Central Intelligence Agency (CIA): At CIA, Section 702 collection enables missions against the full range of foreign intelligence priorities—including all adversarial nation states, counterproliferation, cyber, counterintelligence, counternarcotics, and counterterrorism—and is foundational to our analysis in support of policymakers. Section

702 collection illuminates actionable opportunities against foreign individuals and networks of intelligence concern more comprehensively than any other single data source; for example, Section 702 collection enabled over 70% of the successful weapons and counterproliferation disruptions supported by CIA from 2018 to2022. Section 702 has also been used in efforts to prevent U.S. technology being acquired by adversaries for their advanced weapons programs, and Section 702 supports CIA's ability to run safe human intelligence operations abroad and gain invaluable insight into human assets, the individuals who have put their lives on the line to work for the United States.

(U) Moreover, every day CIA analysts produce dozens of products to inform the President, Congress, and other senior officials within our government, and a sizeable proportion of the intelligence that goes into these products comes from Section 702 collection. To take one example, the WIRe—or the World Intelligence Review—is one of CIA's primary tools for disseminating intelligence electronically. CIA analysts cited at least one FISA Section 702 intelligence report in nearly 40% of WIRe products published over the past year. FISA Section 702–derived intelligence reports are published by several agencies, and they are most-often cited in WIRe products on some of our most critical intelligence targets.

(U) National Security Agency: Section 702 is essential to NSA's foreign signals intelligence (SIGINT) mission: Approximately 20% of NSA reporting in 2022 contained Section 702 information, and 702 also plays a significant role in enabling SIGINT collection under other authorities. Intelligence obtained from Section 702 has protected U.S. and allied forces, stopped significant terrorist plots, and prevented cyber-attacks. Section 702 also regularly provides NSA with insights into the strategic intentions of China, Russia, Iran, and North Korea. Across all of NSA's mission areas, this authority is an invaluable resource. 100% of the President's intelligence priorities topics reported on by NSA were supported by the Section 702. With Section 702, NSA's ability to provide intelligence on the most significant threats to our nation would be significantly diminished.

- (U) Federal Bureau of Investigation: Section 702 collection is critical to the FBI's ability to fulfill its unique role and responsibility in the Intelligence Community, which is focused on protecting the homeland, and Americans, from foreign threats. The FBI uses Section 702 across the entire range of its national security investigations: to go after foreign terrorist organizations seeking to conduct attacks within the U.S., counter foreign spies and proliferators, and get in front of increasingly sophisticated and prolific foreign cyber actors targeting Americans.

  (U) Section 702 is a particularly, and increasingly, important tool in the FBI's mission to protect the United States and its critical infrastructure from malicious foreign cyber activity. Its agility is especially important in a technology environment where those foreign cyber actors can move to new communication accounts and infrastructure in a matter of hours, if not minutes. Section 702 produces valuable insight the FBI uses to notify victims who often don't know they've been compromised, warn targeted entities

who are likely to be compromised next, and provide unclassified threat intelligence to help mitigate active or recent intrusions and prevent potential future incidents.

(U) Many of the most significant examples of the utility and importance of Section 702 remain classified by virtue of the need to protect intelligence sources and methods. While classified examples are available to this Committee, it is essential that the legislative and public discussion of these authorities be informed, to the extent possible, by concrete examples of its value. To that end, the Intelligence Community is working to declassify additional examples of the role Section 702 plays in defending the United States and its citizens.

**(U) III. Overview of Section 702**

*(U) Origin of Section 702*

(U) When Congress first passed FISA in 1978, it primarily intended for the law to regulate surveillance activities inside the United States. The advent of the Internet and changes in the technology supporting international communications led to significant unintended consequences in the operation of FISA. As a result of these technological changes, terrorists, hackers, spies, and other foreign intelligence targets abroad used communications services based in the United States, including those provided by U.S.-based Internet service providers (ISPs).

(U) Prior to the enactment of Section 702, when the Intelligence Community wanted to collect communications between, for example, two terrorism targets both located overseas who happened to be using a U.S.-based ISP, the government was required to obtain a court order under Title I or Title III of FISA ("traditional FISA") from the Foreign Intelligence Surveillance Court (FISC). A traditional FISA order requires that the government demonstrate probable cause that the target is a foreign power or an agent of a foreign power and, in the case of Title I orders, that the target is using or about to use the targeted facility, such as a telephone number or an e-mail account. Requiring individual court orders for intelligence collection aimed at non-U.S. persons abroad was both extraordinarily burdensome operationally and unnecessary legally, because the Supreme Court has held such individuals are not entitled to Fourth Amendment protections. Indeed, no other country is known to require individualized court orders to authorize intelligence activities targeting foreigners outside their borders.

(U) Requiring traditional FISA orders became operationally unsustainable in the years following the 9/11 terrorist attacks because of the increasing terrorist threats emanating from overseas to the United States and our allies. In 2008, against this backdrop, Congress enacted Section 702 as part of the FISA Amendments Act (FAA).[1] As mentioned above, Section 702 authorizes the

[1] (U) The FAA added several other provisions to FISA. Section 701 provides definitions for the Act. Section 703 allows the FISC to authorize an application targeting a U.S. person outside the United States where the acquisition is conducted in this country. Section 704 provides additional protections for collection activities directed against U.S. persons outside of the United States. Sections 703 and 704 require a finding by the FISC that there is probable cause that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. Section 705 allows the government to obtain various authorities simultaneously. Section 708 clarifies that nothing in

government, with the approval and oversight of the FISC on a programmatic basis, to compel the assistance of providers in the United States in obtaining communications of non-U.S. persons located outside the United States to acquire foreign intelligence information. It allows the government to target for collection *only* foreign targets located overseas that are reasonably assessed to have foreign intelligence information.

(U) The statute also provides for comprehensive oversight by all three branches of government. This ensures the information collected about non-U.S. persons overseas is used responsibly and protects the constitutional and privacy interests of Americans whose information may be incidentally acquired when collecting foreigners' communications.

*(U) Legal Structure*

(U) Under Section 702, the FISC approves annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that specify classified categories of foreign intelligence that the government is authorized to acquire pursuant to the authority. The certifications serve as the legal basis for targeting specific non-U.S. persons outside the United States. Based on the certifications, the Attorney General and the DNI can direct U.S. communications service providers to assist in collection against authorized Section 702 targets. The FISC also reviews and approves the agencies' targeting, minimization, and querying procedures on an annual basis.

(U) Multiple provisions ensure that targeting is properly aimed at non-U.S. persons located outside the United States who are likely to possess, receive, or communicate foreign intelligence information that falls within one of the specified categories. First, the law requires the Attorney General and the DNI to certify that a significant purpose of an acquisition is to obtain foreign intelligence information. Second, only non-U.S. persons may be targeted. Third, the government may not target any person known at the time of the acquisition to be located in the United States at that time, regardless of whether they are a U.S. person. Fourth, the government may not target someone outside the United States for the purpose of targeting a particular known U.S. person or anyone in this country ("reverse targeting"). Fifth, Section 702 protects domestic communications by prohibiting the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of the acquisition" to be in the United States. Finally, of course, any collection must be consistent with the Fourth Amendment.

*(U) Targeting and Acquisition*

(U) An agency requesting authority under Section 702 must propose for court approval detailed procedures to ensure that it targets only non-U.S. persons outside the United States and also that it does not intentionally acquire domestic communications.

(U) The National Security Agency (NSA) initiates all Section 702 collection. NSA's targeting procedures require that there be an appropriate foreign intelligence purpose for the acquisition and that a "selector" associated with a particular target—like a phone number or e-mail

---

the FAA is intended to limit the government's ability to obtain authorizations under other parts of FISA. All provisions added by the FAA would expire if Section 702 is not reauthorized.

address—be used by a non-U.S. person reasonably believed to be located outside the United States. An analyst must conduct due diligence to identify information in the NSA's possession that may bear on the location or citizenship status of the potential target. NSA's basis for obtaining communications associated with a particular selector must be documented, and DOJ reviews the documentation for every selector.

(U) Under Section 702, each target is approved for tasking based on an individualized determination. The Intelligence Community has reported that approximately 246,073 targets were authorized for collection under the Section 702 program in 2022.

(U) FBI and CIA do not initiate Section 702 collection but may nominate selectors to NSA for collection.[2] FBI, CIA, and NCTC also do *not* receive all Section 702 collections, but only a small fraction relevant to their respective missions. For example, FBI may receive information only as to those Section 702 targets that the FBI determines are relevant to a full, predicated FBI national security investigation. As of 2022, that amounted to approximately 3.2% of all Section 702 targets.

*(U) Minimization, Querying, Dissemination, and Use*

(U) Under the statute, each agency must have its own minimization procedures. These impose strict controls with respect to all acquired data, regardless of the nationality of the individual to whom the data pertains. All personnel who are granted access to Section 702 information are required to receive training on the minimization procedures. The minimization procedures specify the duration of time for which data can be retained.[3]

(U) Since 2018, the statute has required the government to have separate procedures governing queries, which had previously been addressed as part of minimization procedures. Queries do not result in any additional collection. Rather, they allow an agency to quickly and effectively locate foreign intelligence information within what the agency collected previously through the use of Section 702. The query procedures limit the ways in which personnel can query Section 702 data using a term that is associated with a U.S. person, such as a name or telephone number. As discussed further below, U.S. person queries of Section 702 collection help us detect and evaluate connections between lawfully targeted non-United States persons involved in terrorist plots, cyber attacks, and other national security threats and U.S. persons.

(U) Queries are subject to a three-part standard. First, the query must have an authorized purpose: to obtain foreign intelligence information, or, only in the case of the FBI, to obtain evidence of a crime. Second, the query must be reasonably designed for that purpose. And third, there must be a specific factual basis to believe the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime. As described below, the Intelligence Community

[2] (U) NCTC does not initiate Section 702 collection or nominate selectors to NSA for collection.

[3] (U) In cases in which, despite the government's initial reasonable belief to the contrary, a target is found to be located in the United States or is discovered to be a U.S. person, the procedures require the collected data to be purged, except in the limited circumstance whereby, for example, the Director of the NSA determines that the collection contains significant foreign intelligence information.

and DOJ in recent years have taken steps to impose additional privacy safeguards surrounding querying of Section 702 data.

(U) There are also additional controls on the dissemination and use of Section 702–acquired information. An agency is permitted to disseminate information identifying a U.S. person to other entities only under the limited exceptions in the minimization procedures, for example, when such information is foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime. The statute dictates that all FISA-acquired information, including Section 702 information, may be used in a criminal proceeding only with the approval of the Attorney General. Additionally, the government must give notice to individuals if the government intends to use information against them that is either obtained or derived from Section 702. The statute also prohibits the use in a criminal proceeding of any communication to or from, or information about, a U.S. person acquired under Section 702, except for crimes involving national security or in a limited set of additional enumerated serious crimes.[4]

**(U) IV. Privacy Protections: Compliance, Oversight, and Transparency**

(U) The government is committed to ensuring that the Intelligence Community's use of Section 702 is consistent with the law, complies with FISC orders, and protects the privacy and civil liberties of Americans. By approving the annual certifications, as well as the targeting, minimization, and querying procedures, the FISC plays a central role in ensuring that Section 702 activities are conducted lawfully—consistent with statutory and constitutional requirements. The FISC may require the government to provide additional filings and testimony at hearings to ensure that the court has a full understanding of the operation of the program. In addition, on multiple occasions, the FISC has appointed amici curiae to address Section 702–related legal questions. In the annual evaluation of whether a proposed certification meets all statutory and constitutional requirements, the FISC makes findings regarding the operation of the program and the government's compliance record.

(U) Internal components in each agency with access to Section 702 information, including Inspectors General, oversee activities conducted under the authority. All Section 702 targeting decisions made by NSA are reviewed at least three times—by the drafting analyst, the more senior analyst, and a specifically trained adjudicator—prior to tasking and are further reviewed by NSA compliance personnel and DOJ National Security Division (NSD) personnel after tasking. CIA and FBI require multiple layers of review before nominating selectors to NSA for tasking to Section 702. NSA, CIA, and FBI require that all personnel who nominate selectors for

[4] (U) Other than national security crimes, FISA information may be used in criminal proceedings involving death, kidnapping, serious bodily injury as defined in section 1365 of Title 18, conduct that constitutes a criminal offense against a minor as specified in section 11 of the Adam Walsh Child Protection and Safety Act of 2006, incapacitation or destruction of critical infrastructure, cybersecurity, transnational crime, including transnational narcotics trafficking and transnational organized crime, and human trafficking.

tasking under Section 702 or task selectors complete training on targeting, minimization, and querying procedures, as well as on other agency policies.[5]

(U) DOJ personnel routinely review the agencies' targeting, querying, minimization, and dissemination decisions. This oversight includes DOJ's review of all tasking decisions by NSA and reviews at least once every two months at NSA, FBI, CIA, and NCTC to assess each agency's compliance with its legal procedures. In addition, agencies conducting activities under Section 702 must report promptly to DOJ and to ODNI incidents of noncompliance with the targeting, querying, or minimization procedures. NSD attorneys investigate each potential instance of non-compliance and work with the agencies to remediate any such instances. NSD reports any incident of noncompliance with the statute, court orders, or the approved legal procedures to the FISC and to Congress.

(U) As required by FISA, NSD submits reports regarding the government's use of Section 702 to the congressional intelligence and judiciary committees at least every six months. These semiannual reports are also provided to the FISC and include a description of every identified Section 702 compliance incident in the reporting period. NSD and ODNI also prepare semiannual joint assessments focused on compliance incidents impacting U.S. persons, compliance trends, and remedial measures. The joint assessments are provided to both Congress and the FISC. The FISA statute also requires the government to provide Congress with any pleading, FISC opinion, or order that contains a significant interpretation of the law.

(U) The Intelligence Community and DOJ work to be as transparent as possible with the public regarding the operation of the Section 702 program, consistent with the need to protect sources and methods. We have declassified and released FISC opinions regarding the authorization and operation of the Section 702 program. DOJ has provided to Congress every Section 702 opinion the FISC has issued to date. In addition, by statute, DOJ is required to produce to Congress any FISC opinion that includes a significant construction or interpretation of any provision of law or a novel application of any provision of FISA. Relatedly, the DNI, in consultation with the Attorney General, is required to publicly release such opinions containing a significant construction or interpretation of any provision of law.

**(U) V. Query Compliance and Remedial Measures**

(U) In recent years, a key oversight focus has been on queries of Section 702 information, in particular those involving U.S. person identifiers. As explained above, a query involves using a term to retrieve specific information from an agency's database of previously collected information. In other words, queries do not return newly collected data but merely retrieve lawfully collected data that is already stored in agency computer systems.

[5] (U) NCTC does not nominate or task selectors but instead receives a limited amount of counterterrorism information acquired pursuant to Section 702. Similar to the other agencies, NCTC is subject to specific minimization and querying procedures and requires all personnel with access to Section 702 information to complete annual training.

(U) Queries using U.S. person identifiers, such as a name or e-mail address, are critical to protecting U.S. national security. These queries can identify links between foreign threats and those inside the United States, including those related to terrorism, malicious cyber threats, hostile nation state activity, or other threats to the American people. U.S. person queries are especially important at the early stages of a national security investigation. They can help the government learn critical information needed to protect U.S. victims of malicious foreign adversaries, and they can help the U.S. government learn more about significant threats by foreign surveillance targets in contact with U.S. persons.

(U) This is particularly true for the FBI, which is responsible for protecting the homeland from national security threats emanating from overseas. In many cases, the FBI conducts U.S. person queries to identify U.S. person victims of foreign hacking or spying to enable the agency to warn and protect those individuals. These queries are vital to the ability to protect Americans from terrorism and from escalating cyber and espionage threats. To name but a few examples:

- (U) The FBI U.S. person queries against Section 702-acquired information to identify the extent of a foreign government's kidnapping and assassination plots. The timely identification of the foreign government's plans and intentions in Section 702-acquired information contributed to the FBI's disruption of the plots.

- (U) Through U.S. person queries of Section 702-acquired information, FBI discovered that Iranian hackers had conducted extensive research on the former head of a Federal Department. FBI then notified that individual and the Department of the specific threat, so they could take action to protect them and help secure their accounts.

(U) Just as this tool is critical to protecting the nation, it is vital that the government maintain the trust and confidence of Congress, the courts, and the American public in its use of Section 702 information. In recent years, oversight by DOJ and ODNI has identified serious compliance issues in the FBI's queries of FISA collection for information about U.S. persons. These incidents were reported promptly to the FISC and Congress, and they are described in detail in court opinions that are now public.

(U) The most recent such opinion, which was issued in spring of 2022 and declassified in May 2023, reflects a number of serious incidents of non-compliance, including improper queries of Americans involved in peaceful protests. These incidents are unacceptable. The FBI, the DOJ, and the entire Intelligence Community are committed to addressing them completely, including by implementing stronger safeguards and accountability mechanisms. All these incidents predated a set of significant reforms undertaken by the FBI beginning in the summer of 2021, which are discussed below and were designed to address the root causes of these incidents and prevent similar errors from occurring again.

(U) In 2021 and 2022, FBI worked with DOJ and ODNI to institute remedial measures that have since significantly strengthened compliance. These measures include:

- (U) Requiring FBI Personnel to "Opt-In" to Query Unminimized Section 702 Information: In June 2021, the FBI changed the default settings in the systems where it

stores unminimized Section 702 information so that FBI personnel with access to unminimized FISA Section 702 information need to affirmatively "opt-in" to querying such information. This system change was designed to address the large number of inadvertent queries of unminimized Section 702 information DOJ had identified in its reviews, in which FBI personnel did not realize their queries would run against such collection.

- (U) Heightened Approvals on Large Batch Job FISA Queries: Also in June 2021, the FBI instituted a policy requiring FBI attorney approval prior to conducting a "batch job" that would result in 100 or more queries. The term "batch job" refers to a capability in one of the FBI's systems that allows FBI personnel to more efficiently run queries involving multiple query terms. Attorney preapproval is aimed at providing additional review in situations where one incorrect decision could potentially have a greater privacy impact due to the large number of query terms.

- (U) Supplemental Guidance and Mandatory Training on Query Requirements: In November 2021, DOJ, ODNI, and the FBI issued new comprehensive guidance to all FBI FISA users on the proper application of the query rules, and in December 2021, the FBI instituted new mandatory training on that guidance, which personnel were required to complete by the end of January 2022. The FBI expanded and updated this training at the end of 2022. On an annual basis, all FBI personnel with access to unminimized FISA information are required to complete the expanded and updated query training or lose access to FISA systems.

- (U) Requirement for Case-Specific Justifications for U.S. Person Query Terms in FBI Systems: In the fall of 2021, at the direction of the FISC, the FBI modified its systems containing unminimized Section 702 information to require a case-specific justification for every query using a U.S. person query term before accessing any content retrieved by such a query from unminimized Section 702 information. Previously, personnel were permitted to use a pre-populated common justification, when applicable, for the query. These case-specific justifications are subject to review and audit by DOJ as part of its regular oversight reviews.

- (U) New Restrictions and Oversight of Sensitive Queries: In March 2022, the FBI instituted a new policy requiring enhanced preapproval requirements for certain "sensitive" queries, such as those involving elected officials, members of the media, members of academia, or religious figures. Under the new policy, an FBI attorney must review these queries before they are conducted. The FBI's Deputy Director must also *personally approve* certain queries before they can be conducted. This measure was designed to ensure that there is additional review at a leadership level of queries that reflect particular investigative sensitivities.

(U) These initial remedial measures are already achieving significant compliance benefits and

protecting privacy. For example, the number of U.S. person queries FBI conducted in 2022 was approximately 200,000, more than a 93% decrease from the previous year. Further, the FBI's Office of Internal Auditing—established at the direction of former Attorney General Barr to audit the FBI's use of its national security authorities—found an increase in the FBI's rate of compliance with the FISA query standard from 82% before these measures were instituted to 96% after their implementation.

(U) Implementation of robust privacy protections is not a one-time solution but rather an ongoing and iterative process involving repeated review and evaluation. DOJ and the FBI are continuing to develop additional measures to enhance privacy protections and ensure personnel comply with existing policies.

(U) Compliance reviews conducted by DOJ and ODNI have found that deliberate misconduct with respect to Section 702 information is extremely rare. In those rare cases of intentional misconduct, the individuals involved are referred for investigation and appropriate action—up to and including suspension, revocation of security clearance, or termination. By contrast, the vast majority of the compliance issues that prompted DOJ and FBI's remedial measures were the result of FBI personnel misunderstanding the rules governing U.S. person queries. For example, in some other instances, FBI personnel queried raw Section 702 information inadvertently, without realizing that the Section 702 dataset was included in the query as a default. However, DOJ and FBI are committed to addressing these unintentional errors, and the remedial measures described earlier are designed to do so; DOJ and FBI are also working to implement additional measures to ensure compliance.

**(U) VI. Potential Reforms to Section 702**

(U) The Administration is committed to working with Congress to address concerns regarding the use of Section702 and to identify reforms to enhance privacy and civil liberties protections while fully preserving Section 702's efficacy.

(U) As discussed above, the FBI has imposed a number of remedial measures, the codification of which could serve as the starting point for additional statutory reforms. This would entrench these policies into law, making them hard to undo. The Executive Branch is committed to working with this Committee and the Congress to explore potential additional changes to enhance the authority and its associated privacy, oversight, and transparency functions.

(U) However, it is essential that we pursue reforms that do not impair the benefits of Section 702; doing otherwise would imperil U.S. national security. In particular, more sweeping proposals—such as prohibiting U.S. person queries, imposing a warrant requirement for all such queries, or barring the FBI from receiving Section 702 collection—would force the government to turn a blind eye to threat information that it had lawfully acquired, with potentially grave consequences to our nation's security.

(U) But there is no need to go down that path. Other reforms would meaningfully enhance Section 702 safeguards while also continuing to preserve its national security benefits. We look

forward to continuing to work with this Committee and others in the Congress regarding such proposals.

**(U) VII. Conclusion**

(U) Section 702 is an indispensable foreign intelligence tool that allows our Intelligence Community to target non-U.S. persons located outside the United States to acquire information critical to our national security. Courts have repeatedly found that Section 702 is consistent with the Constitution and upholds the rights of Americans. Section 702 operates under stringent procedures and is subject to oversight from all three branches of government. In a world in which digital authoritarianism and technological repression are on the rise, Section 702 is a model for democratic countries to conduct intelligence activities consistent with the rule of law.

(U) The government recognizes the enormous responsibility it has to use this tool responsibly, protect the privacy and civil liberties of U.S. persons, and uphold the trust and confidence placed in the law enforcement and intelligence community. We are committed to addressing mistakes, being transparent with you and the American people, and continually reinforcing a system and culture that protects Americans' privacy and civil liberties. We look forward to working with this Committee on reauthorization of this critical tool that advances our shared goal of protecting the United States.

**U.S. Department of Justice**

Office of Legislative Affairs

*Office of the Assistant Attorney General* *Washington, DC 20530*

The Honorable Richard J. Durbin
Chair
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chair Durbin:

Please find enclosed responses to questions arising from the appearance of the Assistant Attorney General for National Security, Matthew G. Olsen, before the Committee on June 13, 2023, at a hearing entitled "Section 702 of the Foreign Intelligence Surveillance Act." We apologize for our delay in providing these responses.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that there is no objection to the submission of this letter from the perspective of the Administration's program.

Sincerely,

Slade Bond
Deputy Assistant Attorney General

Enclosure

cc:

The Honorable Lindsey O. Graham
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

# SJC Questions For the Record – AAG Olsen's June 13, 2023

## Senator Mike Lee

1. **Mr. Olsen, regarding DOJ's investigation of the events on January 6, 2021, you stated "the department's investigation is the single largest domestic terrorism investigation in the nation's history." Just a few weeks ago, we received the declassified FISA Court opinion revealing that the FBI conducted backdoor searches of the Section 702 database for "January 6th Capitol violence" in violation of the law. In this same interview, you also said "we are upholding our oath to defend the Constitution against those who tried to prevent the peaceful transfer of power." I find that statement rich considering how many times the DOJ and FBI have violated the constitutional rights of Americans by conducting these illegal searches. They aren't just "noncompliant searches"—every time you read an American's email or listen to their phone call without legal authorization, you are violating their constitutional rights. Now you are asking us to reauthorize Section 702 with little or no reforms. How are we supposed to believe that you will follow the law this time and not continue to illegally spy on Americans for political reasons?**

**Response:** The breadth of the Federal Bureau of Investigation (FBI) past non-compliance with the rules that govern querying Section 702 information using U.S. person identifiers ("U.S. person queries") is unacceptable. In response to the incidents, the FBI has implemented significant measures to address the causes of non-compliance. The initial tranche of such measures, implemented in 2021 and 2022, included:

1. Opt-in: FBI systems for storing unminimized FISA Section 702 information were updated to require personnel to affirmatively "opt-in" to query that information, reducing the risk of inadvertent queries.
2. Batch query approval: FBI personnel were required to obtain pre-approval from an FBI attorney to conduct a "batch job"—a combined query of many terms—when it would result in 100 or more queries.
3. Sensitive query approval: FBI policies were updated to require personnel to obtain FBI attorney pre-approval to conduct queries that present certain investigative sensitivities. In addition, the FBI's Deputy Director must also personally approve certain types of sensitive queries—such as those involving domestic public officials—before they may be conducted.
4. Case-specific justifications: FBI systems were changed to require agents and analysts to enter a case-specific justification for every Section 702 query using a U.S. person query term before accessing any content retrieved by such a query.
5. Revised query guidance and training: In November 2021, the Department of Justice (the Department), the Office of the Director of National Intelligence (ODNI), and the FBI issued new comprehensive guidance to all FBI FISA users on the proper application of

the query rules, and in December 2021, the FBI instituted new mandatory training on that guidance, which personnel were required to complete by the end of January 2022. The FBI expanded and updated this training at the end of 2022. On an annual basis, all FBI personnel with access to unminimized FISA information are required to complete the expanded and updated query training or lose access to FISA systems.

In June 2023, the FBI announced it was building on these compliance reforms in two ways: (1) *all* "batch jobs" would be subject to attorney pre-approval, regardless of the number of queries involved; and (2) the FBI systems would prompt personnel to enter a case-specific justification for each U.S. person query *before the query is ever run*. The FBI also implemented new accountability procedures in June 2023, which impose escalating consequences for compliance incidents resulting from negligence. More information can be found on the Department's website and FBI's website.

We are committed to working with this Committee and the rest of Congress on potential further reforms that improve transparency, accountability, and oversight without undermining the efficacy of Section 702.

Section 702 only authorizes targeting foreigners located abroad. But sometimes these foreign targets communicate with or about U.S. persons. If a foreign target communicates with a U.S. person inside the United States, that communication could be acquired based on targeting the foreign person's communications. Indeed, if we are monitoring a foreign terrorist or adversary, it is important to know if they are communicating with an individual inside the United States—either individuals who could be assisting them or who could be victims, including victims targeted by malicious cyber actors. Such "incidental collection" is not unique to Section 702, but in the context of Section 702 it has been found by the FISC and a number of other federal courts to be consistent with the Fourth Amendment.

A query involves using a term to retrieve specific information already lawfully acquired. The queries do not acquire additional data. Queries are a lawful means to identify relevant information already within an agency's holdings. Query rules and procedures approved by the FISC ensure that the IC seeks to query such communications using U.S. person identifiers only when they are reasonably likely to retrieve foreign intelligence information or, in the case of FBI, evidence of a crime. With respect to the FBI, the only Section 702 data that FBI has available in its analytic databases concerns targets who are relevant to predicated FBI national security investigations—approximately 3.2% of the total number of 702 targets as of 2022. The queries FBI personnel conducted in instances described in the FISC's 2022 opinion did not comply with the FISC-approved procedures required under the FISA statute.

6. **In the 24th Joint Assessment of compliance with Section 702, the oversight team noted that an FBI analyst queried a congressman's name. The report notes that the analyst committed a violation by failing to make the query narrower, but that the query was otherwise allowed under current rules. Can you definitively state this is**

**the only time an elected official has been the subject of a Section 702 US person query?**

**Response:** Section 702 does not authorize the FBI to target for collection communications of any U.S. person or any person inside the United States, including members of Congress. From time to time, however, the FBI may query lawfully collected communications—obtained exclusively by targeting foreign targets who are outside the United States—using identifiers associated with public officials, such as members of Congress. That may happen because other information suggests they may be the targets of foreign intelligence organizations, cyber intrusions, or foreign malign influence campaigns.

Of course, such queries still must meet the rigorous query standard outlined in the FBI's query procedures, which has three prongs:

- Purpose: queries must have an authorized purpose (retrieving foreign intelligence or evidence of a crime);
- Design: they must be reasonably designed; and
- Justification: they must be justified, meaning that the agent or analyst conducting the query must have a specific factual basis to believe that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection.

The query of the U.S. congressman mentioned in the 24th Joint Assessment satisfied the purpose and justification prongs of the query standard. But it failed the design prong of the query standard because it was overly broad as constructed (*i.e.*, queried the congressman's name with no limiters).

Since March 2022, the FBI has instituted a policy requiring that all U.S. person queries involving domestic public officials be pre-approved by the Deputy Director. In the FISC's April 2023 opinion approving the government's 702 certifications and procedures, the court described a set of four non-compliant queries conducted in June 2022 of the last names of a U.S. Senator and a State Senator. As the FISC noted, the analyst had an appropriate purpose and justification to conduct the queries. But the queries failed the design prong of the query standard because they were overbroad. The analyst also failed to follow the pre-approval policy, which had been instituted a few months before the queries were run.

7. **The compliance report cited in question #1 also highlighted that a local political party was subject to a U.S. person query. Can you definitively say that this has happened only once?**

**Response:** To be clear, Section 702 may not be used to target the communications of U.S. persons or domestic institutions or anyone inside the United States. The non-compliant queries of a local political party described in the 24th Joint Assessment were not reasonably likely to retrieve foreign intelligence and should not have occurred.

8. **The same compliance report also revealed that multiple U.S. government officials, journalists, and political commentators were subject to a batch query under Section 702. Can you definitively state that this is the only time U.S. government officials, journalists, and political commentators have been the subject of U.S. person queries?**

**Response:** Because U.S. person queries involving domestic public officials, journalists, and political commentators present particular investigative sensitivities, since March 2022, the FBI has instituted a policy requiring pre-approval for queries involving such sensitive query terms. In the case of queries associated with journalists (both foreign and domestic) and domestic public officials, the FBI must obtain prior approval from the Deputy Director, in addition to a senior FBI attorney, before running the query. Such queries may be conducted, for example, to identify foreign malign influence activities.

9. **FBI officials, including Director Wray, have emphasized that the FBI is now querying Americans hundreds of thousands of times each year, down from several million, after implementing new compliance measures. Has this drop in queries jeopardized national security, or was the FBI conducting millions of unnecessary warrantless searches for Americans' information before the new measures were put in place? And if the latter is the case, why should we believe the government now if, during this reauthorization process, you say that reforms to protect Americans' privacy will jeopardize national security?**

**Response:** As reported in the Office of the Director of National Intelligence Annual Statistical Transparency Report, the number of FBI U.S. person queries decreased from approximately 3.4 million in 2021 to approximately 200,000 in 2022. The 2021 figure was inflated largely as a result of a number of large batch jobs that were run related to one particular investigation involving attempts by foreign cyber actors to compromise U.S. critical infrastructure. These queries included approximately 1.9 million queries related to potential victims.

In June 2021, the FBI changed the default settings in the systems where it stores unminimized Section 702 information so that FBI personnel with access to unminimized FISA Section 702 information need to affirmatively "opt-in" to querying such information. This system change was designed to address the large number of inadvertent queries of unminimized Section 702 information the Department had identified in its reviews, in which FBI personnel did not realize their queries would run against such collection. Historically, users were automatically opted in to querying unminimized Section 702 information in these databases if they had been authorized to access unminimized Section 702 information. This meant that agents or analysts conducting routine database checks for investigations unrelated to foreign intelligence were querying raw FISA by mistake.

We assess this opt-in change is largely responsible for the sharp decrease in U.S. person queries and has not only decreased the number of U.S. person queries overall but has also greatly

reduced the number of inadvertent queries. In addition, based on the Department's recent reviews, FBI appears to be conducting fewer "batch job" queries, which has further reduced the number of U.S. person queries.

So far in 2023, there has been a further reduction in U.S. person queries. It is worth noting, however, that mission needs that arise in the future years could cause the number of U.S. person queries to rise and fall from year to year, consistent with the new remedial measures that were put in place.

By contrast, some reforms that have been proposed to Section 702, such as requiring an individualized court order for each U.S. person query, would undermine the IC's ability to use U.S. person queries *in every instance*, including those that are critical to our ability to identify and disrupt homeland threats.

10. **The 2021 FISA Court opinion noted that the FBI had continued to use a system that does not comport with minimization procedures because it couldn't keep track of when agents were warrantlessly searching Section 702 data for information about Americans. According to the FISA Court, this system directs agents to create a required justification on a separate SharePoint site, and there has been "systemic" non-compliance with that direction. I understand that the FBI is in the process of terminating transmittal of Section 702-derived information to that system and ultimately removing that information. Is it not cause for concern that government agencies have continued to use a system that *could not be* compliant for years? Has use of this non-compliant system stopped entirely? If not, please provide a date by which you expect that process—including removal from SharePoint of all Section 702-derived information—to be finished.**

**Response:** As referenced in the opinion issued by the FISA Court on April 21, 2022 (hereinafter, the "2022 FISC Opinion"), as of October 27, 2021, the FBI had restricted access to unminimized Section 702-acquired information in the relevant system. At that time, FBI also stopped adding new Section 702-acquired information to the system. All Section 702-acquired information had been removed from the system prior to the issuance of the 2022 FISC Opinion.

NSD did not assess that the system "could not" be compliant with the FISA statute and procedures, or that the use of the separate SharePoint site was necessarily non-compliant. Rather, following the discovery that a material number of FBI users had failed to use the SharePoint site as instructed, NSD and FBI concluded that the system, as used in practice, did not comport with the procedures and should no longer contain Section 702-acquired information.

11. **It has become clear that data brokers and similar entities have swept in significant amounts of Americans' most sensitive data—where they pray, who they love and even their most intimate health information. It is also clear that the government—including our intelligence agencies—in lieu of obtaining a warrant under the Fourth Amendment, have purchased highly personal and constitutionally protected**

**information. The data broker-government pipeline raises significant civil rights concerns and is a threat to all Americans. On Friday, June 16, 2023, ODNI declassified a report by its Senior Advisory Group (SAG) on the Intelligence Community's purchase of commercially available information. The report revealed a number of alarming findings about the IC's purchase of data in bulk, including information about Americans. However, ODNI redacted key information revealing the types of information IC elements have purchased. What types of data does the Department of Justice purchase? Please include a breakdown by purchases by division or department.**

**Response:** The Department purchases or licenses commercially available information ("CAI") in connection with carrying out certain authorized core functions. Acquisition and use of this information is conducted in accordance with applicable laws, regulations, and policies, including those that protect personally identifiable information. Such acquisition includes CAI that foreign governments, private corporations, and state governments are legally permitted to purchase or license. The Department makes these purchases of CAI with due consideration for the preservation of individuals' privacy, civil rights, and civil liberties.

The Department purchases a variety of CAI to help carry out its core functions. Examples of types of CAI the Department purchases include legal research tools such as LexisNexis and Westlaw, public records search tools such as Thompson Reuters CLEAR, as well as credit reporting services such as Experian.

12. **What is the Department of Justice's current interpretation of *Carpenter* as it applies to third party data purchased from data brokers?**

**Response:** *Carpenter v. United States*, 138 S. Ct. 2206 (2018), held that the government's acquisition through compulsory process of seven or more days of historical cell-site location records created and maintained by a cell-service provider is a Fourth Amendment search generally subject to the warrant requirement. *Id.* at 2216-2223. The Court characterized its decision as "narrow," and it expressly declined to "express a view on matters not before us," including "other business records that might incidentally reveal location information." *Id.* at 2220. That language makes clear that the Court in *Carpenter* did not intend to address issues not before the Court, including the question of whether or how the Fourth Amendment might apply to third-party data purchased from data brokers.

13. **Does the DOJ interpret *Carpenter* to apply where the DOJ purchases Americans' data from data brokers? What are the parameters?**

**Response:** The Court in *Carpenter* emphasized that its decision was "a narrow one," that it did not "disturb the application of *Smith* and *Miller*" to other types of information, and that it did not "express a view" on other matters, including "other business records that might incidentally reveal location information." 138 S. Ct. at 2220. The Department accordingly has not

interpreted *Carpenter* as addressing matters not before the Court in that case, including whether or how the Fourth Amendment might apply to third-party data purchased form data brokers.

14. **In its recently declassified April 21, 2022 opinion regarding Section 702, the FISA Court admonished the FBI for its repeated violations of Americans' constitutional rights through backdoor searches of Americans' communications obtained under Section 702 of FISA. Page 28 of the opinion, describes one of many instances involving noncompliant searches involving January 6, 2021 as follows: "An analyst ran 13 queries of individuals suspected of involvement in the January 6, 2021 Capitol breach. The analyst said she ran the queries to determine whether these individuals had foreign ties and indicated she had run "thousands of names within FBI systems in relation to the Capitol breach investigation" and did not remember why she ran these 13 queries on raw FISA information. NSD concluded the queries were not reasonably likely to retrieve foreign intelligence information or evidence of a crime." In what other FBI systems did this analyst run "thousands of names" in relation to the January 6th investigation? Why were you not able to obtain a probable cause warrant in these instances?**

**Response:** As the 2022 FISC opinion notes, the Department reported these queries as compliance incidents because they did not satisfy the query standard as they were not reasonably likely to retrieve foreign intelligence information or evidence of a crime. The Department, accordingly, would not have sought an order from the FISC under Section 702(f)(2), as required when personnel seek to review content returned by U.S. person queries conducted purely to retrieve evidence of a crime in connection with a predicated FBI criminal investigation that is unrelated to national security, even if FBI had requested that it do so.

The FBI has more than 100 databases available for analytic review by its agents and analysts, representing data collected from a variety of sources and using a variety of legal authorities—including data from other Federal government agencies, foreign partners, public sources, and local law enforcement. While querying any of these databases requires an authorized purpose, queries of raw FISA data are subject to a heightened legal standard in light of their sensitivity—these queries must be "reasonably likely to retrieve" foreign intelligence information and/or evidence of a crime. Likewise, queries of raw FISA data are subject to oversight review by the Department to ensure compliance with this heightened standard. It was these oversight reviews that uncovered the noncompliant queries in question. However, because the oversight reviews are focused specifically on FISA compliance, the Department does not have information on queries of any non-FISA databases involving these incidents.

15. **According to the FISC opinion referenced in question #10, another analyst ran 23,132 separate queries regarding U.S. person search terms regarding those involved with January 6th looking for evidence of foreign influence. How should we not take this as evidence that the FBI searches the 702 database as a matter of course without due respect to statutory parameters or the Fourth Amendment and will continue to do so until Congress either outlaws backdoor searches of U.S. person information or requires a probable cause warrant?**

**Response:** This incident, as well as the other incidents described in the FISC's April 2022 opinion, were unacceptable and should never have occurred. In order to prevent such incidents from occurring in the future, the FBI took a hard look at the root causes of non-compliance and instituted a series of remedial measures beginning in the summer of 2021 and continuing through 2022 and 2023. These remedial measures have been effective, as found by the FISC in its opinion issued in April 2023, when the Court found the FBI's rate of compliance with the FISA query standard following the institution of the remedial measures to be above 98%. This rate of compliance with the query standard was generally consistent with the Department's own evaluations and those of the FBI's Office of Internal Auditing. The FBI is continuing to consider further remedial measures to prevent noncompliance.

16. **The Department of Justice and the FBI have stated that U.S. person queries are sometimes used to try to identify potential victims of foreign cyberattacks or potential targets of foreign influence. Is this a new use for U.S. person queries of Section 702 data? Why didn't this use come up during any of the testimony provided by government witnesses when Section 702 was reauthorized in 2018?**

**Response:** The use of Section 702 authorities to identify and respond to nation-state threats, including malicious cyber activity and foreign malign influence, is not new. Section 702 has authorized this this type of collection targeting non-U.S. persons outside the U.S. since its inception. However, as the cyber threat has evolved and our adversaries have grown more sophisticated over the past 15 years, the necessity of Section 702 and its utility to counter these threats has increased. In addition, the use of U.S. person queries to ascertain the extent of any of these threats to the homeland is not novel.

17. **When a domestic law enforcement agency is investigating a potential domestic cyberattack with no foreign connection, and they want to identify potential victims, can they ask a company such as Google to turn over Americans' communications without any kind of court order outside of Section 702?**

**Response:** In the case of a domestic-origin cyber incident, obtaining the contents of Americans' communications from a provider generally would require a court order. But often the most important clues to identifying cyber victims come in the form of technical information about an actor's online activity, not the content of communications. Pursuant to the Stored Communications Act, providers can disclose records and other non-content data without a court

order in certain emergency situations, with the consent of the subscriber, or to protect the provider's property.

**18. According to the ODNI's Annual Statistical Transparency Report for 2021, there were 1.9 million queries performed in 2021 to identify potential victims of cyberattacks, including U.S. persons. In how many of those 1.9 million cases did the query result in preventing harm that would have occurred but for that query?**

**Response:** The Department's response to this question is included in the classified addendum submitted by FBI.

**19. Please provide a detailed description of the process by which cyberattacks against U.S. persons or entities are proactively ameliorated via U.S. person queries.**

**Response:** The FBI regularly provides warnings and victim notifications to entities it identifies as being targeted or compromised by hostile foreign cyber actors through our FISA Section 702 collection. U.S. person queries of identifiers associated with the victims are a key part of how the FBI analyzes its Section 702 collection to identify relevant information to provide an informed victim notification to the compromised entity, so that they can take the appropriate corrective action to remedy the breach.

Further detailed information on this process is included in the classified addendum submitted by FBI.

20. **a. In February 2023, you announced that the DOJ is "imposing pre-approval requirements for certain types of sensitive U.S. person...questions," presumably meaning "queries." Who are these "U.S. person[s]" for whom queries are more "sensitive"? Do they have greater Fourth Amendment protections than other Americans?**

**Response:** As the "Recent Efforts to Strengthen FISA Compliance" memo released by the Department on February 28, 2023, indicates, in March 2022, the FBI instituted a new policy requiring pre-approval for certain types of sensitive queries, such as those involving domestic public officials, members of the news media, members of academia, or religious figures. Under the new policy, an FBI attorney must review these queries before they are conducted. The FBI's Deputy Director must also personally approve certain queries before they can be conducted. This measure was designed to ensure that there is additional review at a leadership level of queries that reflect particular investigative sensitivities.

**b. The 2021 FISC opinion on Section 702 discusses at length a "new—even expansive—application of the statute," under which the NSA collects what appears to be some form of non-communications information from electronic communications service providers. While the FISA Court ultimately blessed this**

**expansive application, it did note that the amicus had "marshaled impressive evidence" that Congress did not foresee this application of the statute. However, this section of the opinion is heavily redacted, leaving Americans to wonder what secret interpretation of law the government is operating under. How can the administration ask Congress to reauthorize Section 702, if at the same time it is refusing to tell the American people how this authority is really being used?**

**Response:** Although the FISC acknowledged that it did not appear Congress had this type of collection in mind when it passed Section 702, the Court also stated that "the legislative history's silence regarding a proposed application of a statute 'cannot override the words of the statute,'" and that "Section 702(a) provides the government broad authority to target persons outside the United States to acquire foreign intelligence information." (P. 94, citation omitted.) The portion of the opinion addressing this issue is heavily redacted because it concerns an exceptionally sensitive collection method that is properly classified, and the public release of additional details concerning this matter would be accessible to America's adversaries and therefore seriously jeopardize its effectiveness.

Although the government is not able to publicly release additional details regarding this matter, the government has provided classified versions of the opinion to the Senate and House Intelligence and Judiciary Committees that provide significantly more detail than the public version regarding the collection method and the Court's reasons for approving it.

**c. Will the government provide the American people more information about this new collection method and the government's new and expansive interpretation of 702?**

**Response:** As noted above, this new collection method is highly sensitive and is properly classified. The government has made efforts to release as much as possible about this collection method in the opinion that has already been publicly released and has also provided a classified version of the opinion to Senate and House intelligence and judiciary committees. The public release of additional details concerning this matter would seriously jeopardize its effectiveness.

**21. The government's purchase of Americans' most sensitive data from data brokers poses a grave risk to Americans' privacy—enabling agencies to monitor Americans' religious activities, political affiliations, intimate relationships, and more. It is also clear that government agencies—including our intelligence agencies—have purchased highly personal data, including data that is protected by the Fourth Amendment, instead of obtaining a warrant. However, according to a recently released report commissioned by the ODNI, the Intelligence Community has no community-wide, formal position on the constitutionality of purchasing geolocation information or other sensitive information about Americans. Has the Office of Legal Counsel issued any legal opinions relating to the government's purchase of**

**geolocation information or other sensitive information about Americans from data brokers or similar entities?**

**Response:** Pursuant to longstanding policy, the Department is unable to discuss nonpublic legal advice, including from the Office of Legal Counsel (OLC). With respect to the subject raised in your questions, OLC has not issued a published opinion, and the Department is otherwise unable to confirm or deny whether OLC has provided advice regarding that subject.

**22. If the answer to question #19 is yes, please submit to this committee within 60 days any and all relevant legal guidance, whether issued by OLC or by agencies, relating to the purchase of geolocation information or any other information for which compelled production would require a warrant, court order, or subpoena.**

**Response:** Pursuant to longstanding policy, the Department is unable to discuss nonpublic legal advice, including from OLC. With respect to the subject raised in your questions, OLC has not issued a published opinion, and the Department is otherwise unable to confirm or deny whether OLC has provided advice regarding that subject.

**Senator Thom Tillis**

**1. What is the cost to our national security of failing to reauthorize Section 702?**

**Response:** As the Attorney General and the Director of National Intelligence noted in their letter to Congress in February 2023, Section 702 has proven invaluable in protecting American lives and U.S. national security.

Section 702 has been used to identify and protect against national security threats to the United States and its allies, to include both conventional and cyber threats posed by the People's Republic of China, Russia, Iran, and the Democratic People's Republic of Korea. There is simply no way to replicate Section 702's speed, reliability, specificity, and insight. Without Section 702, we will lose indispensable intelligence for our decision makers and warfighters, as well as those of our allies. And we have no fallback authority that could come close to making up for that loss. We agree with the President's Intelligence Advisory Board, who stated in a report released in July that "history may judge the lapse of Section 702 authorities as one of the worst intelligence failures of our time."

**2. Specifically in the cybersecurity context, how has the use of Section 702 contributed to our ability to counter state actors like those from Russia and the CCP?**

**Response:** Section 702 has proven incredibly versatile. It was a critical source of information at the height of the post-9/11 counterterrorism threat, and now it enables the United States to gain unparalleled intelligence about the threats that will define this decade and the next, including cyber threats.

The Director of National Intelligence has recently declassified a number of real success stories of how Section 702 provided irreplaceable insight on cyber threats.

- Section 702 played an important role in the U.S. government's response to the cyberattack on Colonial Pipeline in 2021. Using Section 702, the IC acquired information that verified the identity of the hacker, as well as information that enabled government efforts to recover the majority of the ransom – sending an invaluable message to our adversaries to back down.
- Section 702-acquired information helped successfully identify and mitigate an Iranian ransomware attack against a non-profit organization's systems in 2022. Within one week, this intelligence enabled the U.S. Government to respond to, mitigate, and ultimately recover the organization's information without paying the ransom.
- U.S. person queries of Section 702 information helped the FBI identify efforts undertaken by the People's Republic of China to hack a transportation hub in the United States. The FBI identified where the hackers had achieved successful compromises of network infrastructure. This enabled the FBI to alert the network operators so they could take action to mitigate the intrusions.

**3. I understand you have been able to use Section 702 as a method to stop the flow of fentanyl into the US. What has DOJ been able to do here, and what would be the result of failing to reauthorize Section 702?**

**Response:** As CIA Deputy Director Cohen testified before the Committee, "[Section] 702 collection illuminates the networks and global supply chains used by foreign-based drug trafficking organizations. This includes how they manufacture and transport everything from precursor chemicals to their foreign labs, to their distribution of their product into the United States. . . . Without 702, we'd be missing essential information on the dangerous groups and individuals behind overseas fentanyl production and distribution[.]"

Section 702-acquired information has revealed the quantities and potency of drugs, including fentanyl, destined for illegal transfer to the United States, as well as specific smuggling techniques used to avoid detection. It also provided insights that have informed the U.S. Government's understanding of the Chinese origins of a chemical used to synthesize fentanyl.

To clarify, FBI receives raw Section 702 collection only for those targets that are relevant to a fully predicated FBI national security investigation. That does not currently include counternarcotics and organized crime investigations. But Section 702 information has been a vital piece of the IC's understanding of global fentanyl networks, and as the President's Intelligence Advisory Board recently highlighted in its report on Section 702, Section 702 information has contributed to the seizure of numerous fentanyl pills, powder, precursor chemicals, and production equipment.

**4. What steps have DOJ and the Intelligence community taken to protect the privacy of the American people from Section 702 searches?**

**Response:** Following a series of query compliance incidents identified by the Department's National Security Division (NSD) in its oversight reviews of FBI field offices, the FBI worked with NSD and the Office of the Director of National Intelligence (ODNI) to issue new, comprehensive guidance to the FBI's national security workforce on FISA queries. The results of those interagency efforts were two documents: the "FBI FISA Query Guidance" and a two-page desk reference companion document entitled "FBI FISA Query Guidance Nutshell." Both documents were issued to all FBI national security personnel in November 2021 and made available to the public on April 24, 2023.[1]

In December 2021, the FBI instituted new mandatory training based on these November 2021 guidance documents, which relevant FBI personnel were required to complete by the end of

[1] FEDERAL BUREAU OF INVESTIGATION, *FBI Releases FISA Query Guidance* (Apr. 24, 2023), https://www.fbi.gov/news/press-releases/fbi-releases-fisa-query-guidance#Background-Information:%20November%202021%20FBI%20FISA%20Query%20Guidance%20Documents.

January 2022 in order to maintain their access to FBI FISA systems. The FBI then expanded and updated this training at the end of 2022, and FBI national security personnel are now required to re-take the expanded FISA query training on an annual basis in order to maintain their access to FBI FISA systems.

Among other things, the FBI FISA query guidance documents make clear the three prongs of the FISA query standard:

- Purpose: queries must have an authorized purpose (retrieving foreign intelligence or evidence of a crime);
- Design: they must be reasonably designed; and
- Justification: they must be justified, meaning that the agent or analyst conducting the query must have a specific factual basis to believe that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection.

The guidance documents also clarify the rules governing so-called "evidence-of-a-crime-only" queries, which are queries of FBI FISA systems that are not designed to retrieve foreign intelligence information, but rather are seeking only to retrieve evidence of a crime. Finally, the guidance documents advise FBI personnel on the requirements of FISA Section 702(f)(2), a section of the statute that requires the FBI to obtain a court order in certain defined circumstances before accessing any content information retrieved by an "evidence-of-a-crime-only" United States person query.

These efforts to improve guidance and training were part of a series of measures the FBI undertook beginning in the summer of 2021 to improve FISA and FISA Section 702 query compliance. Other measures included:

- Opt-in: FBI systems for storing unminimized FISA Section 702 information were updated to require personnel to affirmatively "opt-in" to query that information, reducing the risk of inadvertent queries.
- Batch query approval: FBI personnel were required to obtain attorney pre-approval to conduct a "batch job"—a combined query of many terms—when it would result in 100 or more queries.
- Sensitive query approval: FBI policies were updated to require personnel to obtain attorney pre-approval to conduct queries that present certain investigative sensitivities. In addition, the FBI's Deputy Director must also personally approve certain types of sensitive queries—such as those involving domestic public officials—before they may be conducted.
- Case-specific justifications: FBI systems were changed to require agents and analysts to enter a case-specific justification for every Section 702 query using a U.S. person query term before accessing any content retrieved by such a query.

In June 2023, the FBI announced it was building on these compliance reforms in two ways: (1) *all* "batch jobs" would be subject to attorney pre-approval, regardless of the number of queries involved; and (2) the FBI systems would prompt personnel to enter a case-specific justification

for each U.S. person query *before the query is ever run*. The FBI also implemented new accountability procedures in June 2023, which impose escalating consequences for compliance incidents resulting from negligence. More information can be found on the Department's website and FBI's website.

The Department continues to conduct audits of FBI's queries of unminimized Section 702 information. Based on the results of these ongoing reviews, NSD has provided supplemental guidance on compliance trends to FBI, and FBI has updated its mandatory query-related training. Compliance and oversight is an ongoing process, and FBI and NSD/the Department continue to assess the efficacy of existing remedial measures to address the query compliance issues and identify additional remedial measures that are needed to improve compliance.

In May 2023, the FBI released the results of two query audits conducted by its Office of Internal Auditing (OIA).[2] Based on FBI OIA's second, post-reform audit, the FBI had a 96% compliance rate with the FISA query standard, a 14 percentage point improvement from OIA's first baseline audit, which examined queries that were conducted before the reforms. FBI OIA provided 11 compliance recommendations, all of which Director Wray accepted and directed his leadership team to implement. In its April 2023 opinion approving the government's 702 procedures and certifications, the FISC calculated that FBI queries audited as part of NSD's oversight complied with the query standard more than 98% of the time.

5. **How many personnel have access to unminimized Section 702 information?**

**Response:** In 2023, access to unminimized Section 702 information has been granted to less than 15% of FBI's workforce, including employees and other personnel such as detailees and contractors. A small number of additional personnel within the Department may have access to unminimized FISA information on occasion. For example, personnel within the Office of Intelligence (OI) in the Department's National Security Division sometimes view unminimized Section 702-acquired information while conducting their official duties. OI personnel are generally only able to view unminimized Section 702-acquired information when a member of the Intelligence Community (IC) who has access to such information shows specifically requested information to the OI personnel as part of preparing FISA applications or pursuant to OI's oversight-related work. OI personnel do not have independent access to IC systems containing raw FISA information. In addition, prosecutors within the Department may be granted limited, temporary access to unminimized FISA information in an FBI system on a case-by-case basis if needed in connection with satisfying applicable discovery obligations.

[2] FEDERAL BUREAU OF INVESTIGATION, *FBI Releases Results of OIA FISA Query Audit*, (May 11, 2023), fbi.gov/news/press-releases/fbi-releases-results-of-oia-fisa-query-audit.

*6.* **What is the procedure you follow when incidental collection occurs of communication with US persons?**

**Response:** The FISA statute requires that each agency have minimization and querying procedures governing the acquisition, retention, use, dissemination, and querying of Section 702-acquired information, including non-publicly available information concerning U.S. persons. When U.S. person information is collected pursuant to Section 702, whether because of incidental collection of communications with U.S. persons or because U.S. person information is contained in non-U.S. person communications, each of the relevant agencies applies these procedures to such information. The querying procedures generally require that queries of Section 702-acquired information meet a high standard—that the queries be reasonably likely to retrieve foreign intelligence information or, in the case of FBI, evidence of a crime. The minimization procedures require (among other things) that access to unminimized Section 702-acquired information be restricted, that disseminations of Section 702-acquired information meet the dissemination standard (and any U.S. person information in the dissemination be masked unless it also meets that standard), and that unreviewed data and data that has been reviewed and not determined to meet the retention standard be deleted after a specified period of time.

*7.* **How many Americans have had their communications included in Section 702 collection?**

**Response:** The Department defers to the National Security Agency, which has primary responsibility for the acquisition of communications pursuant to Section 702.

**Senator Peter Welch**

Where you are unable to answer a question completely because the answer is classified or for any other reason, please answer as much of the question as possible in the public record. Further, please explain why you cannot provide complete information publicly, to the extent possible, and indicate where you will follow up with the complete answer separately in a closed setting.

1. **Please provide the total costs incurred by your agency in support of FISA Section 702 collection, storage, and searching for each of the last five years.**

**Response:** Non-FBI personnel do not persistently collect, store, or search data pursuant to Section 702. Prosecutors within the Department may be granted limited, temporary access to unminimized FISA information in an FBI system on a case-by-case basis if needed in connection with satisfying applicable discovery obligations. We do not have an estimate of the costs associated with these tasks.

As an Intelligence Community element, FBI figures for budget and personnel associated with intelligence activities are classified. Further details are available in the classified addendum provided by FBI.

2. **Please provide the total number of personnel and contractors in your agency who perform oversight and compliance duties to ensure the lawful conduct of activities under FISA Section 702, along with the total related budget, for each of the last five years.**

**Response:** Approximately 60 people within NSD's Office of Intelligence perform oversight and compliance duties relating to the Section 702 program, although some of these individuals perform operational work in addition to oversight and compliance duties. The oversight and compliance program accounted for an average of $11.6 million out of NSD's budget for each of the last five years.

As an Intelligence Community element, FBI figures for budget and personnel associated with intelligence activities are classified. Further details are available in the classified addendum provided by FBI.

3. **Except pursuant to a warrant, are personnel or contractors of your agency authorized to conduct a U.S. person query of data collected under FISA Section 702 to search for evidence of a crime committed by an American, in the absence of any evidence of a connection to crime that transcends national boundaries?**

**Response:** Except in connection with satisfying discovery obligations, as described above, non-FBI personnel do not query raw Section 702 data. FBI personnel, unlike other IC elements, are authorized under Section 702 to conduct queries reasonably believed to retrieve evidence of a

crime. In the vast majority of cases, because Section 702 is a foreign intelligence collection tool, there is unlikely to be relevant information in the raw data pertaining to purely domestic crimes. In 2022, there were 16 instances in which FBI personnel reviewed information resulting from queries run purely to return evidence of a crime, and 14 of those were done to fulfill the Department's discovery obligations (*i.e.*, not to advance an investigation).

Section 702(f)(2) of FISA requires that if an evidence-of-a-crime query pertains to a predicated FBI criminal (i.e. non-national security) investigation, the FBI must obtain an order from the FISC before reviewing any content returned.

4. **Has your agency purchased, received, or otherwise come into possession of commercial datasets that contain the location information of Americans or communications of Americans, including related metadata, within the last five years?**
    a. **If yes, has your agency intentionally accessed that information related to Americans in any manner except pursuant to a court order?**
    b. **Please provide copies of all written policies that govern obtaining, retaining, or using commercial datasets containing information of Americans.**

**Response:** In recent years, commercially available information (CAI) lawfully obtained from commercial entities, some of which may contain locational data, has become an important tool in law enforcement and national security investigations and activities, providing invaluable leads, helping bring offenders to justice, and protecting victims and potential victims of crime.

The Department recognizes that misuse of information and information technology risks undermining public trust. It is the policy of the Department to utilize CAI, as it does all information in its possession, in an appropriate and responsible manner that advances the Department's mission, promotes public safety, and protects privacy, civil rights, and civil liberties.

At present, the Department has several policies in place that govern the acquisition and use of data, including:

1. Order 0601, *Privacy and Civil Liberties*, which provides that the Department consider appropriate privacy protections in the collection, storage, use, dissemination, and security of personal identifying information;

2. Order 0903, *Information Technology Management*, providing that the Department acquire, manage, and use information technology in a secure manner that enhances mission accomplishment, improves work processes, provides sufficient privacy protections, and complies with all applicable federal laws and directives; and

3. Order 0908, *Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information*, which mandates the appropriate use of departmental information technology.

In addition to the policies listed above, the Department has a Data Brokers Working Group tasked with exploring how the Department engages with data brokers and, if appropriate, developing recommendations for Department leadership about how to use such services effectively and with due regard for Americans' privacy, civil rights, and civil liberties. The Working Group is comprised of representatives from across the Department, including subject matter experts in data procurement and use, and is co-chaired by the Office of Legal Policy and the Office of Privacy and Civil Liberties. The Department's work in this area is ongoing.

The Department adheres to the legal rules imposed by the Constitution and other governing laws, including Supreme Court precedent, in the use of non-invasive, open-source collection techniques to gather information through the purchase of CAI.

5. **Please provide the complete demographic breakdown of the targets of U.S. person queries of data collected under FISA Section 702 for the last five years. This information should include, but is not limited to, age, gender, sex, race, ethnicity, economic class, residence, nationality, and country of origin. To the extent that this this information is only partially tracked by your agency, please provide the information available and provide copies of written policies that govern the collection and analysis of this demographic data.**

**Response:** None of the IC agencies with access to raw FISA information maintains records of the demographic data associated with the U.S. person identifiers that are queried in the FISA database.

6. **Does your agency currently deploy any AI tools across the database of information collected under FISA Section 702, and does your agency have any plans to do so within the next five years?**

**Response:** Non-FBI components of the Department do not collect, store, or (except in connection with satisfying discovery obligations, as described above) query unminimized Section 702-acquired information, and have no plans to collect, store, or query such information in the next five years. The Department therefore has no such information against which to deploy such tools.

7. **How does your agency define "intentional misconduct" and "negligence" in the context of agency personnel or contractors conducting improper U.S. person queries of FISA Section 702 data?**
    a. **Please provide copies of all related written policies.**

**Response:** The Department's main function in reviewing U.S. person queries of Section 702 conducted by the IC is to determine whether they complied with the FISA statute and the FISC-approved query procedures required by the statute. The Department reports instances of non-compliance to the FISC and to Congress. Each agency is responsible for imposing any personnel consequences, as appropriate, based on non-compliant queries.

8. **The April 2022 FISC memorandum opinion and order revealed that the FBI unlawfully conducted U.S. person queries of data collected under FISA Section 702 in 278,000 instances. Mr. Abbate testified that all such queries were "unintentional." Has the FBI or DOJ ever identified misconduct that rose beyond negligence in the policy or practice of agency personnel or contractors searching FISA Section 702 data?**

**Response:** In connection with its reviews of FBI field offices, the Department has seen rare instances of FBI personnel conducting noncompliant queries where the cause of the noncompliance appeared to be willful misconduct. In one such instance, for example, where the Department identified intentional misconduct with respect to noncompliant queries, the individual lost their job at FBI.

Further details on these instances involving FBI personnel intentionally running non-compliant queries are available in the classified submission from the FBI.

9. **Has the DOJ or FBI ever recommended or pursued prosecution for an agency employee or contractor who improperly queried FISA Section 702 data?**

**Response:** The Department has never recommended or pursued prosecution for an FBI employee or contractor for conducting a non-compliant query of Section 702 information.

10. **Mr. Olsen testified that in at least two instances, the FBI searched FISA Section 702 data for evidence of a non-national security related crime without an affirmative obligation to do so. Please provide the following:**

    a. **A narrative summary and all available records related to these and similar instances.**

**Response:** On a quarterly basis, NSD reviews each U.S. person query that is identified in FBI systems as being conducted for an evidence of a crime-only purpose. Between December 2021 and November 2022, that review revealed two noncompliant U.S. person queries that were run for an evidence of a crime-only purpose.

In the case of the first query, in March 2022, an FBI Special Agent ran a query of a U.S. person's name in response to a lead sent by another field office in connection with the January 6, 2021 U.S. Capitol breach. The query returned Section 702 information, which the agent accessed

under circumstances that NSD found to trigger Section 702(f)(2)'s requirement for a FISC order. NSD also concluded that the query standard was violated because the agent did not have a specific factual basis to believe that the query was reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection. The agent did not use the information for any analytical, investigative, or evidentiary purpose. As discussed in ODNI's Annual Statistical Transparency Report for calendar year 2022, the user who conducted this query did not understand that the lead they received, and the resulting query, was connected with a predicated criminal investigation at the originating field office..

In the case of the second query, in June 2022, an FBI user ran one query in an FBI system of a United States person query term against unminimized Section 702-acquired information. The user conducted this query as part of routine baseline checks in connection with an assessment related to domestic terrorism and without a foreign nexus. NSD concluded that the querying standard was violated because the agent did not have a specific factual basis to believe that the query was reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection.

b. **Copies of all written policies and procedures that governed this category of searches.**

**Response:** The Department's written policies and procedures relating to these sorts of queries are limited to the FBI Section 702 querying procedures and the November 2021 guidance to FBI users, both of which have been produced to the Committee.

**SENATOR SHELDON WHITEHOUSE**

1. **Intelligence gathered under Section 702 of the Foreign Intelligence Surveillance Act helped uncover gruesome atrocities committed by Russia in Ukraine, including the murder of noncombatants and the forced relocation of children from Russian-occupied Ukraine to the Russian Federation, and the detention of refugees fleeing violence by Russian personnel. Has such intelligence gathered under Section 702, either classified or unclassified, been shared with the International Criminal Court? If not, why not?**

**Response:** The Department defers to the Office of the Director of National Intelligence regarding whether Section 702 information has been shared with the International Criminal Court.

2. **Section 7073 of the FY23 Consolidated Appropriations Act (Pub. L. No. 117-328) specifically authorizes the executive branch to share information for "rendering assistance to the International Criminal Court to assist with investigations and prosecutions of foreign nationals related to the Situation in Ukraine, including to support victims and witnesses." How does your agency intend to assist the ICC in accordance with this provision?**

**Response:** With regards to the provision authorizing ICC investigative activities in the United States concerning alleged crimes committed in Ukraine by foreign nationals, the Attorney General is charged with reviewing such requests. In the event that the Attorney General concurs in such a request, U.S. law enforcement will assist by locating persons or evidence of interest to the ICC, deconflicting any ICC investigative activities with any investigations by U.S. law enforcement and ensuring that all ICC investigative activities comply with U.S. law.

**Senator Charles Grassley**

1. **In the Senate Judiciary hearing held on 6/13/2023, the following question was asked: The Foreign Intelligence Surveillance Court found that the government violated 702 policies more than 278,000 times. Mr. Olsen, what is the Justice Department doing to punish folks who abuse FISA? In response, Mr. Olsen discussed the reforms to Section 702 queries that the FBI recently made, and indicated that only one person has been fired as a result of 278,000 instances of failure to follow policy. Mr. Olsen did not discuss if any employees faced formal discipline for the failure to follow policy.**

   **Please provide the exact number of queries that resulted in the 278,000 instances of the FBI's failure to follow its own policy.**

**Response:** As the FISC noted in its April 2022 opinion, an audit conducted by FBI's Office of Internal Auditing in 2021, together with corresponding follow-up work done by the National Security Division's Office of Intelligence, found over 278,000 non-compliant FBI queries of raw FISA-acquired information. However, that figure includes queries that did not run against Section 702-acquired information; nearly 95% of the more than 278,000 queries ran only against information acquired pursuant to other FISA authorities and not Section 702-acquired information. Moreover, a small number of batch jobs accounted for nearly three-quarters of the over 278,000 query errors; so that figure represents significantly fewer than 278,000 improper query decisions.

Of the approximately 5% of query errors that did run against Section 702 information, over 84% complied with the query standard and were only errors because they were not correctly labeled as being U.S. person or non-U.S. person queries.

   a. **Please specifically describe the disciplinary action taken against each employee for each instance of failure to follow policy, and the date on which each of these instances occurred.**

**Response:** The Department's and FBI's oversight of the FISA program has found that instances of personnel intentionally running non-compliant queries against 702 information are exceedingly rare. Rather, the vast majority of the FBI's compliance incidents with respect to querying are—like the incidents in question—the result of good faith mistakes by FBI personnel who had a proper investigative purpose but who failed to meet the heightened standard require for FISA queries. To address these kinds of errors, the FBI worked to identify the root causes of these errors and implemented system changes, such as a change in default system settings and real-time user prompts, and improved training and guidance, as well as other measures. These changes have been effective at reducing both the overall number of U.S. person queries and driving an increase in the FBI's rate of compliance with the FISA query standard, which now

stands at above 98% based on the Department reviews included in the two most recent semiannual reports.

2. **How does National Security Division select which FBI's Section 702 activities it audits each year?**

**Response:** NSD audits FBI's compliance with its Section 702 targeting procedures, minimization procedures, and querying procedures. NSD conducts bi-monthly reviews of FBI's compliance with its targeting procedures by reviewing checklists and supporting documentation provided by FBI for a sample of approved requests for FBI to acquire information using its Section 702 targeting procedures.

Each year NSD selects approximately 23-27 field offices and/or headquarters components for querying reviews. When selecting field offices to review each year, NSD considers a number of factors, including the size of the field office and when it was last reviewed, and attempts to review a representative group of field offices throughout the country. These reviews evaluate whether FBI queries complied with the requirements in FBI's minimization and querying procedures, including its Section 702 querying procedures, as well as other statutory and FISC-ordered requirements. NSD's FBI query reviews evaluate a 90-day sample of queries conducted by personnel at the relevant field office—including both U.S. person and non-U.S. person queries and including queries of Section 702-acquired information and of non-Section 702 FISA-acquired information. The Department also periodically reviews all sensitive query approvals made by FBI personnel. And, the Department has conducted FBI-wide query audits, reviewing queries conducted by personnel in particular systems containing Section 702 information during a set period of time; these FBI-wide audits include queries conducted by personnel at multiple FBI field offices across the country.

Each year NSD also selects approximately 15 field offices for minimization reviews. During its FBI minimization reviews, NSD looks at, among other things, a sample of retention decisions made by FBI personnel in connection with investigations involving the acquisition of data pursuant to Section 702 and a sample of disseminations of information acquired pursuant to Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons.

NSD also conducts quarterly reviews at FBI headquarters of FBI's compliance with its Section 702 minimization procedures. At these reviews, NSD reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. NSD also reviews all disseminations by the relevant FBI headquarters component of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons.

3. **How much additional expense would the National Security Division incur if it were to audit a larger subset of FBI Section 702 activities?**

**Response:** If the National Security Division (NSD) were required to audit *a sample of* queries conducted by FBI personnel at every FBI field office and headquarters component annually, based on NSD's current experience in conducting this type of oversight, the Oversight Section in NSD would require 13 additional attorney positions with a cost of approximately $10.5 million over a three-year period. Alternatively, if the NSD were required to review *all* U.S. person queries of Section 702 information at each FBI field office and headquarters component annually, based on NSD's current experience, the Oversight Section in NSD would require 21 additional attorney positions at a cost of approximately $17.1 million over the course of three years. Finally, if the goal was to review all queries of FISA-acquired information, including Section 702 information, at each field office and headquarters component annually, the Oversight Section in NSD would require at least 45 additional attorney positions with an estimated cost of approximately $36.5 million over the course of three years.

4. **Does the National Security Division have any plans to expand its auditing of FBI FISA activities?**

**Response:** As noted above, NSD reviews a sample of all FBI targeting decisions every two months; NSD also reviews queries conducted by personnel in approximately half of FBI field offices each year, and minimization activities by personnel in approximately one-quarter of FBI field offices each year. This oversight program has consistently allowed NSD to uncover and address common compliance issues across the FBI enterprise and across types of Section 702 activities. We plan to continue this robust oversight going forward. Expanding this operation to include additional required query oversight would require additional resources as outlined above.

5. **The 2021 FISC opinion found a large number of non-compliant searches for communications involving people in the United States. One agent even told the National Security Division that he never marked queries as involving U.S.-person query terms "even if the facts indicated otherwise."**
    a. **Doesn't this mean that the government's estimates on searches of people in the United States are almost certainly an undercount?**
    b. **What is the government doing to specifically address this pattern of misidentifying U.S. query terms?**
    c. **Why is this a problem 15 years after Section 702 was enacted?**

**Response:** Importantly, the total number of U.S. person queries conducted is not the same as the number of U.S. persons queried, as multiple identifiers can pertain to the same individual, and U.S. person queries also include terms not associated with individuals, such as corporations or other organizations being targeted by foreign actors.

Although NSD does not review every single FBI query, whether a query is properly labeled as a U.S. person query is something NSD evaluates in the course of its oversight. Any mislabeling errors NSD finds are reported to the FISC and to Congress.

FBI reports the number of queries run each year in the ODNI Annual Statistical Transparency report. This figure is based on the number of queries that are labeled as U.S. person queries in FBI's IT systems. A number of considerations accompany this figure. First, because of a system configuration, a batch query that contains at least one U.S. person term counts each query term as a U.S. person term—even if the rest of the terms are non-U.S. person terms. For example, if the batch contains 100 total phone numbers, two of which are U.S. numbers, the system records 100 U.S. person queries. This dynamic may contribute to an overcount from the FBI systems. At the same time, mislabeled queries can contribute to both overestimating and underestimating the number of U.S. person queries, because queries that are in fact non-U.S. person queries can be mislabeled as U.S. person queries, and vice versa.

The FBI has implemented several remedial measures since 2021 aimed at improving U.S. person query compliance. Those measures are detailed on the Department's website. In consultation with NSD, FBI updated its query guidance documents, re-vamped its FISA-related training materials, and instituted a requirement that personnel must retake training annually to retain access to raw FISA information. These measures are aimed at improving the workforce's cognizance of the importance of adhering to, among other things, the FISC-approved query procedures. Additionally, in recognition that the workforce must be properly incentivized to scrupulously adhere to these complex procedures, the FBI also launched new accountability practices in July 2023, which impose escalating consequences for compliance incidents resulting from negligence.

**Senator Mazie Hirono**

1. **What definition and/or analysis does the National Security Division currently use to determine whether information is "derived from" electronic surveillance under 50 U.S.C. § 1806?**

**Response:** In November 2016, the Department promulgated internal guidance for all the Department personnel addressing the "derived from" analysis in both criminal Title III and FISA contexts.

Generally, in accordance with 50 U.S.C. §§ 1801(k), 1806(c), 1825(d), 1845(c), and 1881e(a), if the Department intends to "enter into evidence" or "otherwise use or disclose in any trial, hearing, or other proceeding" against an aggrieved person, any information "*obtained*" or "*derived from*" FISA-authorized collection (including electronic surveillance, physical search, pen register/trap-and-trace surveillance, and Title VII acquisitions), it must "notify the aggrieved person and the court or other authority." As a general matter, an aggrieved person is one who was the target of, or whose communications or property were subject to, FISA-authorized collection.

Information is "obtained" from FISA-authorized collection when it is the *direct product* of the surveillance or search (*e.g.*, the contents of communications from a phone call captured through FISA-authorized electronic surveillance). Information may also be "derived from" FISA-authorized collection if it is an *indirect product* of investigation that originated in FISA collection. As an example, if products obtained from FISA-authorized collection were used as the basis for an affidavit in support of a criminal search warrant application, the fruits of such warrant may be "derived from" the information obtained pursuant to FISA.

The "derived from" standard incorporates a "fruit of the poisonous tree" analysis analogous to that conducted in the (non-FISA) Fourth Amendment exclusionary rule context. The key issue in that analysis is whether the evidence has been obtained "by exploitation" of the surveillance "or instead by means sufficiently distinguishable to be purged of the primary taint." *Wong Sun v. United States*, 371 U.S. 471, 488 (1963) (citation omitted). Generally, the doctrines used to determine whether information has been "purged" of any "taint" are described as "independent source," "inevitable discovery," and "attenuation."

2. **Does the definition and/or analysis described in response to question one exist in any memo, guidance, letter, email, or other written or electronic document or communication or collection thereof, whether draft or final? If so, please provide a description of each such document or communication, including its date.**

**Response:** Please see response to question 1.

3. **Has the definition and/or analysis described in response to question one changed since January 20, 2021? If so, please provide the information requested in questions one and two for each such definition and/or analysis. If not, please provide the last date on which this definition and/or analysis changed and provide the information requested in questions one and two for the definition and/or analysis immediately preceding that most recent change.**

**Response:** The analysis has not changed since January 20, 2021. The current guidance was issued by the Department in 2016.

4. **In response to questions about the Fourth Amendment implications of U.S. person queries under Section 702, the Department of Justice contends that every court to have reviewed Section 702 queries has found them to be constitutional. Excluding cases (1) decided by the FISC or FISCR, (2) in which U.S. person queries were not at issue,[3] (3) in which the government obtained a dismissal on the basis of the state secrets privilege, (4) in which the government obtained a dismissal on the basis of standing,[4] (5) in which the court based its ruling at least in part on the misapprehension that individual U.S. person queries under Section 702 do not involve a significant level of intrusion into a person's privacy beyond that which is *required* to implement minimization procedures,[5] and (6) in which the court's reasoning was later overturned on appeal,[6] which cases have *held* that U.S. person queries under Section 702 are constitutional?**

**Response:** In addition to eight different federal judges sitting on the FISC, four district courts have held that a warrant is not needed to conduct U.S. person queries of data collected pursuant to Section 702. *See United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1256 (D. Colo. 2015), aff'd on other grounds, 20 F.4th 558 (10th Cir. 2021); *United States v. Mohamud*, No. 3:10–cr–475, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), aff'd on other grounds, 843 F.3d 420 (9th Cir. 2016); *United States v. Hasbajrami*, No. 11-cr-623, 2016 WL 1029500, at *12-13 & n.20 (E.D.N.Y. Mar. 8, 2016), remanded, 945 F.3d 641 (2d Cir. 2019); Mem. Op. at 55-56, *United States v. Al-Jayab*, No. 1:16-cr-181 (N.D. Ill. June 28, 2018), ECF No. 115. The opinions in

[3] *See, e.g.*, *United States v. Muhtorov*, 20 F.4th 558, 591 (10th Cir. 2021) ("The record confirms that the relevant evidence did not arise from querying. We therefore do not address Mr. Muhtorov's second Fourth Amendment argument."); *United States v. Mohamud*, 843 F.3d 420, 438 (9th Cir. 2016) (Noting case "did not involve the retention and querying of incidentally collected communications.").

[4] *See, e.g.*, *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).

[5] *See, e.g.*, Mem. Op. at 56, *United States v. Al-Jayab*, No. 1:16-cr-181 (N.D. Ill. June 28, 2018), ECF No. 115.

[6] *See, e.g.*, *United States v. Hasbajrami*, No. 11-cr-623, 2016 WL 1029500, at *12 & n.20 (E.D.N.Y. March 8, 2016), *rev'd in part on appeal,* 945 F.3d 641, 669–73 (2d Cir. 2019) ("[Q]uerying that stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable.").

these cases are matters of public record. No court has ever held that a warrant is required for U.S. person queries of Section 702 data.

June 13, 2023

The Honorable Dick Durbin
Chairman
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Lindsey Graham
Ranking Member
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

**Demand Progress Submission for the Record to the Senate Committee on the Judiciary on Behalf of 30 Organizations Regarding Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities**

Dear Chairman Durbin, Ranking Member Graham, and members of the Senate Committee on the Judiciary:

Thank you for conducting this critical oversight hearing. Appended below is an overview of key reform priorities endorsed by a bipartisan coalition of over 30 organizations, submitted in the interest of guiding ongoing discussions around the potential reauthorization of the controversial surveillance law known as "Section 702" of the Foreign Intelligence Surveillance Act.

As you are aware, restoring the right to privacy of people in the United States is one of the most bipartisan causes among Americans and in Congress. A long-running poll from The Associated Press-NORC Center for Public Affairs Research, updated last week, now "shows that Democrats and Republicans have similar views on surveillance tactics" — and that Americans' support for the warrantless surveillance authorized by Section 702 has plummeted to only 28% in favor, with 44% opposing.[1]

The following reform priorities and signatories reflect that bipartisanship and that public will to restore privacy in the United States, as well as organizations' commitment to these reforms. In sum, they form a comprehensive approach to reforming warrantless surveillance that impacts the privacy of people in the United States, which Congress should enact before considering any reauthorization of Section 702.

Sincerely,

Sean Vitka
Senior Policy Counsel
Demand Progress

[1] https://apnews.com/article/intelligence-section-702-apnorc-poll-4ef1e9f300395d0d7cda5b86cf7d5785

**1. Ensure that the government cannot access Americans' most sensitive private information without a warrant and express statutory authority**

*1.1 Close the Section 702 backdoor search loophole.*
*1.2 Close the EO 12333 backdoor search loophole.*
*1.3 Prohibit the government from purchasing data to evade warrant requirements and statutory privacy protections.*
*1.4 Bring the law in line with technology.*
*1.5 Strengthen Section 702's prohibition on reverse targeting.*
*1.6 Expressly prohibit the acquisition of purely domestic communications under Section 702 and EO 12333.*
*1.7 Prohibit warrantless scanning of content.*

**2. Rein in overbroad scope of surveillance**

*2.1 Prohibit bulk collection of sensitive information.*
*2.2 Narrow the permissible pool of foreign targets.*
*2.3 Prohibit "abouts" collection.*
*2.4 Strengthen minimization requirements.*
*2.5 Narrow collection under authorities that only require "relevance."*
*2.6 Limit use of FISA Section 702 for domestic law enforcement.*

**3. Ensure that judicial review is available and effective when Americans are subject to surveillance**

*3.1 Enact measures that will enhance the FISA Court's ability to serve as a check on surveillance.*
*3.2 Ensure that criminal defendants receive notice of foreign intelligence surveillance.*
*3.3 Fix standing problem.*
*3.4 Gag order fix.*
*3.5 Restore judicial review in civil litigation.*
*3.6 Establish judicial oversight over certain EO 12333 activities.*
*3.7 Bolster the FISA Court's role in reviewing targeting decisions.*

**4. Increase transparency and accountability for surveillance activities**

*4.1 Reforms to the classification system.*
*4.2 OLC opinion disclosures.*
*4.3. Timely and effective disclosure of FISA Court opinions.*
*4.4 Require ODNI publish an estimate of US person information acquired pursuant to Section 702 and EO 12333.*
*4.5 Prohibit the government from requiring or incentivizing encryption backdoors.*
*4.6 Strengthen transparency reporting, Congressional and public oversight, and accountability measures.*

**1. Ensure that the government cannot access Americans' most sensitive private information without a warrant and express statutory authority**

*1.1 Close the Section 702 backdoor search loophole*. Communications are collected without a warrant under Section 702 based on the government's certification that it is targeting *only* foreigners overseas. Yet the FBI routinely conducts searches of Section 702-acquired data to find information about *Americans*, including their communications (which are "incidentally" acquired in massive amounts). Agencies should be required to obtain a warrant or FISA Title I order before conducting such searches to stop the use of Section 702 as an end-run around the Fourth Amendment.

*1.2 Close the EO 12333 backdoor search loophole*. Collection under Executive Order 12333 (which includes overseas collection activities, as well as certain domestic collection of non-contents information) frequently results in the "incidental" acquisition of Americans' communications and other Fourth Amendment-protected data, like geolocation information. Agencies perform backdoor searches of such data, thus evading the Fourth Amendment's warrant requirement. As with Section 702, the government should have to obtain a warrant or FISA Title I order before performing such searches.

*1.3 Prohibit the government from purchasing data to evade warrant requirements and statutory privacy protections*. The government has argued that even in cases where a warrant would be required to compel the production of information, it can avoid that requirement by simply purchasing the data. Congress should put an end to this circumvention of the Constitution by prohibiting law enforcement and intelligence agencies from purchasing data they would otherwise need a warrant, court order, or subpoena to obtain. (The Fourth Amendment Is Not For Sale Act would go a long way toward that end.)

*1.4 Bring the law in line with technology*. Due to changes in how data is produced, stored, and analyzed, certain data that can be "crunched" to reveal extremely sensitive details of our personal lives — such as geolocation data, communications metadata, Internet search and web browsing records, biometric information, and health data — are routinely held by third parties and therefore lack Fourth Amendment protection. With its 2018 decision in *Carpenter v. United States* (ruling that police need a warrant to obtain geolocation data held by a cell phone company), the Supreme Court began the long, slow process of updating the law. Congress should step in and accelerate the process by requiring the government to get a warrant in order to obtain these highly sensitive types of records.

*1.5 Strengthen Section 702's prohibition on reverse targeting*. Currently, Section 702 requires the government to certify that "the" purpose of collection is not to target particular, known Americans. This weak prohibition still allows the government to conduct warrantless surveillance even where spying on Americans is the government's *primary* purpose. Collection under Section 702 should be prohibited if "a" purpose is to target Americans.

*1.6 Expressly prohibit the acquisition of purely domestic communications under Section 702 and EO 12333*. Section 702 and EO 12333 are warrantless surveillance authorities, and as such, they

should never be used to collect communications between or among Americans. Congress should clearly specify that such collection is prohibited.

*1.7 Prohibit warrantless scanning of content*. When the government conducts surveillance of communications in transit over the Internet backbone, it temporarily seizes and scans the content of all communications flowing past the point of interception in order to locate the communications of targets. This is similar to a general warrant in which police search all the homes in a city to see which of them contain incriminating evidence. Although the scanning is done without manual review, a police search of every home in a city would not be acceptable simply because the search was performed by robots. Congress should specify that any scanning must be limited to the communications metadata in order to minimize the unnecessary intrusion on Fourth Amendment rights.

**2. Rein in overbroad scope of surveillance**

*2.1 Prohibit bulk collection of sensitive information*. Under various surveillance authorities (including even administrative subpoena authorities), the government has engaged in "bulk collection" — the indiscriminate collection of data without any specific targets. As a general matter, most of the people whose data is obtained through "bulk collection" are entirely innocent and unrelated to any investigation. Moreover, under EO 12333, bulk collection can result in the acquisition of purely domestic communications, and does result in the collection of unquantified but massive amounts of information about Americans. Congress should prohibit the bulk collection of communications or other sensitive data under any authority, with at most an exception for areas experiencing active hostilities during wartime.

*2.2 Narrow the permissible pool of foreign targets*. Under Section 702 and EO 12333, the government can conduct surveillance of almost any foreigner abroad, subject only to (1) an exceptionally broad definition of "foreign intelligence" in FISA, and (2) a list of legitimate objectives set forth in EO 14086, which the next president could revoke and which the current president may amend in secret (as expressly provided in the order). Allowing surveillance of foreigners who pose no threat to the U.S. jeopardizes the privacy of the Americans with whom they communicate. It also threatens U.S. business interests: Overbroad U.S. surveillance authorities have led European courts to strike down data-transfer agreements between EU and U.S. companies. This reform will require some combination of the following approaches:

1. Require intelligence analysts to have reasonable suspicion to believe that the target of surveillance is a foreign power or agent of a foreign power, as broadly defined in FISA (but excluding civil society NGOs)
2. Remove the overbroad catch-all provisions from FISA's definition of "foreign intelligence" (i.e., remove 50 U.S.C. 1801(e)(2))
3. Codify legitimate purposes similar to those set forth in EO 14086, and require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to provide information that is directly relevant to one or more of the objectives

*2.3 Prohibit "abouts" collection*. Under Section 702, the government for years collected not only communications *to* and *from* the targets of surveillance, but also communications *about* those

targets. This practice swept in many conversations among innocent people who did not meet the criteria for targeting, as well as purely domestic communications. After pushback from the FISA Court, the government stopped this practice under Section 702's Upstream program (which directly taps into and scans internet backbone traffic) in 2017, but under current law the government is free to restart it as long as it gives Congress 30 days' notice. Meanwhile, some experts are concerned that a similar practice may be occurring "downstream," where most Section 702 surveillance occurs. Downstream "abouts" collection would be alarming because it would mean the government is still warrantlessly acquiring communications that merely mention a target, rather than only communications to or from a target. "Abouts" collection is unnecessary and intrusive, and Congress should prohibit it.

*2.4 Strengthen minimization requirements.* Under both Section 702 and EO 12333, the government is currently allowed to retain "incidentally" collected U.S. person information for up to 5 years, and there are several exceptions that allow much longer retention periods. These long and flexible periods cannot be squared with the statutory and constitutional mandate to "minimize" the retention of Americans' information. Congress should shorten the time period to three years and eliminate the multiple exceptions. Retention beyond this limit should be permitted only for information that has actually been reviewed by an individual who makes a written determination that the information constitutes foreign intelligence or evidence of a crime. In addition, Congress should mandate protections for information subject to attorney-client privilege.

*2.5 Narrow collection under authorities that only require "relevance."* The USA Freedom Act sought to prohibit bulk collection under a range of FISA authorities that are available on a low "relevant to" an investigation standard, including Section 215, pen register/trap-and-trace orders, and national security letters. Prior to the USA Freedom Act, the government and the FISA Court had interpreted this "relevance" standard to permit the NSA's bulk collection of Americans' phone records under Section 215. The USA Freedom Act attempted to address this problem by requiring collection to be based on "specific selection terms" (SSTs) defined separately for each authority. The government's statistical reports, however, suggest that large numbers of people other than the actual targets are continuing to be swept up under these provisions, raising the specter of "bulky" collection. Congress should tighten the definitions for SSTs, removing potentially broad terms like "entity," which could encompass at least hundreds or thousands of people. Alternatively, it should replace the "relevance" standard, and permit collection only where the government has reasonable grounds to believe that the subject of the information to be collected is a foreign power or agent of a foreign power. This would also reinforce reform 2.1.

*2.6 Limit use of FISA Section 702 for domestic law enforcement.* Current law permits Section 702 — ostensibly a foreign intelligence authority — to broadly be used for routine domestic law enforcement. The law permits use of Section 702-acquired information in assessments and investigations concerning *any* crime. Although current law imposes some limitations on the use of this information in criminal court proceedings, those limitations are vague, elastic, and give the Attorney General broad authority to set parameters for how the rules apply. Information acquired under Section 702 should only be used in assessments, investigations, and criminal proceedings involving a narrow set of serious offenses that are specifically enumerated, and this

limit should apply to *all* stages of investigation and prosecution, not just use in criminal court proceedings.

**3. Ensure that judicial review is available and effective when Americans are subject to surveillance**

*3.1 Enact measures that will enhance the FISA Court's ability to serve as a check on surveillance*. In 2020, the Senate approved an amendment offered by Senators Leahy and Lee by a vote of 77-19. The amendment included several provisions that would bolster the role of FISA Court amici, giving them better access to information and expanding the categories of cases in which they should presumptively be involved — namely cases involving sensitive targets like domestic media, religious groups, and political groups. It also included provisions to ensure that the materials the government presents to the FISA Court are accurate and include any exculpatory information. This amendment should be enacted into law as part of FISA without being watered down, given its overwhelming bipartisan support.

- flowchart available

*3.2 Ensure that criminal defendants receive notice of foreign intelligence surveillance*. Congress required the government to provide notice to criminal defendants when using notice "obtained or derived from" FISA surveillance. The government has frequently avoided this obligation by engaging in "parallel construction," i.e., reconstructing an evidentiary trail using information it wouldn't have obtained but for FISA in an effort to avoid disclosing more controversial surveillance practices. Not only does this practice deprive defendants of their right to challenge the surveillance used against them, but it also deprives the public at large of the government accountability that results from courts considering the legality of novel or controversial surveillance. Congress should close off this loophole by clarifying that evidence "derived from" FISA includes evidence that would not have been obtained "but for" the FISA collection.

*3.3 Fix standing problem*. The Supreme Court has made it nearly impossible for plaintiffs to challenge unlawful surveillance if they lack proof that they have been surveilled — something few plaintiffs would ever have. Congress should provide that individuals and organizations have a right to sue if they regularly communicate foreign intelligence information with foreigners abroad and have taken objectively reasonable measures to avoid surveillance, or if they have demonstrated a concrete injury arising from a good-faith belief that their rights have been, are being, or imminently will be violated through surveillance.

*3.4 Gag order fix*. One reason challenges to surveillance are rare is because the law makes it far too easy for the government to silence service providers who have been required to turn over their customers' communications or other records to the government. Bills like Sen. Wyden's Government Surveillance Transparency Act or Rep. Nadler's NDO Fairness Act would strike a much better balance between providing notice to people who have been surveilled and safeguarding the integrity of investigations. Congress should include such legislation as part of reauthorization.

*3.5 Restore judicial review in civil litigation*. Even if plaintiffs can show standing, the Supreme Court recently held that FISA's provisions for handling national security

information in surveillance cases — provisions that require the court to issue a ruling on the lawfulness of the surveillance — are not meant to displace the "state secrets privilege," which the government routinely uses to shut down lawsuits entirely. If this decision is allowed to stand, civil challenges to unlawful foreign intelligence surveillance will be effectively taken off the table. Congress should clarify that FISA's provisions for handling national security information are the exclusive means for addressing national security information in electronic surveillance cases.

*3.6 Establish judicial oversight over certain EO 12333 activities*. No program that involves the collection of Americans' communications and other constitutionally protected information should occur without any judicial oversight. At a minimum, the government should be required to provide notice to criminal defendants when using evidence obtained or derived from EO 12333 surveillance so the defendant may bring a challenge.

*3.7 Bolster the FISA Court's role in reviewing targeting decisions*. Currently, the FISA Court reviews and approves targeting procedures and the broad purposes for which a person or entity may be targeted, but it does not review targeting decisions — which means the government could be violating the procedures and the Court wouldn't know it unless the government chose to self-report. Congress should require the FISA Court to audit a random sample of targeting decisions to determine whether the government is adhering to the targeting procedures and the frequency of any non-compliance.

**4. Increase transparency and accountability for surveillance activities**

*4.1 Reforms to the classification system*. It is increasingly clear that legislative reforms will not be effective if the surveillance system remains in a black box, inaccessible to lawmakers and judges as well as the public. Moreover, the presence of classified documents in the homes of former President Trump, President Biden, and former Vice President Pence have led to calls for classification reform, and there is broad bipartisan support in Congress for such an undertaking.

*4.2 OLC opinion disclosures*. Like overclassification, it is increasingly clear that secret legal opinions issued by the Office of Legal Counsel within the DOJ can eviscerate even explicit Congressional intent, especially in relation to surveillance authorities, like the faulty opinions used to enable the illegal mass surveillance programs known as StellarWind (one of which was the precursor to Section 702). Reliable oversight of surveillance would include a requirement that legal conclusions considered binding on the executive branch be declassified, if necessary, and published as required by the SUNLIGHT Act.

*4.3. Timely and effective disclosure of FISA Court opinions.* The USA FREEDOM Act required that the government publish any novel or significant FISA Court opinions, a measure designed to prevent secret law. Unfortunately, the government has delayed the publication of some important rulings by a year or more. The law should be amended to require timely disclosure of FISA Court opinions within 60 days of their being issued. The amici should also have the ability to petition for rulings to be designated as significant.

*4.4 Require ODNI to publish an estimate of US person information acquired pursuant to Section 702 and EO 12333*. For Congress and the public to fully understand the privacy impact of foreign intelligence surveillance, agencies must release at least an estimate of how much information about and communications of Americans they are acquiring under relevant authorities. The government previously committed to providing this estimate for Section 702.

*4.5 Prohibit the government from requiring or incentivizing encryption backdoors*. Historically, this prohibition was linked to the "backdoor search fix" as offered in the House as an appropriations amendment, which passed the House in 2014 and 2015. Many members are on the record supporting this fix and it may also be attractive to companies. Prohibiting requirements or incentives for backdoors would also serve to increase confidence in US technology.

*4.6 Strengthen transparency reporting, Congressional and public oversight, and accountability measures*. This involves strengthening existing transparency, oversight, and accountability provisions, and adding certain additional requirements. Importantly, however, reforms to ensure better oversight of surveillance should not come at the expense of reforms that would actually rein in surveillance.

- Transparency:
    - Allow private actors to provide more granular transparency around directives, national security letters, targets, and estimated USP communications and metadata ("incidentally" or otherwise) acquired
    - Expand reporting requirements
    - Codify reporting requirements concerning the number of US person queries the FBI conducts
    - Implement false-positive testing, for instance by requiring the FISA Court or other auditor to sample acquired information (under both Section 702 and EO 12333) and estimate the proportion of acquired information that is not later determined to constitute foreign intelligence information (i.e. drawing from scientific methodological best practices around disclosing error rates)
    - Require PCLOB to examine and publicly report on the degree to which FISA disproportionately targets and impacts various marginalized groups, such as racial, ethnic, and religious minorities, as well as political dissidents and immigrants, including by auditing discrete, randomized samples of intelligence agency targeting and querying decisions, and disclosing how that information is used and the false positive error rates for these practices
- Enhance Congressional and public oversight:
    - Require ODNI to publish descriptions of the subject matter for each Section 702 certification and report the number of persons targeted under each
    - Strengthen PCLOB by allowing it to review foreign intelligence and cyber activities (currently its jurisdiction is limited to "terrorism") and permitting whistleblower complaints to PCLOB
    - Allow members of Congress to hear from Intelligence Community whistleblowers
    - House-specific: TS/SCI clearances for personal offices
- Accountability:
    - Enhance penalties for wrongful targeting and wrongful use of information acquired under FISA

- Require that statutorily compelled "technical assistance" for surveillance be necessary, narrowly tailored, and not overly burdensome, and require FISA Court approval
- Require and preserve documentation of FISA Court proceedings and communications between the government and the FISA Court

**ENDORSING ORGANIZATIONS:**

Advocacy For Principled Action In Government
American Civil Liberties Union
Americans for Prosperity
Asian Americans Advancing Justice | AAJC
Brennan Center for Justice at NYU School of Law
Center for Democracy & Technology
Center for Security, Race and Rights
CommonDefense.us
Constitutional Alliance
Defending Rights & Dissent
Demand Progress
Due Process Institute
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press Action
Freedom of the Press Foundation
FreedomWorks
Government Information Watch
Libertas Institute
Media Alliance
National Association of Criminal Defense Lawyers
Oakland Privacy
Organization for Identity & Cultural Development
PEN America
People For the American Way
Project for Privacy and Surveillance Accountability (PPSA)
Project On Government Oversight
Public Citizen
Restore The Fourth
Secure Justice
Surveillance Technology Oversight Project
Wikimedia Foundation
X-Lab

## Section 702 of FISA:
## A "Foreign Intelligence" Law Turned Domestic Spying Tool

In 2008, Congress passed Section 702 of FISA to give the government greater powers to conduct warrantless surveillance of suspected foreign terrorists. The law allows the National Security Agency (NSA), when collecting information inside the United States or from U.S. companies, to target almost any foreigner abroad and acquire all their communications without an individualized court order. Congress explicitly prohibited the targeting of Americans, and it charged the FISA Court with approving the program and its procedures once a year.

Although purportedly targeted at foreigners, **Section 702 has become a rich source of warrantless government access to Americans' phone calls, texts, and emails.** Since Section 702 was last reauthorized, a series of disclosures has revealed the extent of this problem. **In 2022 alone, the FBI conducted over 200,000 warrantless searches of Section 702 communications to find Americans' information.**[1] This has turned Section 702 into something Congress never intended: a domestic spying tool.

Other equally serious problems have emerged. The secret and one-sided nature of FISA Court proceedings has undermined the court's ability to conduct effective oversight, while Congress's efforts to enable other means of judicial review have been thwarted. Gaps in the law are allowing the collection of Americans' communications and other personal information outside of FISA, without *any* statutory limits or judicial oversight. And Section 702's failure to establish any meaningful limits on the scope of surveillance is threatening U.S. companies' ability to do business in Europe.

It's high time for Congress to step in and enact reforms that will safeguard Americans' rights and business interests. The well-documented problems with the law's operation are described in more detail below, along with the solutions. **Congress should not reauthorize Section 702 without these critical reforms.**

### Section 702: Problems and Solutions

*1. Problem: Use of Section 702 to Spy on Americans.* Surveillance under Section 702 inevitably sweeps in Americans' communications, which ordinarily would require a warrant to obtain. Congress therefore required agencies to "minimize" the sharing, use, and retention of such "incidentally" collected information about Americans. Congress also required the government to certify to the FISA Court that it is not engaging in "reverse targeting" — i.e., using Section 702 to spy on Americans. **Over the past decade and a half, it has become clear that these critical protections for Americans' constitutional rights have failed.**

Rather than "minimize" the sharing and retention of Americans' data, the NSA routinely shares such data with the FBI, CIA, and National Counterterrorism Center, and all agencies retain it for at least five

[1] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf. In addition to the 204,090 query number, this report also includes a "de-duplicated query figure" of 119,383, which represents the number of unique identifiers used in the queries. The lower number, however, would exclude instances of the same U.S. person being subject to multiple queries— such as if a U.S. person's communications are queried by different FBI personnel for independent reasons, or on multiple occasions over the course of an investigation to find any new communications—even though each query would represent a distinct privacy intrusion.

years. Worse, **all agencies have adopted rules allowing them to search through the data for Americans' communications – even though the data is acquired without a warrant based on the government's certification that it is targeting *only* foreigners overseas.** This practice is a bait and switch that guts Americans' Fourth Amendment protections, and it occurred over 200,000 times last year.[2]

Congress and the FISA Court have tried to rein in backdoor searches by imposing certain limitations — but the FBI has consistently violated them. When Congress last reauthorized Section 702 in 2018, it added a provision requiring the FBI to obtain a warrant before accessing Americans' communications in a very small subset of criminal investigations. This requirement has been triggered at least 100 times.[3] But by the government's own admission, **the FBI has never once adhered to the statutory warrant requirement.**[4]

For investigations that don't fall within the statutory warrant requirement, the FISA Court allows backdoor searches *if* they are likely to yield foreign intelligence or evidence of a crime. But according to several recent FISA Court opinions and government reports, **the FBI has engaged in "widespread violations" of this minimal court-ordered privacy protection.**[5] To name just a few examples, **FBI agents searched for the communications of:**[6]

- More than 100 Black Lives Matter protesters
- a batch of 19,000 political donors who gave money to a congressional campaign
- a U.S. congressman
- a "local political party"
- "multiple current and former United States Government officials, journalists, and political commentators"
- two "Middle Eastern" men, flagged by a witness because they were loading boxes of cleaning supplies into a vehicle
- 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
- colleagues and relatives of the FBI agent performing the search

---

[2] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.
[3] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.
[4] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2021*, April 2022. https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.
[5] Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019), available at https://perma.cc/94E9-A6BE.
[6] Memorandum Opinion and Order (FISA Ct. Apr. 21, 2022), available at https://perma.cc/26EN-YUHS; Office of the Director of National Intelligence, 22nd Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (August 2021), https://perma.cc/JB3J-NXWP; Office of the Director of National Intelligence, 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (December 2021), https://perma.cc/E76T-RKBG; Memorandum Opinion and Order (FISA Ct. Nov. 18, 2020) available at https://perma.cc/8U2N-5GYP; Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019), available at https://perma.cc/94E9-A6BE.

These represent just a small portion of the FBI's misuse of Section 702. Based on the 4 percent noncompliance rate reported in its most recent audit,[7] which reflects compliance rates *after* the FBI implemented new training and oversight requirements and made changes to its data systems, **the FBI conducted over 8,000 U.S. person queries that violated rules in 2022 alone, an average of over 20 improper queries every day.**

*Solution: Require a Warrant to Search for Americans' Communications.* Lawmakers must put a stop to the government using Section 702 as an end-run around Americans' constitutional rights. **Congress should require agencies to obtain a warrant (in criminal investigations) or a FISA Title I order (in foreign intelligence investigations) before searching Section 702-acquired information for Americans' communications.** The House has twice passed legislation that would impose a warrant requirement for U.S. person queries.

*2. Problem: Barriers to judicial review.* The mechanisms Congress established for judicial review of surveillance are not working as intended. The FISA Court provides limited, general oversight of Section 702 surveillance, but it operates in secret and often hears only from the government.

Although Congress authorized the FISA Court to appoint amici to provide advice, amici don't have full access to the information they need, and they are left out of many important cases. In addition, FISA requires the government to give notice to criminal defendants when using evidence derived or obtained from Section 702, but the government has evaded this requirement through "parallel construction" (recreating the evidence using less controversial means). And a recent Supreme Court decision gutted a provision of FISA designed to enable judicial review of surveillance in civil cases.[8]

*Solution: Bolster judicial review provisions.* Congress should strengthen FISA's amici provisions by giving amici better access to relevant information and by encouraging appointment of amici in cases involving sensitive targets such as religious or political organizations, candidates for public office, and the media. **An amendment that would have implemented these measures, offered by Senators Leahy and Lee, passed the Senate by a vote of 77-19 in 2020.**[9] Congress also should prohibit the government's use of "parallel construction"[10] to avoid notice obligations. And it should correct the Supreme Court's misreading of FISA by clarifying that federal courts may review surveillance materials in civil cases.

*3. Problem:* Gaps in FISA that allow surveillance of Americans outside of any statutory framework and without judicial oversight. Many of FISA's key definitions and distinctions are rooted in obsolete communications technologies. As technology has evolved, these anachronistic provisions have opened up gaps in the law's coverage, **allowing the government to collect vast amounts of Americans' communications and other personal data with no statutory limits, no effective congressional oversight, and no judicial oversight.** In particular, the government conducts sweeping surveillance overseas, and collects geolocation data and other sensitive information *inside the United States* (often purchasing it from data brokers), subject only to Executive Order (EO) 12333 and related agency

[7] Federal Bureau of Investigations Office of Internal Auditing, "FISA Query Audit," May 10, 2023. https://int.nyt.com/data/documenttools/fisa-query-audit-5-10/d9d8e20bafef27c8/full.pdf.
[8] See, *Clapper v. Amnesty International USA*; see also, *Jewel v. National Security Agency*.
[9] Roll Call Vote 116th Congress - 2nd Session, Lee Amdt. No. 1584, May 13, 2020. https://perma.cc/96XQ-D8BF.
[10] Human Rights Watch, *Dark Side Secret Origins of Evidence in US Criminal Cases*, January 9, 2018. https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

policies — which include even fewer protections for Americans' rights than Section 702. We learned in 2022 that **the CIA has been exploiting these gaps in FISA's reach for years to conduct a bulk collection program that pulls in Americans' data.**[11]

*Solution: Establish legislative safeguards and judicial oversight for EO 12333 surveillance affecting Americans.* Any surveillance that results in the collection of Americans' communications and other sensitive data should take place pursuant to statute and with oversight by Congress and the courts. Accordingly, **Congress should legislate basic protections for any EO 12333 surveillance that impacts Americans.** These protections should include limits on bulk collection, which poses unique threats to Americans' privacy; a warrant requirement for backdoor searches of EO 12333 data; and oversight by Congress and the FISA Court.

*4. Problem: Economic and privacy impact of overbroad surveillance.* Although the purpose of Section 702 is to prevent terrorism and head off other foreign threats, the law allows surveillance of an extremely broad class of foreigners abroad, including law-abiding private citizens. This jeopardizes the privacy of foreigners who pose no threat to the United States as well as the Americans with whom they communicate. For this reason — combined with the lack of sufficient mechanisms for redress when unlawful surveillance occurs — European courts, seeking to protect individuals' privacy from overbroad surveillance, have struck down legal agreements that facilitate data transfers from EU companies to U.S. companies. **The overbroad scope of Section 702 thus undermines the ability of 5,000+ U.S. companies to do business overseas, and recently led to a $1.3 billion EU fine for an American company based on risks of its data being subject to overbroad surveillance.**[12]

*Solution: Codify reasonable limits on the scope of surveillance and remove barriers to judicial review.* **Congress should enact limits that will prevent the targeting of ordinary private citizens who are unlikely to be communicating information about foreign threats.** Congress also should remove barriers to judicial review and establish limits on bulk collection, as described above. These measures would both protect Americans' privacy and address the threat that Section 702 surveillance poses to U.S. businesses.

American Civil Liberties Union
Americans for Prosperity
Brennan Center for Justice
Center for Democracy & Technology
Defending Rights & Dissent
Demand Progress
Due Process Institute
Electronic Frontier Foundation
Electronic Privacy Information Center
Fight for the Future
Free Press Action
Freedom of the Press Foundation
Libertas Institute
National Association of Criminal Defense Lawyers
Project for Privacy and Surveillance Accountability
Project On Government Oversight
Restore The Fourth
Surveillance Technology Oversight Project
TechFreedom
Wikimedia
X-Lab

[11] Charlie Savage, *New York Times*, "C.I.A. Is Collecting in Bulk Certain Data Affecting Americans, Senators Warn," February 10, 2022. https://www.nytimes.com/2022/02/10/us/politics/cia-data-privacy.html
[12] Adam Satariano, *New York Times*, "Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules," May 22, 2023 https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html.

**Statement for the Record**
**for Senate Judiciary Committee Hearing,**
**"Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities"**
**Submitted by Jake Laperruque,**
**Deputy Director of the Security and Surveillance Project of the**
**Center for Democracy & Technology**

**June 12, 2023**

The Center for Democracy & Technology ("CDT") submits the following statement for the record regarding Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). CDT is a 501(c)3 nonpartisan nonprofit organization that works to promote democratic values by shaping technology policy and architecture, with a focus on equity and justice. Among our priorities is preserving the balance between security and freedom. We have long expressed concerns that FISA Section 702 permits overbroad surveillance and lacks adequate safeguards, threatening the privacy and civil liberties of both individuals abroad and within the United States.

Any reauthorization of FISA Section 702 must be accompanied by significant reform and establishment of new safeguards to end misuse of this authority, which has occurred with shocking frequency in recent years. This statement will focus on two key reforms: 1) closing the "backdoor search loophole" by requiring a warrant for US person queries of communications collected under Section 702, and 2) narrowing Section 702 surveillance to genuine security threats. In addition to these issues, a broad range of other reforms are critical to a successful FISA Section 702 reauthorization. [1]

## *I. Congress should close the "backdoor search loophole" by requiring a warrant for US person queries*

FISA Section 702 significantly impacts Americans because it is regularly used to seek out and review Americans' communications that were collected without a warrant. Although FISA Section 702 is often framed by its proponents as a foreign-focused surveillance system that only targets foreigners located abroad, it is inevitable and expected that many Americans' private communications will be swept in. This occurs via "incidental collection" — whenever Americans speak with a foreign target, their communications are subject to warrantless surveillance. And because the scale of permissible targets is incredibly broad (targets need not have any suspected ties to foreign powers, security threats, or malicious activities), Americans speaking with innocent foreigners abroad such as friends, family, and business associates have their communications collected.

The government can — and frequently does — query databases of FISA Section 702-acquired communications to deliberately seek out these Americans' conversations without any judicial oversight or even suspicion. The intelligence community maintains that US person queries do not constitute a search because they are made on data already in the government's possession. This distinction does not justify the harm to privacy: these queries have *the same effect as a direct search* — government officials deliberately seek out, review, and use US persons' private communications without ever going through the checks and rules required for upfront searches. Individuals face the same harm to their privacy rights, but without any of the protections.

The scale and nature of US person queries reflect how FISA Section 702 has morphed into a domestic surveillance system. Last year the FBI conducted over 204,000 US person queries, an average of over 558 per

[1] These reforms include expanding the role of FISA Court amici and instituting other court reforms, expanding access to courts to litigate overbroad surveillance, providing defendants with notice when Section 702 was used in investigations, and ensuring that if Section 702 is reformed, improper surveillance practices are not simply shifted to other methods such as purchases of data from brokers or monitoring via Executive Order 12333. We focus here on U.S. person queries and scope of surveillance because they are priority reforms likely to be discussed at this hearing, and because we plan to address the additional reforms in subsequent comments to the Committee.

day.[2] While FISA Section 702 was created to respond to international security threats, today US person queries are used for an array of domestic law enforcement activities totally disconnected from national security such as health care fraud, bribery, and public corruption.[3] Even more troublingly, FISA Section 702 also is used to seek out the private communications of Americans in no way suspected of wrongdoing. The government has mis-used FISA Section 702 data by querying with the identifiers of US persons such as:[4]

- Over 100 Black Lives Matter protesters
- A group of 19,000 donors to a Congressional campaign
- A sitting US Congressperson
- Relatives of an FBI official performing a query
- Journalists
- A "local political party"
- Political commentators
- Current and former US government officials
- Victims who reported crimes to the FBI
- Law enforcement sources
- Individuals applying to work in local law enforcement
- Workers conducting maintenance at FBI offices
- Business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy" program
- College students participating in a "Collegiate Academy" program

These queries are non-compliant because they do not meet the requirements for conducting them that the Attorney General imposed in guidelines that Congress required. For many of these queries, "the [intelligence analyst] struggled to articulate a 'reasonable belief' that the queries would return foreign intelligence information or evidence of a crime," as required by Attorney General guidelines, or compliance assessments determined there was no reasonable basis to believe the queries would return such information.[5]

In 2018, when Congress last reauthorized Section 702, it established a warrant requirement for US person queries in some limited situations. But this system is riddled with exceptions that subsume the rule, and in its complexity has fostered a culture of noncompliance. The warrant requirement only applies to queries made "in connection with a predicated criminal investigation," permitting the FBI to make such queries in "assessments" when it doesn't even have the minimal level of suspicion required for opening a preliminary investigation. This means that situations where the government has the *least* suspicion of wrongdoing are those in which it has the *most* power to conduct US person queries without court authorization. Further, the warrant requirement does not apply to any queries that "relate to national security" or might mitigate "a threat to life or serious bodily harm."

---

[2] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf. In addition to the 204,090 query number, this report also includes a "de-duplicated query figure" of 119,383, the number of unique identifiers used in the queries. This lower number poorly reflects FBI practices, as it excludes any instances of the same US person being subject to multiple queries, which could be made on different dates, by different personnel, for different reasons, and return entirely different communications.

[3] Memorandum Opinion and Order (FISA Ct. Nov. 18, 2020) available at https://perma.cc/8U2N-5GYP (hereinafter *FISA Court 2020 Opinion*).

[4] For information on the full set of examples listed below, see, Memorandum Opinion and Order (FISA Ct. Apr. 21, 2022), available at https://perma.cc/26FN-YUHS (hereinafter, *FISA Court 2022 Opinion*); Office of the Director of National Intelligence, 22nd Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (August 2021), https://perma.cc/JB3J-NXWP (hereinafter, *22nd FISA Section 702 Compliance Report*); Office of the Director of National Intelligence, 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (December 2021), https://perma.cc/E76T-RKBG (hereinafter, *24th FISA Section 702 Compliance Report*); *FISA Court 2020 Opinion*; Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019) (hereinafter, *FISA Court 2019 Opinion*, available at https://perma.cc/94E9-A6BE.

[5] *FISA Court 2022 Opinion*; *22nd FISA Section 702 Compliance Report*; *24th FISA Section 702 Compliance Report*.

These categories are overbroad and undefined in statute, giving the government immense flexibility to claim queries have some nexus to either category.

The convoluted nature of these rules has also bred a culture of noncompliance, with the FISA Court stating that the FBI has "conducted a large number of suspicionless queries," engaged in "widespread violations of the querying standard," and displayed "a misunderstanding of the querying standard — or indifference to it."[6] Despite claims that new internal rules and measures have solved these issues, noncompliance still occurs at a shocking rate. Even with the FBI's newest internal reforms, an internal audit found a four percent noncompliance rate.[7] Given that the FBI conducted over 204,000 US person queries in 2022, this means the Bureau conducted over 8,100 US person queries last year in violation of rules, an average of 20 noncompliant queries for US persons' communications *every day* (and that assumes the FBI's internal assessment is accurate and does not understate noncompliance). The only way to stop this pattern of improper conduct and protect Americans' privacy is to put a judge between the FBI and the data it seeks by imposing a clear and consistent warrant rule for US person queries.

Congress should also reject the FBI's assertion that Congress should permit warrantless "defensive searches" that focus on a target of foreign influence operations or victims of cyberattacks. The FBI argues that when its queries are for the data of these categories as opposed to investigative targets, they should be excluded from any warrant requirement. Such an exception would continue to permit, for example, querying to find the communications of Congressman Darin LaHood, as was recently disclosed not by the FBI, but by Rep. LaHood himself.[8] The queries relating to 19,000 donors to an undisclosed congressional campaign are an astounding example of the "defensive searches" such an exception would open the door to.

Additionally, history is filled with chilling examples of how easily the notion of conducting defensive surveillance to protect Americans from foreign influence can be a pretense for politically motivated surveillance abuse. For example, J. Edgar Hoover authorized the monitoring of Dr. Martin Luther King Jr. ostensibly to defend against alleged communist influence efforts aimed at King and other civil rights leaders.[9] In reality, it was motivated by Hoover's racism and hatred of the civil rights movement.[10]

Detecting and defending against purported foreign influence and subversion was a frequent excuse for monitoring political dissidents—such as the antiwar movement, Black activists, students, and other left-leaning groups—throughout the 1960s and 70s for the abusive COINTELPRO surveillance program. The FBI even described defensive surveillance as something that "offers us a fertile field to develop valuable intelligence" on leftist political groups despite a lack of evidence of actual foreign danger.[11] Justifying spying on vulnerable communities and dissidents as a defensive measure to protect against foreign actors has continued into the 21st century. After the September 11 attacks, the New York Police Department, with federal support, engaged in mass surveillance of Muslim communities. They justified monitoring mosques, community centers, student groups, and the daily lives of average Americans—actions with serious harms—as necessary to guard against influence and infiltration by foreign actors like al Qaeda.[12]

---

[6] *FISA Court 2020 Opinion*; see also, Memorandum Opinion and Order (FISA Ct. Oct. 18, 2018) available at https://perma.cc/9CSR-63QM; see also, Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019) available at https://perma.cc/FTJ7-LDLG.
[7] Federal Bureau of Investigations Office of Internal Auditing, "FISA Query Audit," May 10, 2023. https://int.nyt.com/data/documenttools/fisa-query-audit-5-10/d9d8e20bafef27c8/full.pdf.
[8] Charlie Savage, New York Times, "F.B.I. Feared Lawmaker Was Target of Foreign Intelligence Operation," April 13, 2023. https://www.nytimes.com/2023/04/13/us/politics/fbi-darin-lahood.html.
[9] The Martin Luther King, Jr. Research & Education Institute, Stanford, "Federal Bureau of Investigations (FBI)." https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi.
[10] Alvaro Bedoya, Slate, "The Color of Surveillance," January 18, 2016. https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.
[11] Church Committee Report, Book II, April 26, 1976. https://perma.cc/8WWY-TETS.
[12] Saher Khan and Vignesh Ramachandran, *PBS News Hour*, "Post-9/11 surveillance has left a generation of Muslim Americans in a shadow of distrust and fear," September 16, 2021. https://www.pbs.org/newshour/nation/post-9-11- surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear.

The decades-long pattern shows that a blank check for warrantless "defensive" searches of Americans' communications collected pursuant to Section 702 could be abused for political or other purposes. To be sure, there are certain to be many genuine situations where the FBI and other intelligence agencies want to investigate and root out foreign influence efforts or other nefarious actions by foreign actors targeting Americans. The government should be able to pursue those investigations through its broad arsenal of lawful investigative powers, including appropriately predicated and judicially authorized searches of communications. This can also include US person queries related to victims and targets of foreign malfeasance, and Title III Wiretap warrants permit surveillance based on a probable cause showing that the government's actions will return evidence of wrongdoing.[13] Therefore, there could still be victim-focused queries in this realm—such as for information relating to a cyberattack—so long as they are still properly predicated on probable cause and subject to independent approval by courts. These key checks are necessary to prevent the abuses that have marred "defensive" surveillance for decades.

There's a reason the Fourth Amendment does not prohibit only "unreasonable *offensive* search and seizures": no matter what the government's motive is or is purported to be, we need a strong and consistent shield to protect our citizens and our democracy. Before searching for an American's private communications, get a warrant.

## II. *Congress should narrow the parameters of Section 702 targeting to genuine security needs*

In addition to closing the backdoor search loophole, Congress should narrow the scope of FISA Section 702 surveillance. FISA Section 702 permits the overbroad designation of targets, which endangers the privacy of Americans and foreigners, and threatens US business interests. Congress enacted this law to facilitate monitoring of foreign agents, terrorists, and intelligence operatives abroad, but its lax rules permit surveillance far beyond these types of legitimate targets. Any non-US person located abroad can be designated as a target, so long as a significant purpose of doing so is to obtain foreign intelligence information. This is problematic because foreign intelligence information is defined extremely broadly, including in a subclause — 50 USC 1801(e)(2) — that encompasses any information relating to the conduct of US foreign affairs.

This unnecessarily broad definition opens the door to abuse through mass targeting of innocent people who are in no way suspected of wrongdoing or connected to malicious activities by foreign powers. For example, the current definition would allow, in certain circumstances, targeting the following types of individuals:[14]

- A director screening an American produced film abroad
- An international businessperson
- Human rights activists and protesters
- Journalists covering public affairs
- Organizers of international sports events
- Humanitarian aid workers
- A scientist following fish migration paths
- Plant and wildlife conservation workers
- A musician on an international concert tour
- An expert examining the safety of consumer products

This type of unchecked surveillance causes an array of harms. For example, even though Americans cannot be FISA Section 702 targets, they will be swept up in this warrantless surveillance whenever they communicate with targets. And the scale of FISA Section 702 surveillance has swelled massively: Since Congress last reauthorized the law, the number of publicly known targets has increased 118 percent, from 106,469 to 232,432.[15] Because FISA Section 702 is used to target so many individuals under such broad parameters, there is significant risk that Americans—even while speaking with friends, work colleagues,

[13] 18 USC 2518(3).
[14] For additional information on these and other types of potential overbroad Section 702 targets, see, Mana Azarmi, The Center For Democracy & Technology, "Urgent Fix Needed: USA Liberty Act Needs To Better Focus Surveillance Under FISA 702," October 20, 2017. https://cdt.org/insights/urgent-fix-needed-usa-liberty-act-needs-to-better-focus-surveillance-under-fisa-702/.
[15] See, Jake Laperruque, "CDT Submitted Comments to PCLOB on FISA Section 702 Reform," The Center for Democracy &; Technology, November 4, 2022. https://perma.cc/EFN6-SHJ6

and relatives with no connection to security threats—will have their intimate conversations collected and subject to warrantless search by the government.

Permitting such broad targeting of innocent individuals also infringes on the privacy rights of foreigners abroad and threatens US business interests. The stability of US-EU transatlantic data flows has been seriously compromised due to the breadth of FISA Section 702 surveillance. Over the past decade, the European Court of Justice has twice struck down US-EU data flow agreements—first in *Schrems I* in 2015 and again in *Schrems II* in 2020 — due to inadequate safeguards on US surveillance. Last year the Administration took steps to lay the foundation for a new agreement, but absent significant reforms to FISA Section 702 by Congress, there is serious concern that future agreements on data flows will simply be struck down again.[16] The ramifications of inaction to U.S. businesses will be severe: Just last month an American company – Meta -- received a $1.3 billion fine due to concerns that the data of Europeans that it transfers was vulnerable to overbroad U.S. surveillance.[17]

Congress can ensure FISA Section 702 targeting is properly limited in two distinct ways. First, it could require that whenever targets are designated for the purpose of collecting information related to foreign affairs (the problematic §1801(e)(2) subclause of the "foreign intelligence information" definition), there must be reasonable suspicion that those targets are agents of a foreign power. This would grant the government significant flexibility for designating targets based on national security needs — as well as reasonably restrained capacity to designate targets in order to gather information related to foreign affairs — while removing risk of mass surveillance of innocent individuals.

Alternatively, another effective remedy would be to establish a reasonably narrowed set of purposes for which the government can designate FISA Section 702 targets. There is strong basis to believe that a balanced targeting rule that protects the privacy of Americans and foreigners without compromising security needs can be put in place: Last fall the Administration issued an Executive Order on signals intelligence, which included a rule limiting the purposes for which signals intelligence (including via FISA Section 702) can be conducted. Based on this Executive Order, FISA Section 702 surveillance can only be conducted for a set of thirteen enumerated purposes, which, collectively, are narrower than the statutory purposes for which Section 702 surveillance can be conducted. If the executive believes it can meet operational needs while voluntarily adhering to these limits, it should have no objection to them being codified into statute. Doing so would ensure their continued use without risk of the current executive order being supplanted or watered down, which the current Administration – and any future administration – could do unliterally and in secret. Enshrining effective guardrails in statute would provide strong assurance to EU courts, protecting transatlantic data flows and aiding US businesses.

***

We thank the Senate Judiciary Committee for considering this statement and our recommendations, and we look forward to working with members of the Committee as they examine how best to protect privacy, civil rights, and civil liberties as it considers possible reauthorization of FISA Section 702. For further information, please contact Jake Laperruque, Deputy Director of the Security and Surveillance Project at the Center for Democracy & Technology, at jlaperruque@cdt.org.

[16] See, Greg Nojeim and Iverna McGowan, "Report – Transatlantic Data Flows: More Needed to Protect Human Rights," The Center for Democracy & Technology, November 3, 2022.https://perma.cc/Q9JW-3GE3.
[17] Adam Satariano, *New York Times*, "Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules," May 22, 2023 https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html.

**STATEMENT OF**

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

**SUBMITTED FOR THE RECORD OF THE**

**UNITED STATES SENATE**
**COMMITTEE ON THE JUDICIARY**

**HEARING ON**

# OVERSIGHT OF SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND RELATED AUTHORITIES

**JUNE 13, 2023**

**Introduction**

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

Needless to say, these activities are not why Section 702 has become so deeply controversial, leading many lawmakers to demand either sunset or reform. If the government were using Section 702 solely to spy on hostile foreign actors, there would be little to debate in this year's reauthorization. The fundamental problem with Section 702 is that the government is also using it as a rich source of warrantless access to *Americans*' communications. According to the government, the FBI conducted more than *two hundred thousand* searches of Section 702 data in 2022 for the purpose of finding Americans' communications and other personal information. This outcome is contrary, not only to the original intent of Section 702 and to basic Fourth Amendment principles, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms.

Moreover, with every new release of an opinion issued by the Foreign Intelligence Surveillance Court ("FISA Court"), it becomes increasingly clear that the rules designed to protect Americans' privacy are being honored in the breach. Agencies have repeatedly, and in some cases systemically, violated statutory or court-ordered limitations on collection, retention, querying, and dissemination. Some of these violations have rendered the operation of the program unconstitutional. When Congress last reauthorized Section 702, it sought to shore up privacy protections by requiring FBI agents to obtain a warrant before accessing Section 702 data about Americans in a small subset of investigations. As of the most recent statistical report issued by the government, the FBI had *never* complied with this requirement.

Congress should not reauthorize Section 702 without sweeping reforms to ensure that it cannot be used as a domestic spying tool. At a minimum, that means closing the back door search loophole that enables government officials to access Americans' phone calls, text messages, and emails without a warrant. It also means strengthening the law's reverse-targeting prohibition and shoring up minimization requirements, as well as ending so-called "abouts" collection, to more strictly limit the collection, retention, and use of Americans' data. And it means narrowing the scope of surveillance to reduce "incidental" collection while still preserving the ability to target foreigners abroad who pose a threat to the United States.

Addressing the problems with Section 702 will also necessitate reforms to FISA more generally — starting with its judicial review provisions. Despite changes that Congress made in 2015, the FISA Court still hears only from the government in too many cases, and recent audits have shown that the government's submissions to the Court are riddled with errors and omissions. At the same time, the government has thrown up artificial barriers to judicial review

in civil litigation and criminal prosecutions, thwarting Congress's express intent to provide for such review. Congress must strengthen these mechanisms to ensure that the government can be held accountable for violations of the rule of law and Americans' civil liberties.

In addition, Congress should finish the job of modernizing FISA that it began in 2008. Generally speaking, FISA (including Section 702) applies when the collection of information takes place inside the United States or from a U.S. company; overseas surveillance, with few exceptions, is subject to neither legislative limits nor judicial oversight. In the digital era, however, communications and other personal information are often routed or stored in places around the globe. Overseas surveillance can therefore have just as great an impact on Americans' privacy as domestic surveillance, if not greater. Reforms to Section 702 will have limited effect if large swathes of overseas surveillance continue to be carved out of foreign intelligence surveillance legislation.

Indeed, it critical to recognize Section 702 as one authority within an ecosystem of often-overlapping surveillance authorities. Many of these authorities are outdated and/or contain gaps and loopholes, with the result that warrantless surveillance of Americans' most sensitive information is becoming increasingly common. Reform of any single statute, on its own, is unlikely to make a serious dent in the broader problem, given that surveillance can often migrate to an alternative authority. Moreover, Section 702 is one of the few such laws that includes a sunset. Congress should thus view the expiration of Section 702 this year as a rare and vital opportunity to reverse the broader drift, in the law and in practice, toward warrantless surveillance.

## I. History and Design of Section 702

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

Under Title I of FISA, the government was required to obtain an order from a special court (the FISA Court) to conduct "electronic surveillance." To obtain the order, the government had to show probable cause that the target of surveillance — whether that target was a foreigner or a "U.S. person" (an American citizen or legal permanent resident) — was a foreign power or an agent of a foreign power.[2] For non-U.S. persons, the terms "foreign power" and "agent of a foreign" power are defined quite broadly,[3] but for U.S. persons, "agent of a foreign power" is defined to require potential involvement in certain criminal activities, including espionage,

---

[1] *See* Lee Lacy, *Curtailment of the National Security State: The Church Senate Committee of 1975 – 1976*, BOISE STATE, FRANK CHURCH INSTITUTE (May 13, 2019), https://www.boisestate.edu/sps-frankchurchinstitute/2019/05/13/curtailment-of-the-national-security-state-the-church-senate-committee-of-1975-1976/.

[2] 50 U.S.C. § 1805.

[3] 50 U.S.C. § 1801(a), (b)(1).

sabotage, and terrorism.[4] This requirement remains in place today for electronic surveillance that is not targeted at foreigners abroad.

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

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

The law's sweeping new surveillance powers did not satisfy the government, however. President George W. Bush authorized a set of secret programs, code-named Stellar Wind, to collect communications and other personal data without congressional authorization.[8] One of these programs involved the domestic warrantless collection of the content of communications between suspected foreign terrorists and Americans in the United States. This was a clear violation of FISA: although the Patriot Act expanded the purposes for which the government could seek a Title I order, it did not eliminate the requirement to obtain one.

After investigative journalists exposed the program,[9] the government attempted to obtain legal cover by securing the FISA Court's approval. When the court balked,[10] the government

---

[4] 50 U.S.C. § 1801(b)(2).
[5] 50 U.S.C. § 1801(f).
[6] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U. S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 254-77, 339-60 (2004).
[7] *See* Electronic Privacy Information Center, *PATRIOT Act* (accessed Jun. 11, 2023), https://epic.org/issues/surveillance-oversight/patriot-act/; Kate Tummarello, *Debunking the Patriot Act as It Turns 15*, EFF (Oct. 26, 2016), https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15.
[8] *See* OFF. INSPECTORS GEN., DEP'T OF DEFENSE, DEP'T OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NAT'L SEC. AGENCY & OFF. DIR. NAT'L INTELLIGENCE, REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009), *available at* https://int.nyt.com/data/documenttools/savage-foia-stellarwind-ig-report/fd1368590db24fe1/full.pdf; Jake Laperruque, *Secrets, Surveillance, and Scandals: The War on Terror's Unending Impact on Americans' Private Lives,* POGO (Sept. 7, 2021), https://www.pogo.org/analysis/2021/09/secrets-surveillance-and-scandals-the-war-on-terrors-unending-impact-on-americans-private-lives.
[9] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Court*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.
[10] *See* Charlie Savage, *Documents Shed New Light on Legal Wrangling Over Spying in U.S.*, N.Y. TIMES (Dec. 12, 2014), https://www.nytimes.com/2014/12/13/us/politics/documents-shed-new-light-on-legal-wrangling-over-spying-in-us-.html?ref=politics.

turned to Congress. Officials observed that changes in communications technology had altered which communications qualified as "electronic surveillance." As a result, the government was being required to obtain a FISA Title I order to collect foreigners' communications handled by U.S. service providers. Officials argued that this was impeding counterterrorism efforts, and they asked Congress to "modernize" FISA by loosening its restrictions.[11]

Congress responded by enacting the Protect America Act in 2007,[12] soon to be replaced by the FISA Amendments Act — which created Section 702 of FISA — in 2008.[13] Section 702 allows the government to target any foreigner abroad for foreign intelligence collection. Under this authority, the government may collect all of the target's communications, including those with Americans, without obtaining any individualized court order. The only substantive restriction is that a significant purpose of the collection must be the acquisition of foreign intelligence information, defined extremely broadly to include information "related to . . . the conduct of U.S. foreign affairs."[14] The FISA Court must approve general procedures for the surveillance on an annual basis, but it has no role in approving individual targets.[15]

The government uses Section 702 to engage in two types of surveillance. The first is "upstream collection," whereby communications flowing into and out of the United States on the Internet backbone are scanned for selectors associated with designated foreigners. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired.[16] The second type of Section 702 surveillance is "PRISM collection," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn over any communications to or from the selector.[17]

Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011 — the last year for which such information is publicly available.[18] Because agencies generally store Section 702 data for at least five years, a yearly intake of 250 million Internet communications would result in at least 1.25 billion such communications residing in government databases at any given time. Given the growth in the program — from

---

[11] *Modernizing the Foreign Intelligence Surveillance Act, Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. (May 17, 2007) (statement for the record of J. Michael McConnell, Dir. Nat'l Intelligence), https://www.dni.gov/files/documents/Newsroom/Testimonies/20070501_testimony.pdf.
[12] Pub. L. 110-55 (2007).
[13] Pub. L. 110-261 (2008).
[14] 50 U.S.C. § 1801(e)(2).
[15] 50 U.S.C. § 1881a.
[16] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 36-41 (2014) [hereinafter PCLOB 702 REPORT], *available at* https://www.pclob.gov/library/702-report.pdf.
[17] *Id.* at 33–34.
[18] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).

89,138 targets in 2013[19] to 246,073 targets in 2022[20] — the number of communications collected today is likely closer to one billion annually, with several billion sitting in storage.

## II. The Impact on Americans' Privacy

Although Section 702 may only be targeted at foreigners overseas, it inevitably sweeps in Americans' communications, for the simple reason that Americans communicate with foreigners. The government does not deny that Section 702 results in the collection of Americans' communications in large numbers, although it has rebuffed lawmakers' requests[21] to provide a rough estimate of how many Americans' communications are collected.[22] Given the prevalence of international communication, however, it is safe to assume that the billions of communications acquired under Section 702 include millions of communications involving Americans.

The government refers to the collection of Americans' communications as "incidental," to signify that Americans are not the intended targets of the surveillance. Indeed, if the government's purpose were to spy on those Americans, the program would be unlawful. Such surveillance would require either a warrant (in a criminal investigation) or a FISA Title I order (in a foreign intelligence investigation). To prevent the government from using Section 702 as an end-run around these constitutional and statutory requirements, Congress included two key provisions in the law. First, it required the government to "minimize" the collection, retention,

---

[19] OFF. DIR. NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013 (Jun. 2014), *available at* https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

[20] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2022 at 18 (Apr. 2023) [hereinafter OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023)], *available at* https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.

[21] *See* Letter from Senators Ron Wyden and Mark Udall to The Honorable I. Charles McCullough III, Inspector General of the Intelligence Comm., and Dr. George Ellard, Inspector General, Nat'l Sec. Agency (May 4, 2011), *available at* https://www.wyden.senate.gov/download/?id=CE360936-DFF9-4273-8777-09BF29565086&download=1; Ron Wyden, *Senators Seek Answers from DNI on How Many of Americans' Communications Have Been Monitored* (Jul. 12, 2012), https://www.wyden.senate.gov/news/press-releases/senators-seek-answers-from-dni-on-how-many-of-americans-communications-have-been-monitored; Letter from Rep. John Conyers, Jr., et al., to James Clapper, Dir. Nat'l Intelligence (Apr. 22, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

[22] Initially, the government claimed that providing such an estimate would itself violate Americans' privacy. *See* Letter from The Honorable I. Charles McCullough, III, Inspector General of the Intelligence Comm., to Senators Ron Wyden and Mark Udall (Jun 15, 2012), *available at* https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1. After privacy experts and advocates refuted that claim, *see* Letter from Brennan Ctr. for Justice, et al., to James Clapper, Dir. Nat'l Intelligence (Oct. 29, 2015), *available at* https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf, the Obama administration agreed to provide an estimate in early 2017. *See* Press Release, U.S. House Comm. on the Judiciary Democrats, *Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance* (Dec. 16, 2016), *available at* https://democrats-judiciary.house.gov/news/press-releases/bipartisan-house-coalition-presses-clapper-information-phone-email-surveillance. The Trump administration then reneged on that promise, *see* Dustin Volz, *NSA Backtracks On Sharing Number of Americans Caught in Warrant-less Spying*, REUTERS (Jun. 12, 2017), http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B, and there is no sign that the current administration intends to take a different approach.

and sharing of U.S. person information.[23] Second, it required the government to certify to the FISA Court, on an annual basis, that it is not engaged in "reverse targeting"—i.e., using Section 702 as a way to gain access to the communications of "particular, known" Americans.[24]

Over the past 15 years, it has become abundantly clear that these protections have failed. Rather than actually "minimize" the retention and use of Americans' communications, as Congress directed, the government retains such data for years on end — and routinely searches it for Americans' communications to use against them in both criminal and foreign intelligence investigations. The government also has engaged in so-called "abouts" collection, a practice that inevitably results in the acquisition of purely domestic communications. These problems are exacerbated by the broad scope of surveillance authorized by the law, which not only increases the potential volume of "incidental" collection, thus directly implicating Americans' privacy, but also is creating legal headaches for U.S. businesses.[25]

### A. Minimization and Its Loopholes

While the concept behind minimization is fairly simple, the statutory language is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[26] The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[27]

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data from its PRISM collection with the FBI, the CIA, and (as of April 2017) the National Counterterrorism Center (NCTC).[28] All four

---

[23] 50 U.S.C. § 1881a(e).
[24] 50 U.S.C. § 1881a(b)(2), (h)(2)(A)(iii).
[25] In this statement, I use quotation marks for the terms "target," "incidental," and "minimize," to underscore that they are terms of art with particular legal meanings. Legal and policy defenses of Section 702 rely heavily on these terms and concepts. The impact on Americans' privacy, however, does not. If the government is collecting tens of millions of Americans' communications and keeping them for years in databases where they are vulnerable to abuse, inadvertent mishandling, or theft, it matters little — from a practical perspective — that their initial acquisition was "incidental," or that the procedures allowing them to be kept and stored include "minimization" in their title. And if FBI agents are searching this data for Americans' communications, reading and listening to them, and using them against Americans in legal proceedings, those Americans will not be particularly comforted (indeed, they may well be baffled) to hear that they are not "targets."
[26] 50 U.S.C. § 1801(h)(1).
[27] 50 U.S.C. § 1801(h)(3).
[28] MATTHEW G. OLSEN, ASS'T ATT'Y GEN., NAT'L SEC. DIV., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE

agencies generally may keep unreviewed raw data — including data about U.S. persons — for five years after the certification expires;[29] they also can seek extensions from a high-level official,[30] and the 5-year limit does not apply to encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) or communications that "reasonably appear[]…to contain secret meaning."[31] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[32]

If the NSA discovers U.S. person information that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.[33] The NSA, however, interprets this requirement to apply only if the NSA analyst determines "not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need."[34] This is an impossibly high bar, and so, "in practice, this requirement rarely results in actual purging of data."[35]

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

---

INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 9 (Mar. 14, 2022) [hereinafter NSA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_NSA_Minimization_Procedures-Amended.pdf.

[29] *Id.* at § 4(c)(1)-(2) (2020); LISA O. MONACO, DEPUTY ATT'Y GEN., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § III.D.4.b (Oct. 14, 2021) [hereinafter FBI 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_FBI_Minimization_Procedures.pdf; LISA O. MONACO, DEPUTY ATT'Y GEN., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 2.a (Oct. 14, 2021) [hereinafter CIA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_CIA_Minimization_Procedures.pdf; LISA O. MONACO, DEPUTY ATT'Y GEN., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § B.2.a (Oct. 14, 2021) [hereinafter NCTC 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_NCTC_Minimization_Procedures.pdf.

[30] PCLOB 702 REPORT, *supra* note 16, at 60; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § B.2.a.

[31] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 7(a)(1).a; FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § I.4; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at § 3.c.

[32] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at §§ 6(1), 7(a); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.A.3, C.1.b; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at §§ 3.a, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § B.3.

[33] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 4(b)(1), (c).

[34] PCLOB 702 REPORT, *supra* note 16, at 62.

[35] *Id.*

of a crime, the 5-year limit evaporates, and the FBI may keep the data for 15 years.[36] A similar rule applies to the NCTC.[37]

If any of the four agencies — all of which have access to raw data — disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person's identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.[38]

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

### B. Back Door Searches

Perhaps the most glaring failure of the protections Congress put in place for Americans' privacy is the practice of "back door searches." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans (which would constitute "reverse targeting"). Immediately upon obtaining the data, however, all four agencies have procedures in place that allow them to sort through the data looking for the communications of particular, known Americans — the very people in whom the government just disclaimed any interest.[39] This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the requirements of the Fourth Amendment and Title I of FISA.

According to the Privacy and Civil Liberties Oversight Board (PCLOB), the FBI routinely conducts these searches at the "assessment" phase of its investigations[40]—i.e., before agents have a factual basis to suspect criminal activity, let alone probable cause and a warrant. For years, the FBI resisted calls to disclose how many backdoor searches it performs each year. But after Congress and the FISA Court forced the FBI to track those queries, the government lost its excuse to withhold the number. In 2022, the ODNI's annual statistical transparency report revealed that, in 2021 alone, the FBI conducted up to *3.4 million* U.S. person queries of federated

---

[36] FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.D.4.c.
[37] [Redacted], at 40 (FISA Ct. Apr. 26, 2017), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
[38] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 8(2), (9); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § IV.A.1–2, B; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at §§ 5, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § D.1–2. In addition, the FBI may disseminate unminimized Section 702 data to the NSA, CIA, and in some cases the NCTC. FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § IV.E.
[39] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 4(b)(4); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.D.3; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at § 4; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § C.1.
[40] PCLOB 702 REPORT, *supra* note 16, at 59.

data systems that included Section 702 data.[41] In 2022, after the FBI made changes to its data systems that required FBI agents to "opt in" to receiving Section 702 data in response to queries rather than having to "opt out," that number dropped to around 200,000,[42] which is likely to be a more typical number going forward. While that represents a sizeable decrease, it is still an enormous number by any standard, comprising more than 500 warrantless searches for Americans' communications each day.

Indeed, on some days, that number is much higher. The FBI has adopted a practice of "batch queries," in which it runs hundreds or thousands of queries under a single justification. In March 2017, against the advice of its Office of General Counsel, the FBI performed a batch query for 70,000 people — most of whom were presumably U.S. persons, given that the targets of the query were people with access to FBI facilities.[43]

Government officials have defended back door searches, claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose.[44] This legal defense entirely misses the point. The staggering figure of 200,000 U.S. person queries per year,[45] even with all the government's caveats,[46] makes clear that there is nothing "incidental" about Section 702's impact on Americans. Warrantless access to Americans' communications has become a core feature of a surveillance program that purports to be solely foreign-focused.

In any event, the argument that Section 702 data may lawfully be used for any purpose ignores Congress's command to agencies to "minimize" information about U.S. persons. The very meaning of "minimization" is that agencies may *not* use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: As Judge Bates of the FISA Court has observed, "[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[47] Whatever merit the government's defense might

---

[41] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2021 at 21 (Apr. 2022) [hereinafter OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022)], *available at* https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.

[42] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023), *supra* note 20, at 24. The government has provided a "de-duplicated" number of 119,383, which represents the number of unique identifiers used to perform queries. *Id*. That is likely a more accurate proxy for the number of Americans affected, but it fails to capture situations in which the FBI performs repeated searches of the same account to find additional information. Each of those searches is a distinct privacy intrusion. Accordingly, the number of total searches (204,090) is a better indicator of the cumulative privacy impact of this practice.

[43] [Redacted], 402 F. Supp. 3d 45, 76 (FISA Ct. 2018).

[44] *See, e.g., FISA Reauthorization, Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (Jun. 27, 2017), *available via* CSPAN, 44:02, https://www.c-span.org/video/?430549-1/fisa-reauthorization (testimony of Stuart J. Evans, Deputy Ass't Att'y Gen. for Intelligence, Nat'l Sec. Div., Dep't of Justice).

[45] Although the FBI is by far the most prolific user of back door searches, other agencies also make use of them. In 2022, the NSA, CIA, and NCTC used 4,684 U.S. person terms to query communications content and metadata. OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023), *supra* note 20, at 20.

[46] ODNI notes that its figures likely overstate the number of Americans affected, in part because there could be multiple searches relating to a single individual. But even if ODNI's numbers are off by an order of magnitude, 20,000 warrantless searches for Americans' communications each year is an alarming number.

[47] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011).

or might not have in other contexts,[48] it is contrary to the constitutional and statutory grounding of the Section 702 program.

Despite these principles, the FISA Court has held that backdoor searches are lawful. But among the handful of regular federal courts outside the FISA Court that have had the opportunity to weigh in on this question, a divide has emerged, with several judges — including a unanimous panel of the Second Circuit Court of Appeals — raising constitutional concerns.[49] Notably, the judges on the other side of this divide have relied heavily on a misrepresentation that the Department of Justice made in litigation, i.e., that government officials need to review Americans' communications anyway as part of the minimization process.[50] Outside of the courts, constitutional scholars have argued that backdoor searches must be treated as a separate Fourth Amendment event than the underlying collection, [51] thus triggering (in most cases) the warrant requirement.[52] In short, the constitutionality of backdoor searches is anything but settled.

---

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

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

[50] *See* United States v. Mohamud, 2014 WL 2866749, at *26 (D. Oregon 2014); United States v. Hasbajrami, 2016 WL 1029500, at *12n.20 (E.D.N.Y. 2016); United States v. Al-Jayab, No. 16 CR 181, at 55-6 (N.D. Ill. June 28, 2018), *available at* https://storage.courtlistener.com/recap/gov.uscourts.ilnd.324196/gov.uscourts.ilnd.324196.115.0.pdf; *see also* Elizabeth Goitein, *Americans' Privacy at Stake as Second Circuit Hears Hasbajrami FISA Case*, JUST SEC. (Aug. 24, 2018), https://www.justsecurity.org/60439/americans-privacy-stake-circuit-hears-hasbajrami-fisa-case/ (explaining the misrepresentation on which the court relied).

[51] *See* Orin Kerr, *The Fourth Amendment and querying the 702 database for evidence of a crime*, WASH. PO. (Oct. 20, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/20/the-fourth-amendment-and-querying-the-702-database-for-evidence-of-crimes/.

[52] The Supreme Court has held that warrantless searches are *per se* unreasonable unless they fall within an established exception to the warrant requirement. City of Los Angeles v. Patel, 576 U.S. 409, 419-420 (2015). A few circuit courts have held than there is a "foreign intelligence" exception to the warrant requirement in at least some cases; the Fourth Circuit, for instance, recognized such an exception in cases where the surveillance is for the primary purpose of obtaining foreign intelligence and the target is a foreign power or agent of a foreign power. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980). The Supreme Court has not recognized such an exception, however. Accordingly, it would be a stretch to say that there is an established foreign intelligence exception to the Fourth Amendment's warrant requirement, let alone one that is broad enough to support the government's current practice with regard to U.S. person queries. *See* ELIZABETH GOITEIN & FAIZA PATEL, WHAT

### C. "Abouts" Collection

The government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, *or about* the target.[53] The inclusion of "about" in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been applied to collect communications between non-targets that include the "selectors" associated with the target (e.g., the target's e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention Vladmir Putin, the Chinese government, or a wide array of other individuals and groups who are common topics of conversation. Although Section 702 prohibits the intentional acquisition of purely domestic communications, such acquisition is an inevitable result of so-called "abouts" collection.[54]

The NSA's failure to comply with special minimization rules for "abouts" collection (discussed later in this statement), which delayed the FISA Court's approval of the program in 2016, led the agency to stop the practice in April of 2017.[55] When Congress reauthorized Section 702 in early 2018, it required the government to provide 30 days' notice if it intended to restart "abouts" collection. There is no public indication that this has happened, and no FISA Court decision approving the reinstitution of "abouts" collection has been released. However, the door remains open to the NSA resuming this practice in the future.

### D. Scope of Surveillance

The permissible scope of surveillance under Section 702 is exceedingly broad. Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only substantive limitation on collection imposed by the statute is that the government must certify, on a program-wide basis, that acquiring foreign intelligence is a significant purpose of the collection.[56]

FISA's definition of foreign intelligence is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information "that relates to . . . the conduct of the foreign affairs of the United States."[57] This could encompass everyday discussions of current events. A conversation between friends or colleagues about trade between the U.S. and China "relates to the conduct of foreign affairs," as does a conversation about whether the U.S. should do more to support Ukraine. Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether.[58] Finally, the statute requires the FISA Court to accept the government's

---

WENT WRONG WITH THE FISA COURT 11-12 (Brennan Ctr. for Justice 2015), https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court (discussing case law on foreign intelligence exception).

[53] PCLOB 702 REPORT, *supra* note 16, at 37.

[54] PCLOB 702 REPORT, *supra* note 16, at 119-122.

[55] Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets,* N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.

[56] 50 U.S.C. § 1881a(g)(2)(A)(v).

[57] 50 U.S.C. § 1801(e)(2).

[58] *In re* Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).

certifications under Section 702 as long as they contain the required elements.[59] These factors greatly weaken the force of the "foreign intelligence purpose" limitation.

Going forward, Section 702 surveillance might be somewhat constrained by President Biden's recent executive order establishing new rules for the collection of signals intelligence. The order sets forth twelve legitimate objectives for signals intelligence collection, [60] which are more specific than the general language contained in FISA's definition of "foreign intelligence information." However, these purpose-based limitations do not necessarily translate into constraints on the scope of surveillance. For instance, one of the permissible purposes is to protect against threats to cybersecurity — a goal that could in theory justify constant monitoring of any and all Internet networks. Furthermore, the order permits the president to add to the list of objectives, and to do so secretly if the president determines that disclosure of the new objective(s) would harm national security.

The overbroad scope of permissible Section 702 surveillance not only disregards the privacy rights of foreigners who pose no threat to the United States; it has significant implications for Americans' privacy, as well. The larger the pool of foreigners who may be targeted, the larger the pool of Americans whose communications are subject to "incidental" collection. Moreover, the ability to target ordinary private citizens of other nations greatly increases the likelihood of the government acquiring entirely innocent conversations between Americans and their friends, relatives, and business colleagues overseas.

Section 702's expansive reach is also causing significant legal and economic problems for U.S. businesses. On two occasions, the Court of Justice for the European Union (CJEU) has struck down agreements between the United States and the European Union governing the transfer of data between EU and U.S. companies.[61] One major reason for the court's rulings is that Section 702 provides the U.S. government with ready access to EU citizens' data in the hands of U.S. companies, in contravention of European law. President Biden's recent executive order was issued to pave the way for a new data-transfer agreement, but observers doubt whether that order includes sufficient constraints on surveillance to satisfy the CJEU.[62] More than 5,000 U.S. companies rely on a U.S.-EU data-sharing agreement to do business.[63] Highlighting the risk to U.S. companies, Meta was recently fined $1.3 billion by Irish privacy regulators for transferring EU citizens' data to the United States without a valid agreement in place.[64]

---

[59] 50 U.S.C. § 1881a(i)(3)(A).
[60] Exec. Order 14086, § 2(b)(i)(A), 87 Fed. Reg. 62283-4 (Oct. 7, 2022).
[61] *See* Case C-311/18, Data Protection Commissioner v. Schrems, ECLI:EU:C:2020:559 (Jul. 16, 2020), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4231279; Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.
[62] American Civil Liberties Union, *To Make Real Progress, ACLU Calls on Congress to Enact Meaningful Surveillance Reform* (Oct. 7, 2022), https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy.
[63] *See* Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. TIMES (Jul. 16, 2020), https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html.
[64] Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, CNN (May 22, 2033), https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html.

## III. Violations of Statutory and Court-Ordered Privacy Protections

Section 702 has been marked since its inception by repeated, often systemic violations of the rules Congress and the FISA Court have put in place to protect Americans' privacy. The extent of this non-compliance is alarming in its own right. Any unauthorized collection, search, or dissemination can result can result in Americans being investigated without proper legal basis or sensitive information falling into the hands of people who could misuse it. But recent violations raise even more acute concerns: the targeting of Americans based on race, ethnicity, politics, or journalistic activity.

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

Although no court order is required to conduct U.S. person queries in most cases, Congress and the FISA Court have attempted to place some limits on the conduct of these backdoor searches. The FBI, however, has routinely violated those limits.

In 2018, Congress required the FBI to obtain a probable-cause order from the FISA Court before reviewing the results of U.S. person queries in a very small subset of cases, i.e., predicated criminal investigations unrelated to national security.[65] This provision is rarely triggered, both because "related to national security" is a subjective and malleable criterion and because the FBI, according to the PCLOB, routinely performs U.S. person queries at the "assessment" stage — i.e., before the FBI has sufficient information to open a predicated investigation.[66] Nonetheless, according to the ODNI's statistical transparency reports, this requirement has been triggered on approximately 100 occasions over the past four years.[67] Incredibly, the FBI did not obtain a FISA Court order in a *single one* of those cases.

Addressing this issue in its December 2019 opinion, the FISA Court noted that "*[s]ome* violations resulted *in part* from the manner in which FBI systems displayed information in response to queries" (emphasis added).[68] Specifically, systems would display query results in a

---

[65] 50 U.S.C. § 1881a(f)(2)(A).

[66] PCLOB 702 REPORT, *supra* note 16, at 59.

[67] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2020 at 21 (Apr. 2021) [hereinafter OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2021)], *available at* https://www.dni.gov/files/CLPT/documents/2021_ASTR_for_CY2020_FINAL.pdf; OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 41, at 22; OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023), *supra* note 20, at 26. Before 2021, rather than reporting the number of times the court-order requirement (which appears in Section 702(f)(2)) was triggered, the government reported a slightly broader number, i.e., how many times the government reported to the FISA Court that FBI agents had accessed Section 702 data in response to queries not designed to return foreign intelligence. (Congress had required this reporting in 2018.) However, in its 2020 report, the government noted that "a Section 702(f)(2) order should have been obtained . . . in nearly all of [these] queries." OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT at 20 (2021). The government also stated that, "in some instances, a single report to the Court involved multiple queries on the same day by the same user that returned and displayed Section 702 content." *Id.* at 21. Accordingly, the total number of cases in which the government should have obtained a court order before accessing queries is almost certainly higher than 100.

[68] [Redacted], at 69 (FISA Ct. Dec. 6, 2019), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1060343/gid_c_00282.pdf?sequence=1&isAllowed=y.

summary field that showed 100 characters of text around the query term within the records identified as responsive to the query. Of course, FBI agents still could have obtained FISA Court orders before opening the results to see more than the 100 characters. According to the Court, however, "FBI personnel are known to have taken further steps in response to such displays (e.g., opening 'products' containing contents returned by a query), thereby accessing Section 702-acquired contents beyond what was initially displayed to them."[69] In any event, this feature of the FBI systems did not account for all of the violations.

The vast majority of U.S. person queries fall outside this narrow court-order requirement. In those cases, the only substantive restriction on queries is the standard set forth in the FBI's querying procedures (and previously in its minimization procedures, before Congress required agencies to develop separate querying procedures when it reauthorized Section 702 in 2018). Under that standard, "[e]ach query of FBI systems [containing raw Section 702 data] . . . must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime, unless otherwise specifically excepted in these procedures."[70] This is a fairly low bar, to be sure. Even so, government reports and FISA Court opinions issued in recent years show that the FBI has engaged in "widespread violations" of this rule.[71]

A recently declassified April 2022 FISA Court opinion and two 2022 compliance reports reveal a series of particularly disturbing violations. In 2021, FBI agents conducted more than a hundred backdoor searches on people arrested during protests in the spring of June 2020 — i.e., following the police killing of George Floyd. The agents said they wanted to find out whether the protesters had ties to foreign terrorists, but they had no reason to suspect any such connections.[72] In addition, agents ran thousands of searches relating to the January 6th attack on the U.S. Capitol, also on a baseless hunt for evidence of foreign ties.[73] And agents ran searches for information about a sitting U.S. congressman;[74] a local political party;[75] multiple U.S. government officials, journalists, and political commentators;[76] 19,000 donors to a political

---

[69] *Id.* at 70.
[70] [Redacted], 402 F. Supp. 3d 45, 75 (FISA Ct. 2018).
[71] [Redacted], at 44 (FISA Ct. Nov. 18, 2020), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1061209/gid_c_00289.pdf?sequence=1&isAllowed=y.
[72] [Redacted], at 27 (FISA Ct. Apr. 21, 2022), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.
[73] *Id.* at 28-9.
[74] *See* DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE 58 (Dec. 2021) [hereinafter DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT (Dec. 2021)], https://www.intelligence.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf.
[75] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT 58 (Dec. 2021).
[76] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE 60 (Aug. 2021), https://www.intel.gov/assets/documents/702%20Documents/declassified/22nd_Joint_Assessment_of_FISA_702_Compliance_CLEARED_REDACTED_FOR_PUBLIC_RELEASE.pdf.

campaign;[77] and two "Middle Eastern" men who were reported by a witness because they were loading boxes labeled "Drano" into a vehicle.[78]

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

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

- people who came to the FBI to perform repairs;[79]
- victims who approached the FBI to report crimes;[80]
- business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy";[81]
- college students participating in a "Collegiate Academy";[82]
- police officer candidates;[83] and
- colleagues and relatives of the FBI agent performing the search.[84]

The FISA Court expressed "serious concern" about "the large number of queries evidencing a misunderstanding of the querying standard — or indifference to it."[85] The Court posited that the reported violations were likely the tip of the iceberg. It noted that some FBI offices field offices go for periods of two years or more between oversight visits, and ultimately, Justice Department overseers "review only a small portion of the queries conducted."[86] The Court wrote, "[I]t appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the Court."[87]

The government told the FISA Court that these errors stemmed from "fundamental misunderstandings by some FBI personnel [about] what the standard 'reasonably likely to return foreign intelligence information' means."[88] The FBI claims to have addressed this problem through new training requirements, internal oversight measures, and data systems adjustments that were implemented in 2021 and 2022. This response would be more reassuring if the standard

---

[77] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 29.
[78] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT 61 (Dec. 2021).
[79] [Redacted] (FISA Ct. Nov. 18, 2020), *supra* note 71, at 40.
[80] *Id.* at 40.
[81] *Id.* at 39.
[82] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 68, at 66.
[83] *Id.*
[84] [Redacted], 402 F. Supp. 3d 45, 78 (FISA Ct. 2018).
[85] *Id.*
[86] *Id.* at 79.
[87] *Id.* at 79–80.
[88] *Id.* at 77.

in question were a new one. But that standard has been in place for well over a decade,[89] and throughout that period, the government has been touting its rigorous training and oversight,[90] assuring lawmakers that these protections were more than adequate to safeguard Americans' rights. The notion that the FBI simply needs a little more time to get its house in order is both difficult to credit and far too dismissive of the constitutional rights that have been violated.

Indeed, the recent FISA Court opinions are only the latest in a string of opinions dating back to 2009 that reveal an unbroken pattern of violations — by the FBI, NSA, and CIA — of the rules designed to protect Americans' privacy. On numerous occasions, the government has responded by pledging to improve its training and/or bolster internal oversight. None of these efforts has been sufficient to disrupt the pattern for any significant length of time. In the words of surveillance expert Julian Sanchez, the FISA Court and the government have been engaged in a game of "compliance whackamole."[91]

In any event, the FBI's own data suggest that an unacceptable number of violations are still occurring, despite the changes it has put in place. A report of the FBI's newly-created Office of Internal Audits found that the FBI's adjustments reduced the non-compliance rate from 18% to 4%.[92] There are serious questions about the report's methodology; among other things, FBI agents were asked to justify their queries long after they had taken place, and they were aware that their answers were being considered as part of a compliance audit. Even accepting the 4% number on its face, however, applying it to the 200,000 U.S.-person-query figure yields more than *8,000 searches each year* that violate even the FBI's own low internal standard.

The additional changes the FBI announced today (June 13, 2023) will not solve the problem. FBI agents who are found to engage in "performance incidents involving negligence" will now face escalating consequences for each incident. The first incident will result in a temporary loss of access to FISA data while the agent undergoes retraining and one-on-one counseling, while subsequent incidents would prompt "further measures, up to and including indefinite loss of FISA access, reassignment to a new role, and/or referral to the FBI's Inspection

---

[89] *See* [Redacted], at 26-7 (FISA Ct. Nov. 6, 2015), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/official-statement/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (noting that foreign-intelligence and evidence-of-a-crime queries "have been explicitly permitted by the FBI Minimization Procedures since 2009."). Indeed, a similar standard is part of the minimization rules for FISA generally, so the standard actually predates the Section 702 procedures. *See* MICHAEL MUKASEY, U.S. DEP'T OF JUSTICE, STANDARD MINIMIZATION PROCEDURES FOR FBI SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT § III.D (Oct. 22, 2008), *available at* https://www.aclu.org/sites/default/files/field_document/2017.5.8_savage-nyt-foia-fbi-2008-09-fisa-standard.pdf.

[90] *See, e.g.,* Off. Dir. Nat'l Intelligence, *Section 702 Overview,* at 8-9 (accessed Jun. 16, 2023), https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

[91] *See* Privacy & Civil Liberties Oversight Bd., *PCLOB Public Forum on FISA Section 702*, YOUTUBE (Jan. 12, 2023), 57:50, https://www.youtube.com/watch?v=AZvaimMTqio&t=357s (comments of Julian Sanchez).

[92] FEDERAL BUREAU OF INVESTIGATION, OFF. OF INTERNAL AUDITING, FISA QUERY AUDITING at slide 6 (May 10, 2023), *available at* https://int.nyt.com/data/documenttools/fisa-query-audit-5-10/d9d8e20bafef27c8/full.pdf.

Division." In addition, performance ratings of field office leaders will eventually incorporate the offices' FISA compliance.[93]

It is frankly shocking that such basic accountability measures were not in place before. It is unclear, however, what conduct the FBI would consider to be "negligent" for purposes of triggering remedial measures. In the same announcement, the FBI notes that "instances of intentional or reckless behavior have been extremely rare, and there have been none identified since 2018."[94] Yet the FISA Court's April 2022 opinion recounts a 2021 incident in which an agent admitted that "he always recorded queries as not involving U.S.-person query terms even if the facts indicated otherwise, *e.g.,* identifiers for local businesses and mosques."[95] An agent also queried *19,000* campaign donors to find evidence of foreign ties, when there was reason to suspect such ties in only eight cases. The fact the FBI does not consider these and similar incidents to reflect "recklessness" raises serious questions about how it evaluates agents' conduct. When one also considers that compliance audits reach only a small fraction of U.S. person queries;[96] that the consequences of the first infraction are fairly minor; and that even repeated violations seemingly will not lead to suspension or termination, it is hard to imagine that these belated measures will result in the dramatic behavior change that is necessary.

### B. Other Violations

On multiple other occasions in the past fifteen years, the FISA Court has had occasion to rebuke the government for repeated, significant, and sometimes systemic failures to comply with statutory requirements or court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, access, dissemination, and retention. It is instructive to review some of the Court's comments in these cases. The following statements are excerpted from nine opinions spanning the years 2009 through 2020:

- "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively."[97]

---

[93] *See* Federal Bureau of Investigation, *FBI Deputy Director Highlights Bureau's New FISA Query Accountability Procedures* (Jun. 13, 2023), https://www.fbi.gov/news/press-releases/fbi-deputy-director-highlights-bureau-s-new-fisa-query-accountability-procedures#Fact-Sheet.

[94] *Id.*

[95] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 48.

[96] *See* [Redacted], 402 F. Supp. 3d 45, 79 (FISA Ct. 2022) (noting that "some [field] offices go for periods of two years or more between oversight visits" and that oversight personnel "review only a small portion of the queries conducted").

[97] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 10–11 (FISA Ct. Mar. 2, 2009).

- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[98]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[99]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[100]
- "[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last."[101]
- "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions [under Section 702] mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[102]
- "The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISA orders."[103]
- "As far as can be ascertained, the requirement was simply ignored."[104]
- "Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . ."[105]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[106]
- "[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."[107]
- "The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition…presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve."[108]
- "As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained… The government has provided no meaningful explanation why these violations occurred, but it seems likely

---

[98] *Id.* at 6.
[99] *Id.* at 10.
[100] *Id.* at 15.
[101] *Id.* at 16.
[102] [Redacted], 2011 WL 10945618, at *5 n. 14 (FISA Ct. Oct. 3, 2011).
[103] [Redacted], Docket No. PR/TT [Redacted], at 4 (FISA Ct. [Redacted]), *available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[104] *Id.* at 19.
[105] *Id.* at 20.
[106] *Id.* at 21.
[107] *Id.* at 22.
[108] *Id.* at 77.

that widespread ignorance of the rules was a contributing factor."[109]

- "Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information."[110]
- "[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance."[111]
- "The Court was extremely concerned about these additional instances of non-compliance."[112]
- "Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information . . . ."[113]
- "The Court did not find entirely satisfactory the government's explanations of the scope of [its] segregation errors and the adequacy of its response to them . . . ."[114]
- "[A] non-compliance rate of 85% raises substantial questions about the appropriateness of using [a redacted tool] to query FISA data."[115]
- "At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those [Inspector General] and [NSA Office of Compliance for Operations] reviews at the October 4, 2016 hearing to an institutional lack of candor on NSA's part and emphasized that this is a very serious Fourth Amendment issue."[116]
- "Beginning in October 2016, while the 2016 Certifications were pending before the FISC, the government reported that NSA had violated that querying prohibition much more frequently than had been previously disclosed."[117]
- "The quarterly reports also revealed that in several of these incidents the CIA or the FBI was responsible for conducting post-targeting content review but did not conduct timely reviews."[118]
- "It must be noted, however, that the government has unjustifiably disregarded the current reporting requirement [with respect to retention of raw Section 702 data]. Instead of taking concrete steps to comply even partially with the Court's directive (or timely seeking relief from it), it chose to wait while the FBI reportedly worked on guidance to instruct its personnel on how to handle unminimized Section 702 information on these archival systems."[119]

---

[109] *Id.* at 95.
[110] *Id.* at 115.
[111] [Redacted], at 48–49 (FISA Ct. Nov. 6, 2015), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/official-statement/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[112] *Id.* at 50.
[113] *Id.* at 58.
[114] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 37, at 80.
[115] *Id.* at 82.
[116] *Id.* at 19 (internal quotation marks omitted).
[117] [Redacted], 402 F. Supp. 3d 45, 56 (FISA Ct. 2018).
[118] *Id.* at 104.
[119] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 68, at 44.

- "It should be unnecessary to state that government officials are not free to decide for themselves whether or to what extent they should comply with Court orders."[120]
- "The government has not reported such instances [of misuse of Section 702-acquired information] in timely fashion. Rather, they have been reported to the Court belatedly, usually after they were uncovered during oversight reviews."[121]
- "The FBI's handling of the Carter Page applications, as portrayed in the OIG report, was antithetical to the heightened duty of candor . . . . The frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable."[122]
- "[T]he OIG expressed a 'lack of confidence that the Woods Procedures are working as intended' — i.e., 'as a means toward achiev[ing]' the FBI's professed policy 'that FISA applications be "scrupulously accurate."' . . . It would be an understatement to note that such lack of confidence appears well founded. None of the 29 cases reviewed had a Woods File that did what it is supposed to do: support each fact proffered to the Court. For four of the 29 applications, the FBI cannot even find the Woods File . . . . For three of those four, the FBI could not say whether a Woods File ever existed."[123]

A particularly notable Section 702 compliance failure, discussed in the FISA Court's April 26, 2017 opinion, was the NSA's widespread use of U.S. person identifiers to query certain data obtained through upstream collection. The FISA Court had prohibited such queries in 2011, in response to its discovery that the NSA had for years been pulling in substantial numbers of wholly domestic communications by virtue of "abouts" collection. The Court had found the NSA's handling of this data unconstitutional, and the ban on U.S. person queries of upstream data was one of the key remedies adopted to cure the constitutional defect.

In January 2016, however, the NSA Inspector General reported internally that agency analysts were not fully complying with this limitation, based on an examination of three months of audit data from early 2015. The Inspector General and the NSA's Office of Compliance for Operations began studies of other time periods, and "preliminary results [suggested] the problem was widespread during all periods under review."[124] In other words, at no point during the operation of upstream collection — either in the years before the NSA informed the Court that it was collecting wholly domestic communications, or in the subsequent years when this data was supposedly off limits to U.S. person queries — had this surveillance operated within the bounds of the Constitution.

---

[120] *Id.* at 45.
[121] *Id.* at 71-72.
[122] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, at 3 (Dec. 17, 2019), *available at* https://www.fisc.uscourts.gov/sites/default/files/MIsc%2019%2002%20191217.pdf.
[123] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, at 2 (Apr. 3, 2020), *available at* https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Order%20PJ%20JEB%20200403.pdf.
[124] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 37, at 19.

Nonetheless, the NSA waited for several months before informing the FISA Court of the problem, which it blamed on "human error" and "system design issues."[125] The Court chided the government for this "institutional lack of candor."[126] It granted short-term extensions of Section 702 surveillance authority while the government attempted to resolve the issue, but as of late January 2017, "[t]he government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries,"[127] and as of March, "continued to . . . investigate potential root causes of non-compliant querying practices."[128] With no resolution in sight, and with the Court unwilling to certify the program while the problem remained, the NSA made the only possible choice: to halt "abouts" collection for the time being.

The Court's April 2017 opinion also includes a long list of other compliance failures. For instance, between November 2015 and May 2016, no less than *85 percent* of the NSA's queries using identifiers of U.S. persons targeted under Sections 704 and 705(b) resulted in improper querying of Section 702 data.[129] The Court also found that the FBI had shared raw Section 702 information with a redacted entity "largely staffed by private contractors," and that "the [redacted] contractors had access to raw FISA information that went well beyond what was necessary" to perform their jobs.[130] And the Court noted that "[r]ecent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements," resulting in "indefinite retention" of some data.[131]

More compliance incidents followed. As recounted in the FISA Court's December 2019 opinion, the NSA determined that it was losing foreign intelligence information as a result of a court-ordered rule that required the agency to use certain technical methods to limit collection of purely domestic communications. Its solution was to disregard the rule. Only when Section 702 was next up for reauthorization did the NSA disclose the violation and ask the Court to rescind the requirement. The Court, in a model of understatement, noted that "the proper course would have been to seek amendment of the procedures earlier, rather than unilaterally deciding to deviate from them."[132] The Court's November 2020 decision also makes reference to a heavily redacted "potential compliance incident" involving NSA that was under investigation by the government.[133]

Another revelation of NSA non-compliance came last November, when the agency responded to a Freedom of Information Act request filed six years ago by releasing a heavily redacted 2016 report of the NSA's Inspector General.[134] The report details how one NSA analyst launched a surveillance project in early 2013 that targeted Americans' communications without a

---

[125] *Id.* at 20.
[126] *Id.* at 19.
[127] *Id.* at 21.
[128] *Id.* at 23.
[129] *Id.* at 82.
[130] *Id.* at 84.
[131] *Id.* at 87–9.
[132] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 68, at 13.
[133] [Redacted] (FISA Ct. Nov. 18, 2020), *supra* note 71, at 37–8.
[134] OFF. INSPECTOR GEN., NAT'L SEC. AGENCY, REPORT OF INVESTIGATION: MISUSE OF SIGINT SYSTEMS (Feb. 12, 2016), *available at* https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rgMApjakmUtM/v0.

FISA Court order and without a foreign intelligence purpose, in violation of FISA, Executive Order 12333, and multiple agency policies. Despite whistleblowers' complaints, NSA officials allowed the project to continue because — as they explained to the Inspector General — the project was complex and they didn't understand it. This illegal project continued for three years until the Inspector General's office completed its investigation.

Former NSA Director Keith Alexander, commenting on the report's release, asserted that "[w]hen somebody does the wrong thing, we find them, and we hold them accountable."[135] In fact, the Inspector General's report specifically found that oversight by NSA officials was inadequate, and the NSA has refused to answer questions about whether any action was taken against the analyst who developed and ran the illegal program.[136]

Most recently, the April 21, 2022 FISA Court opinion (which the government did not publicly release until May 2023) confirms that improper U.S. person queries continue at the NSA. The Court reported that a flawed processing system used by the NSA resulted in 18 identified instances of improper U.S. person queries, and that "other improper U.S.-person queries also likely occurred."[137] Separately, the NSA conducted 77 U.S. person queries that had not been properly approved.[138]

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

## IV. Needed Reforms

The above discussion makes clear that Congress should not reauthorize Section 702 without far-reaching reforms. Section 702 itself should be amended to close the backdoor search loophole, strengthen the reverse-targeting prohibition and minimization requirements, prohibit "abouts" collection, and narrow the scope of surveillance. For these reforms to be effective, however, Congress must go beyond Section 702. It also must address broader problems in FISA by bolstering judicial oversight and by completing the modernization of FISA to ensure protections for Americans' communications regardless of where they are routed or stored. Finally, Congress should address statutory gaps and outdated laws that could allow warrantless

---

[135] Jason Leopold, Katrina Manson & William Turton, *NSA Watchdog Concluded One Analyst's Surveillance Project Went Too Far*, BLOOMBERG (Nov. 1, 2022), https://www.bloomberg.com/news/articles/2022-11-01/nsa-watchdog-concluded-one-analyst-s-surveillance-project-went-too-far.
[136] *Id.*
[137] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 70.
[138] *Id.*

surveillance of Americans to migrate from backdoor searches of Section 702 data to other methods.

## A. Section 702

### 1. Close the Backdoor Search Loophole

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

Section 702 surveillance also can result in the "incidental" collection of other types of sensitive data that do not receive full Fourth Amendment protection but that Congress has chosen to protect by statute. Depending on the information in question, the government ordinarily may be required to obtain a court order (e.g., under 18 U.S.C. §2703(d) or Section 215 of the U.S.A. Patriot Act[139]) or a subpoena (e.g., under §2703(c)(2) or with a National Security Letter) to obtain it. Before performing a U.S. person query of such data, agencies should be required to follow the legal process that would apply if the agencies were collecting the data in the first instance.

Importantly, this requirement should apply to all agencies that conduct U.S. person queries, not just the FBI, and it should apply regardless of whether the underlying investigation pertains to purely domestic criminal activity or to cases that involve a national security or foreign intelligence component. The Supreme Court has made clear that warrants are required to conduct surveillance in domestic national security investigations.[140] Moreover, even when an American is acting on behalf of a foreign entity and is engaged in international terrorism or other transnational crimes, FISA prohibits surveillance of that American unless the government obtains a FISA Title I order, which requires a showing of probable cause that the target is an agent of a foreign power.[141] Allowing the government to perform a U.S. person query of Section 702 data without that showing creates an end-run around the protections of the law.[142]

---

[139] Although Section 215 expired in 2020, it is still available for investigations commenced before the provision expired, as well as investigations into actions that took place before the expiration. *See* USA Patriot Act Improvement and Reauthorization Act, Pub. L. 109-177, 109th Cong. § 102(b)(2) (2005) (as amended by Pub. L. 116-69, 116th Cong. § 1703(a) (2019)).

[140] United States v. U.S. Dist. Court for E. Dist. of Mich. (Keith), 407 U.S. 297 (1972).

[141] 50 U.S.C. §1805.

[142] In addition, as noted above, there is no firmly established "foreign intelligence" exception that would justify warrantless U.S. person queries for foreign intelligence purposes. *See supra* note 52.

The government has stated that the FBI sometimes uses U.S. person queries to identify potential victims or targets of foreign cyberattacks, foreign influence campaigns, or foreign efforts to recruit spies, and that a warrant requirement would prevent the government from doing this. Indeed, the government has asserted that it performed 1.9 *million* warrantless U.S. person queries in 2021 for the purpose of identifying potential victims of foreign cyberattacks.[143] Notably, government officials did not mention this "defensive" practice when testifying before Congress during the 2017-2018 reauthorization of Section 702, despite the fact that backdoor searches were the subject of intense debate. This new justification raises more questions than it answers, given that the government has provided no public information about how this technique operates or its relative utility.[144]

In any event, the need to protect victims is hardly unique to the Section 702 context. Domestic law enforcement agencies are routinely faced with this task. They manage to keep the American public safe using investigative techniques that comport with the Fourth Amendment — including obtaining the consent and cooperation of potential victims themselves, or invoking the "exigent circumstances" exception to the warrant requirement in cases where victims are in imminent danger. There is no blanket "victim" exception to the Fourth Amendment, however; nor does the Constitution draw any distinction between "offensive" or "defensive" searches or seizures.

There is good reason for that. Whatever the *purpose* of the search, the *result* is to expose an American's personal information to manual review by an FBI agent, with all the potential for abuse such access entails. Indeed, the line between victim and suspect, particularly when it comes to foreign actors' efforts to recruit spies or exert influence, can be extremely murky. Throughout the FBI's darkest decades, the Bureau spied on anti-war protesters and racial justice activists, including Martin Luther King, Jr., on the ostensible grounds that they had been targeted and potentially infiltrated by foreign communists. Claims of potential foreign influence were also used to justify government monitoring of Muslim American communities after 9/11 and, more recently, the Movement for Black Lives and Antifa.[145]

---

[143] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 41, at 20.

[144] For instance, with respect to the use of backdoor searches to identify potential cyberattack victims in 2021, how did the FBI identify the 1.9 million U.S. persons in question? Of those 1.9 million queries, how many resulted in the identification of a potential victim and the implementation of successful evasive measures? Was there no probable cause to suspect malicious cyber activity in those cases?

[145] Martin Luther King, Jr. Research & Education Institute, Stanford University, *Federal Bureau of Investigation (FBI)* (accessed Jun. 16, 2023), https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi; SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT OF THE SENATE SELECT COMM. TO STUDY GOVERNMENT OPERATIONS: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 69-70 (1976); American Civil Liberties Union, *Factsheet: The NYPD Muslim Surveillance Program* (accessed Jun. 16, 2023), https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program; Micah Lee, *How Northern California's Police Intelligence Center Tracked Protests*, INTERCEPT (Aug. 17, 2020), https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters/; Devan Cole, *FBI director says bureau is looking into possible foreign influence in Floyd protests*, CNN (Jun. 24, 2020), https://www.cnn.com/2020/06/24/politics/christopher-wray-fbi-protests-foreign-influence/index.html; Sarah N. Lynch & Andy Sullivan, *Attorney General Barr says foreign groups, extremists stoking divisions in U.S. protests*, REUTERS (Jun. 4, 2020), https://www.reuters.com/article/uk-minneapolis-police-barr-idAFKBN23B35B.

The government is also attempting to ward off a warrant requirement by promising that the FBI's recent changes to its training, oversight, and data-access procedures will put an end to agents' "widespread violations" (as the FISA Court described them) of the FBI's court-approved rules for conducting U.S. person queries. As noted above, the FBI's own data suggest that violations are continuing to occur at a rate of over 8,000 per year, despite these changes. But even if the FBI could ensure perfect compliance, that would not obviate the need for a warrant. An agency's internal determination that a search of Fourth Amendment-protected data is reasonably likely to yield foreign intelligence or evidence of a crime is not the same as, and cannot substitute for, a showing of probable cause before a neutral magistrate. As the Supreme Court stated in a Fourth Amendment case where the government had argued that its protocols for searching cell phones were sufficient to protect Americans' privacy: "The founders did not fight a revolution to gain the right to government agency protocols."[146]

Finally, FBI officials have occasionally suggested that requiring a warrant or FISA Title I order for U.S. person queries would be tantamount to re-building "the wall."[147] This notion is utterly baseless. "The wall" refers to a set of pre-9/11 procedures that — in practice, if not on paper[148] — restricted intelligence officials' ability to share identified threat information with criminal prosecutors. The information in question was obtained under Title I of FISA, which means the government had *already* secured a probable-cause order at the point in the case where "the wall" kicked in.[149] Moreover, requiring a warrant for U.S. person queries would in no way inhibit the sharing of threat information — including information about Americans — that officials encountered in the course of querying and reviewing *foreigners'* communications. Any such discovery would be analogous to the "plain view" exception to the Fourth Amendment's warrant requirement.[150] What the Fourth Amendment cannot tolerate is the government collecting information without a warrant or Title I order with the intent of mining it for use against Americans.

Some government officials have questioned why FBI agents should be prohibited from using U.S. person queries when they could theoretically access the same information through the much less efficient process of reviewing each and every communication obtained under Section 702. The simple answer is that manual review of the tens of millions of Section 702-obtained communications residing in FBI databases — or even a relatively small fraction of those communications — would not just be inefficient; it would be impossible. The Supreme Court has made clear that where technology enables a privacy intrusion that would not be possible or practicable with more traditional techniques, the Fourth Amendment may be triggered. Thus, for

---

[146] Riley v. California, 573 U.S. 373, 398 (2014).
[147] *See* Christopher Wray, Dir., Federal Bureau of Investigation, *Defending the Values of FISA Section 702* (Oct. 13, 2017), https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702; Privacy & Civil Liberties Oversight Bd., *PCLOB Public Forum on FISA Section 702, supra* note 91, at 2:00:55 (comments of Mike Herrington, Senior Operations Advisor, FBI).
[148] *See* Barbara A. Grewe, Senior Counsel for Special Projects, Comm'n on Terrorist Attacks Upon the United States, *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations* (Aug. 20, 2004), https://irp.fas.org/eprint/wall.pdf.
[149] *See id.* at 29.
[150] For a discussion of the "plain view" exception, *see* Coolidge v. New Hampshire, 403 U.S. 443 (1971); Horton v. California, 496 U.S. 128 (1990).

instance, the government must obtain a warrant to attach a GPS device to a car for 28 days[151] or to obtain a week's worth of cell phone location information,[152] even though a police department could *theoretically* (but not realistically) obtain the same information without a warrant by deploying multiple police officers to follow the person in question twenty-four hours a day for days or weeks on end.

Recognizing the acute privacy and civil liberties concerns raised by U.S. person queries, President Obama's Review Group on Intelligence and Communications Technologies — a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) — unanimously recommended closing the "back door search" loophole by prohibiting searches for Americans' communications without a warrant.[153] Many in Congress have already embraced this approach. Senators Diane Feinstein, Mike Lee, Patrick Leahy, and Kamala Harris cosponsored an amendment requiring the government to obtain a probable-cause order for U.S. person queries the last time Section 702 was reauthorized,[154] although it didn't receive a vote. And the House has twice passed a similar amendment (in 2014[155] and 2015[156]) with both Democratic and Republican support.

### 2. Strengthen the Reverse-Targeting Prohibition and Minimization Requirements

In addition to ending the backdoor search loophole, Congress should shore up the provisions designed to minimize the collection, retention, sharing, and use of Americans' information. It should start by strengthening the bar on "reverse targeting." Currently, this provision states that the government may not conduct Section 702 surveillance if "the purpose" of the surveillance is to target a "particular, known" American. The clear intent behind this provision was to prohibit the use of Section 702 as a domestic spying tool. But Congress's wording would in theory allow the government to conduct Section 702 surveillance even if its *primary* purpose was to acquire a particular, known American's communications, as long as its secondary purpose was to target a foreigner abroad. The provision also could be construed to allow collection where the *sole* purpose was to acquire Americans' communications, as long as the government did not know those Americans' identity (i.e., they were not "known" Americans).

The warrantless collection of Americans' communications under Section 702 should truly be "incidental"; it should never be purposeful. Congress accordingly should tighten the language

---

[151] *See* United States v. Jones, 565 U.S. 400 (2012). Although the plurality opinion rested on the property intrusion caused by attaching the GPS device to the car, five justices concluded that the GPS tracking itself violated a reasonable expectation of privacy.
[152] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).
[153] *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 29 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[154] *See* S. Amdt. 1875, S. 139, 115th Cong. (2018).
[155] *See* H. Amdt. 935, H.R. 4870, 113th Cong. (2014).
[156] *See* H. Amdt. 503, H.R. 2685, 114th Cong. (2015).

of the reverse-targeting provision by prohibiting the use of Section 702 if "a purpose" of the collection is to "acquire the communications or information of U.S. persons."

Congress also should add specificity to its definition of "minimization." In the absence of objective statutory criteria, there has been a predictable steady slide toward wider sharing of raw data, greater access to the data by agency personnel, and more exceptions to retention limits. On retention in particular, Congress should clarify that keeping Americans' information for five years, and for even longer in cases where that information has been reviewed and no determination of its status has been made, is not "minimization." Congress should specify that all information not subject to a litigation hold must be destroyed within three years of the authorization for the acquisition, unless it has been reviewed and determined to be foreign intelligence or evidence of a crime.[157]

### 3. Prohibit "Abouts" Collection

Congress should codify the current cessation of "abouts" collection. This type of surveillance greatly increases the chances of pulling in wholly domestic communications, not to mention other completely innocent communications between people who are not themselves legitimate targets of surveillance. Moreover, although "abouts" collection poses uniquely significant risks to privacy, it was a relatively small part of the upstream program, which itself comprises less than one tenth of Section 702 collection.[158] This is clearly a situation in which the privacy risks outweigh the benefits — a point the NSA effectively acknowledged when it stopped "abouts" collection in April 2017.[159]

### 4. Narrow the Scope of Surveillance

Congress should narrow the scope of permissible Section 702 targets in a way that preserves the government's ability to address foreign threats to the nation, while reducing the volume of "incidental" collection of Americans' communications and increasing the likelihood of a U.S.-EU data-sharing agreement withstanding European courts' scrutiny. Congress can accomplish this task using one of three approaches — or, better yet, some combination of the three.

---

[157] In its review of the NSA's bulk collection program, the PCLOB concluded that the collected metadata began to lose its usefulness after three years. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 170 (2014), *available at* https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf. It seems likely that this would also be true for the data obtained under Section 702. Of course, information that has been reviewed and determined to constitute foreign intelligence information or evidence of a crime could be retained for longer periods.

[158] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).

[159] *See* Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities* (Apr. 28, 2017), *available at* https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml ("NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate 'about' communications from its upstream 702 collection without also excluding some of the relevant communications directly 'to or from' its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.").

The first approach consists of requiring the government to have a reasonable belief, based on specific and articulable facts, that the target of surveillance is a foreign power or an agent of a foreign power. These terms are broadly defined in FISA and give the government ample leeway to target a wide range of malign foreign actors. Moreover, the determination of whether a target is a foreign power or agent of a foreign power would be an internal one; it would not have to be submitted to the FISA Court for case-by-case approval or meet a "probable cause" standard. However, Congress should require the FISA Court to review a sample of targeting decisions as part of its annual approval process. (Indeed, Congress should impose this review requirement regardless of whether it creates new criteria for targeting.)

The second approach is to amend the definition of "foreign intelligence" information. The current definition has two parts. The first part encompasses any information about an extensive list of threats that may posed by foreign powers or agents of foreign powers, including actual or potential attacks, actual or potential "grave hostile acts," sabotage, international terrorism, proliferation of weapons of mass destruction, and clandestine intelligence activities.[160] The second part of the definition is a catch-all, extending to any information that "relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[161] As discussed above, the latter part of the definition is far too broad, enabling surveillance of everyday conversations about current events, and Congress should eliminate it. If the government can identify specific threats that would be excluded by such an approach, Congress can accommodate these concerns by adding those threats to the first part of the definition.

The third approach is to codify the legitimate objectives identified in President Biden's executive order (with a small number of revisions[162]) and prohibit the adoption of additional objectives without congressional authorization. Because purpose-based restrictions are difficult to enforce, however, Congress should translate the objectives into constraints on targeting. Specifically, Congress should require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to provide information that is directly relevant to one or more of the objectives. The statute should make clear that the absence of information cannot itself be deemed relevant for this purpose — i.e., it is not permissible to target groups or individuals simply to "rule them out" as sources of useful information.

---

[160] 50 U.S.C. § 1801(e)(1).

[161] 50 U.S.C. § 1801(e)(2).

[162] First, with respect to the goal of "understanding or assessing the capabilities, intentions, or activities of . . . a foreign-based political organization," Congress should interpret the term "foreign-based political organization" to exclude civil society non-governmental organizations. *See* Exec. Order 14086, *supra* note 60, at § 2(b)(i)(A)(1). Second, the goal of protecting against "transnational criminal threats" should apply only to serious crimes that significantly impact the lives, safety, or property of U.S. persons or the national security of the United States. Third, the goal protecting the integrity of U.S. "government property" should apply only where there is a threat of significant property damage involving a risk to the personal safety of persons on or near the property. See Elizabeth Goitein, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, JUST SEC. (Oct. 31, 2022), https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/.

## B. FISA

Section 702 is a part of FISA and is directly affected by many of FISA's other provisions, such as the mechanisms FISA establishes for judicial review of electronic surveillance and the geographic limitations on FISA's reach. Moreover, recent events have revealed serious problems with the operation of FISA Title I, a permanent authority that has no sunset. Congress should therefore address FISA more broadly in the course of enacting reforms to Section 702.

### 1. Remove Artificial Barriers to Judicial Review

Congress provided three different mechanisms by which courts could review electronic surveillance conducted under FISA. First, the FISA Court reviews applications to conduct electronic surveillance and engage in other types of collection of Americans' information; it also approves Section 702 certifications and procedures and conducts general oversight of that program. Second, Congress required the government to disclose any use of FISA-derived information in criminal prosecutions or other legal proceedings, thus enabling challenges by the non-government party. Third, Congress expressly provided for civil lawsuits to challenge unlawful surveillance under FISA.

None of these mechanisms is working as Congress intended. The FISA Court's effectiveness is hampered by one-sided proceedings and inaccurate government submissions. The government is evading its notice obligations to criminal defendants through "parallel construction." And civil litigation has been thwarted by misapplications of the standing and state secrets doctrines. Congress must amend the law to ensure that there is effective judicial review and accountability for violations of Section 702 and other FISA authorities.

#### a. Increase Adversariality and Improve Accuracy in FISA Court Proceedings

The secrecy and one-sided nature of FISA proceedings are inherently problematic. When judges hear only from one party and their decisions in favor of that party are never subject to appeal, there is a higher risk of skewed and erroneous decisions — as evidenced by the FISA Court's approval of the NSA's bulk collection program, which three regular federal courts have now ruled unlawful.[163]

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

At the same time, there has been a troubling pattern of the government presenting inaccurate or incomplete information to the FISA Court. In December 2019, a report from the

[163] United States v. Moalin, 973 F.3d 977 (9th Cir. 2020); American Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013).

Department of Justice Inspector General reviewed four FISA Title I surveillance applications submitted as part of the FBI's investigation into alleged Russian interference in the 2016 presidential election.[164] The report identified 17 separate errors or omissions in these applications. This prompted the Inspector General to review FISA Title I applications more broadly. Reviewing a sample of 29 applications, the Inspector General found that 25 of the 29 applications contained "apparent errors or inadequately supported facts";[165] for the remaining four applications, the FBI could not even locate the files containing the documentation on which the applications were ostensibly based. The FISA Court has broadly observed that the government "has exhibited a chronic tendency" to provide inaccurate, incomplete, or materially misleading information to the FISC in its filings.[166]

To address both these problems, Congress should enact the reforms to FISA Court proceedings set forth in the "Lee-Leahy" amendment — an amendment offered by Senators Mike Lee and Patrick Leahy to the USA FREEDOM Reauthorization Act of 2020.[167] Although Congress failed to pass the reauthorization bill, the amendment passed by an overwhelming bipartisan vote of 77-19.[168]

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

**b. End the Government's Use of "Parallel Construction" to Evade FISA's Notice Requirement**

The government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. Before 2013, the government interpreted "obtained or derived from" so narrowly that it notified no one. In the ten years since the government's approach reportedly changed,[169] the government has provided notification in fewer than ten known cases, even though the PCLOB reports that the FBI searches Section 702 every time it

---

[164] *See* OFF. INSPECTOR GENERAL, DEP'T OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (Dec. 2019), *available at* https://www.justice.gov/storage/120919-examination.pdf.

[165] *See* OFF. INSPECTOR GEN., DEP'T OF JUSTICE, MANAGEMENT ADVISORY MEMORANDUM FOR THE DIRECTOR OF THE FBI REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FISC RELATING TO U.S. PERSONS 3 (Mar. 2020), *available at* https://oig.justice.gov/sites/default/files/reports/a20047.pdf.

[166] [Redacted], No. [Redacted], at 13-14 (FISA Ct. [Date Redacted]), *available at* https://www.dni.gov/files/documents/icotr/51117/.

[167] S. Amdt. 1584, H.R. 6172, 116th Cong. (2020).

[168] *Id.* (as agreed to in Senate, May 13, 2020).

[169] For more background, see Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, JUST SEC. (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

conducts a national security investigation and there have been more than two thousand terrorism and national security convictions during this time.[170]

There is reason for concern that the government is avoiding its notification requirements by engaging in "parallel construction" — i.e., recreating the Section 702 evidence using less controversial means.[171] This is a well-documented practice that the government has used in a variety of settings, including foreign intelligence surveillance cases.[172] Attorneys have asked the Department of Justice to share its policies for determining when information is considered to be "derived from" Section 702, but the Department refuses to provide them.

Even though Congress clearly intended for defendants to be able to challenge the use of Section 702-derived evidence in criminal cases, the government's notification policies are thwarting this intent. Congress should clarify that evidence is "derived" from Section 702 surveillance if the government would not otherwise have possessed this evidence, regardless of any claim that the evidence is attenuated from the surveillance, would inevitably have been discovered, or was subsequently reobtained through other means. This definition will remove the government's ability to evade its notice obligations through parallel construction.

### c. Clarify Application of Standing and State Secrets Doctrines

Congress clearly intended for civil lawsuits to serve as a means to challenge electronic surveillance activities — indeed, Congress authorized the award of actual and punitive damages in such lawsuits.[173] Congress also was aware that much of the information at issue in such lawsuits — and any other legal proceedings involving evidence derived from FISA — would be classified. It therefore included a provision that carefully directs courts how to handle sensitive information in such cases. In short, if the government claims that the disclosure of information through litigation would harm national security, the court must review the information *in camera* and *ex parte* to determine whether the surveillance was lawful.[174]

---

[170] *See* Brief for the Brennan Ctr. for Justice et al. as Amicus Curiae at 23 n.23, *Wikimedia v. Nat'l Sec. Agency*, No. 22-190 (2022); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2022 at 14 (280 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2021 at 14 (133 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2020 at 14 (172 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2019 at 14 (181 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2018 at 14 (185 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2017 at 14 (196 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2016 at 14 (210 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14 (273 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 14 (265 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60 (290 guilty dispositions).

[171] *See* Toomey, *supra* note 169; John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans,* REUTERS (Aug. 5, 2013), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805#X7BeCQSb0GrEDTJX.97.

[172] *See* Human Rights Watch, *Dark Side: Secrets Origins of Evidence in US Criminal Trials* (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

[173] 50 U.S.C. §1810.

[174] 50 U.S.C. §1806(f).

Despite Congress's intent to permit civil litigation, civil lawsuits have consistently been derailed by the misapplication of two legal doctrines. First, courts have taken an overly rigid review of the standing doctrine, refusing to allow plaintiffs to bring lawsuits unless they can prove they have been surveilled.[175] Because FISA surveillance is always conducted in secret, even plaintiffs who have ample reason to suspect they have been surveilled generally require discovery to confirm these suspicions. The courts' interpretation of standing presents a Catch-22 in which plaintiffs cannot move to the discovery phase of litigation without providing the evidence that can only be acquired through discovery.

Second, the Supreme Court recently ruled that Congress, in establishing special procedures for the handling of sensitive information in FISA cases, did not intend to displace the operation of the state secrets privilege.[176] The Court's reasoning was that FISA's special procedures and the procedures courts currently use when the government claims the state secrets privilege are not incompatible — but that is clearly false. At the most basic level, some courts have interpreted the state secrets privilege to permit the dismissal of cases at the pleadings stage, which would not be permitted under the special FISA procedures.[177] As a result of the Court's ruling, the government can almost always avoid an adjudication on the merits of any civil lawsuit challenging unlawful surveillance.

Congress must take action to ensure that its intent to make civil litigation available is honored. To that end, Congress should specify that a person has standing to bring a civil lawsuit if she has a reasonable basis to believe her information has been (or will be) acquired, and if she has expended (or will expend) time or resources in an attempt to avoid acquisition. In addition, Congress should amend the provision that establishes special procedures for handling sensitive information in FISA cases to clarify that these procedures govern how courts should resolve any governmental claims of the state secrets privilege.

### 2. Complete the Modernization of FISA by Eliminating Obsolete Geographical Distinctions in the Protection of Americans' Communications

As a general matter, FISA applies when the government collects foreign intelligence inside the United States or from U.S.-based companies. (A significant exception to this rule is discussed in Part IV.C of this statement.) When the government collects foreign intelligence abroad, it usually relies on claims of inherent presidential authority, as regulated by Executive Order (EO) 12333 and related executive branch policies. The distinction has critical consequences; as explained further below, there are exceedingly few legislative protections for Americans' privacy when the government conducts surveillance under EO 12333, and such surveillance is not subject to any judicial oversight whatsoever.

---

[175] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
[176] FBI v. Fazaga, 142 S. Ct. 1051 (2022).
[177] *See* Elizabeth Goitein, *The State Secrets Sidestep:* Zubaydah *and* Fazaga *Offer Little Guidance on Core Questions of Accountability*, CATO S. CT. REV. 193 (2022), *available at* https://www.cato.org/sites/cato.org/files/2022-09/Supreme-Court-Review-2022-Chapter-8.pdf.

A geographic limitation on FISA's reach might have made some sense in 1978, when FISA was enacted. At the time, surveillance inside the United States generally meant surveillance of Americans and surveillance overseas generally meant surveillance of foreigners. To be sure, FISA did not restrict the government's ability to collect communications between foreigners and Americans when the surveillance took place overseas or was accomplished by satellite. Nonetheless, the volume of international communications in 1978 was exponentially smaller than it is today. Communications were generally ephemeral and had to be captured in transit; they did not rest in electronic storage for years or decades. And there were significant technological limitations on storing, processing, and analyzing data. These factors greatly limited overseas collection of Americans' international communications.[178]

As for purely domestic communications, they were transmitted almost entirely through wires inside the United States (and therefore covered by FISA). Today, communications are routinely routed and stored all over the world, in places far removed from the points of origin and receipt. Indeed, the fact that purely foreign communications were being handled by internet service providers inside the United States — which, under FISA as originally enacted, would have triggered the requirement to obtain a probable-cause order — is one of the main reasons the government sought to "modernize" FISA in 2008 through the enactment of Section 702.[179]

But Section 702 failed to address the other half of this problem: the fact that purely domestic communications and other personal data are routinely routed and stored abroad, which can in some cases remove them from FISA's protections and expose them to EO 12333 surveillance. Congress did extend FISA to cover the intentional targeting of Americans who are themselves located overseas,[180] and EO 12333 policies generally prohibit targeting Americans or intentionally collecting domestic communications.[181] These limits, however, are subject to various caveats and exceptions. Moreover, they have little practical effect when the government

---

[178] *See* ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT 19–21 (Brennan Ctr. for Justice 2015), https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court.

[179] *See* Ex Parte Brief for Respondents at 8-9, *In re* Directives to Yahoo Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (FISA Ct. Rev. 2008), *available at* https://cdt.org/wp-content/uploads/2014/09/2-yahoo702-governments-ex-parte-merits-brief.pdf (noting that when the government obtains stored emails from an internet service provider, this acquisition is covered by the fourth prong of the definition of "electronic surveillance," which applies to collection inside the United States regardless of the U.S. person status of the communicants). The government also argued that technological changes restricted its ability to collect foreigners' communications with Americans in a way that undermined Congress's original intent in passing FISA. As I explained in congressional testimony in 2017, this reading of Congress's original intent is incorrect. *See The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties, Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 2–3n.4 (Jun. 27, 2017) (testimony of Elizabeth Goitein, Co-Dir., Liberty & Nat'l Sec. Program, Brennan Ctr. for Justice), *available at* https://www.judiciary.senate.gov/imo/media/doc/06-27-17%20Goitein%20Testimony.pdf.

[180] 50 U.S.C. §1881c.

[181] DEP'T OF DEFENSE, DOD MANUAL S-5240.01-A, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES: ANNEX GOVERNING SIGNALS INTELLIGENCE INFORMATION AND DATA COLLECTED PURSUANT TO SECTION 1.7(C) OF E.O. 12333 at 2.2.a, 2.4.a (Jan. 7, 2021), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/S-524001-A.PDF?ver=SPh6FZicXc8uH192MI8o3w%3D%3D&timestamp=1610651794685.

engages in bulk collection — a dragnet approach in which the government does not identify particular targets. Bulk collection is prohibited under FISA, but it is permitted under EO 12333.

In February 2022, through the efforts of Senators Ron Wyden and Martin Heinrich, Americans learned that the CIA has for years been conducting bulk collection programs under EO 12333 that pull in Americans' data.[182] One set of activities includes the bulk acquisition of information about financial transactions involving Americans and others.[183] Another program collects an unspecified type of data, but the CIA's sparse public statements on the program suggest that it impacts "Americans who are in contact with foreign nationals,"[184] which implies that it involves communications records. A document partially declassified by the CIA shows that CIA analysts query the data acquired under this program for information about U.S. persons, and that they do so without recording the justification for the queries[185] — making it virtually impossible to conduct even internal oversight.

Even when EO 12333 surveillance is targeted at specific foreigners (rather than used to conduct bulk collection), it results in the "incidental" collection of Americans' communications, just as Section 702 does. Yet protections for this data are left entirely to executive branch policies, with no judicial review to ensure that these policies comport with the Constitution—or that agencies' practices comport with the policies. Inadequate as the protections of Section 702 are, the protections agencies have adopted under EO 12333 are even weaker.[186]

---

[182] *See* Charlie Savage, *C.I.A. Is Collecting In Bulk Certain Data Affecting Amendments, Senators Warn* N.Y. TIMES (Feb. 10, 2022), https://www.nytimes.com/2022/02/10/us/politics/cia-data-privacy.html.

[183] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON CIA FINANCIAL DATA ACTIVITIES IN SUPPORT ON ISIL-RELATED COUNTERTERRORISM EFFORTS (accessed Jun. 16, 2023), *available at* https://www.cia.gov/static/63f697addbbd30a4d64432ff28bbc6d6/OPCL-PCLOB-Report-on-CIA-Activities.pdf.

[184] Katie Bo Lillis, *Senators allege CIA collected data on Americans in warrantless searches*, CNN (Feb. 11, 2022), https://www.cnn.com/2022/02/10/politics/cia-data-collection-americans/index.html.

[185] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., RECOMMENDATIONS FROM PCLOB STAFF (accessed Jun. 16, 2023), *available at* https://www.cia.gov/static/f61ca00cbcda9b5d46a04e0b53b5f2b9/OPCL-Recommendations-from-PCLOB-Staff.pdf.

[186] For instance, the CIA's EO 12333 procedures allow it to run U.S. person queries for any information "related to a duly authorized activity of the CIA"— a much broader standard than that contained in the agency's Section 702 querying procedures, under which queries "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA." *Compare* CENTRAL INTELLIGENCE AGENCY, THE CIA'S UPDATED EXECUTIVE ORDER 12333 ATTORNEY GENERAL GUIDELINES 6 (accessed Jun. 12, 2023), *available at* https://www.cia.gov/static/100ea2eab2f739cab617eb40f98fac85/Detailed-Overview-CIA-AG-Guidelines.pdf *with* WILLIAM BARR, U.S. DEP'T OF JUSTICE, QUERYING PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § IV.A (Sept. 16, 2019), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_CIA_Querying_Procedures.pdf. The distinction is even more stark when it comes to U.S. person queries by the FBI. For Section 702 data, such queries "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime." LISA O. MONACO, DEPUTY ATT'Y GEN., U.S. DEP'T OF JUSTICE, QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § IV.A.1 (Oct. 14, 2021), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_FBI_Querying_Procedures.pdf. For data obtained under EO 12333, there are no specific restrictions on querying. Rather, under the Attorney General's Guidelines for Domestic FBI Operations, there is simply a general admonition that "[a]ll activities under

There is no justification for giving lesser protections to Americans' constitutional rights based simply on the accident of where our digital data happens to travel. If anything, the privacy implications of EO 12333 for Americans are likely even greater than those of Section 702. The government has acknowledged that the majority of its foreign intelligence surveillance activities take place under EO 12333.[187] Accordingly, it reasonable to expect that there is more "incidental" collection of Americans' information under EO 12333 than under Section 702, even when such surveillance is targeted. And, of course, bulk collection has the potential to sweep in Americans' data in amounts that far exceed what normally occurs during targeted surveillance.

To complete the modernization of FISA that began with Section 702, Congress should extend basic protections to Americans' communications and other Fourth Amendment-protected information, regardless of where they are obtained. If it fails to do so, any reforms to Section 702 will have limited effect, as the government will be able to obtain at least some of the same information — with more effort, to be sure, but with far fewer protections for Americans' privacy — entirely outside the FISA framework. At a minimum, Congress should enact measures that:

- Prohibit the targeting of Americans under EO 12333.
- Require the government to minimize the retention, sharing, and use of Americans' information that is "incidentally" acquired under EO 12333.[188]
- Close the EO 12333 backdoor search loophole by requiring the government to obtain a warrant or FISA Title I order before conducing U.S. person queries of the data.
- Reduce the scope of "incidental" collection of Americans' information by codifying a modified version the legitimate objectives for surveillance set forth in President Biden's recent executive order,[189] and requiring the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to produce information directly relevant to one or more objectives.
- Ensure the availability of judicial oversight by requiring the government to inform criminal defendants when using evidence obtained or derived from EO 12333 surveillance.

In addition to these measures, Congress should prohibit bulk collection, or at least tightly limit its availability — e.g., to geographic areas of active or impending hostilities. Bulk collection poses unique risks to Americans' privacy, not to mention the privacy of countless foreign nationals who pose no threat whatsoever to the United States. It is also one reason why European courts have struck down the U.S.-EU agreements that allow EU companies to share

---

these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines." U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 13 (accessed Jun. 12, 2023), *available at* https://www.justice.gov/archive/opa/docs/guidelines.pdf.

[187] Nat'l Sec. Agency, *Legal Fact Sheet: Executive Order 12333* (Jun. 19, 2013), *available at* https://www.aclu.org/sites/default/files/field_document/Legal%20Fact%20Sheet%20Executive%20Order%12333_0.pdf.

[188] One of the few statutory limits on EO 12333 surveillance is a requirement to delete any unencrypted U.S. person information after 5 years if it does not constitute foreign intelligence or evidence of a crime; however, there is a broad "national security" exception that greatly weakens the force of this provision. *See* 50 U.S.C. §1813.

[189] *See supra note* 162.

customer data with U.S. companies. And the government has never demonstrated the necessity for this highly problematic practice. To the contrary, even though Section 702 has a targeting requirement (i.e., it does not permit bulk collection), intelligence officials have described it as the most effective foreign intelligence surveillance tool in its arsenal;[190] the government has never suggested that the targeting requirement makes Section 702 less effective or results in the loss of vital intelligence.

In implementing these changes, Congress need not call into question the president's constitutional authority to conduct surveillance of foreigners abroad. But where such surveillance extends beyond foreigners and sweeps in the Fourth Amendment-protected information of Americans, there can be no question regarding the necessity and appropriateness of legislative and judicial involvement. As the Supreme Court has made clear, the Constitution "most assuredly envisions a role for all three branches [of government] when individual liberties are at stake."[191]

### C. Close Other Statutory Gaps and Update the Law to Prevent Warrantless Surveillance of Americans

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

Moreover, the problem at the heart of Section 702 in its current form — namely, the government's ability to access Americans' most personal information in ways that undermine statutory and constitutional protections — is present across a range of surveillance authorities and activities today. Yet very few of these authorities or activities are subject to a sunset. Congress would thus be wise to use the scheduled expiration of Section 702 to address other manifestations of the same core problem.

#### 1. Prohibit the Government from Buying Its Way Around FISA and Other Statutory Limits on Surveillance

FISA includes an "exclusivity" provision, which provides that FISA, along with various criminal law provisions authorizing electronic surveillance, "shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic

---

[190] *See, e.g.*, Matthew G. Olsen, Ass't Att'y Gen., Dep't of Justice, *Remarks at Brookings Institution on Section 702* (Feb. 28, 2023), https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-g-olsen-delivers-remarks-brookings-institution-section ("In the 15 years since enactment, Section 702 has become the Intelligence Community's most valuable national security legal tool.").

[191] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

communications may be conducted."[192] FISA's highly technical definition of "electronic surveillance,"[193] however, does not cover the collection of many types of records containing communications metadata and other sensitive non-contents information, such as geolocation data. The government can thus claim that certain provisions of FISA — including Section 702 itself, to the extent it authorizes collection activities that do not qualify as "electronic surveillance," as well as the provisions governing physical searches and the collection of some third-party records — are *not* the exclusive means by which such activities may be conducted, and that the government may ignore the restrictions and procedures contained in such provisions.

There's ample reason to believe that's happening now. In 2020, Congress was debating whether to reauthorize Section 215, the so-called "business records" provision of FISA that the NSA relied on to collect Americans' phone records in bulk. Senator Richard Burr — who then chaired the Senate Select Committee on Intelligence — warned that if Section 215 expired, "the president under 12333 authority can do all of this without Congress's permission, with no guardrails."[194] The authority indeed expired (although pending investigations were grandfathered), and the conspicuous absence of any serious government efforts to reinstate it strongly suggests that the government is obtaining the same information through other means.

That's alarming, because the information that the government may obtain under Section 215 and other provisions of FISA not fully covered by the exclusivity provision can be extremely sensitive. Take the phone records that were the subject of the NSA's bulk collection program. After Edward Snowden's disclosure of the program, experts explained how communications "metadata" — a term many Americans had never encountered — could be crunched to reveal people's associations, activities, and even beliefs.[195] Geolocation information can similarly reveal the most intimate aspects of people's private lives. Indeed, for that very reason, the Supreme Court in *Carpenter v. United States* (2018) held that police need a warrant to obtain a week's worth of geolocation information from a cell phone company.[196]

If the government wanted to obtain such information without adhering to FISA, one workaround would be to purchase it from data brokers. This appears to be an increasingly common practice among federal agencies. In one particularly disturbing example, Vice News reported that "[m]ultiple branches of the U.S. military have bought access to a powerful internet monitoring tool that claims to cover over 90 percent of the world's internet traffic, and which in some cases provides access to people's email data, browsing history, and other information such as their sensitive internet cookies."[197] In addition, multiple agencies have reportedly purchased access to Americans' cell phone location information, including the Federal Bureau of

---

[192] 50 U.S.C. §1812.
[193] 50 U.S.C. §1801(f).
[194] *See Sen. Burr claims EO 12333 permits mass surveillance "without Congress's permission"*, C-SPAN (Mar. 12, 2020), 00:18, https://www.c-span.org/video/?c4860932/user-clip-sen-burr-claims-eo-12333-permits-mass-surveillance-without-congresss-permission.
[195] Declaration of Professor Edward W. Felten at 16, American Civil Liberties Union v. Clapper, 785 F.Supp.2d 724 (S.D.N.Y. 2013), *available at* https://s3.documentcloud.org/documents/781486/declaration-felten.pdf.
[196] 138 S. Ct. 2206 (2018).
[197] Joseph Cox, *U.S. Military Bought Mass Monitoring Tool that Includes Internet Browsing, Email Data*, VICE (Sept. 21, 2021), https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data.

Investigation[198] (as recently confirmed by FBI Director Chris Wray[199]), the Drug Enforcement Administration,[200] multiple components of the Department of Homeland Security (including Immigration and Customs Enforcement[201] and Customs and Border Protection[202]), the Secret Service,[203] and the Department of Defense.[204] Even the Internal Revenue Service, according to the Wall Street Journal, "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."[205]

This warrantless collection of Americans' cell phone location information — potentially in massive amounts — would seem to violate the Supreme Court's holding in *Carpenter*. But agency lawyers have found a way around the case law. They have construed *Carpenter* to apply only when the government *compels* companies to disclose location information.[206] When the government merely *incentivizes* such disclosure — by writing a big check — the warrant requirement simply disappears. At that point, the argument goes, the government may obtain this Fourth Amendment-protected information in unlimited quantities without any individualized suspicion of wrongdoing, let alone probable cause and a warrant. This is legal sophistry, but it could take years for the courts to resolve the issue. In the meantime, the government has effectively sidelined the Fourth Amendment when it comes to data purchases.

Another apparent barrier to these purchases — the Electronic Communications Privacy Act (ECPA) — has also proven inadequate. ECPA prohibits phone and Internet companies from disclosing customer records to government agencies unless the government produces a warrant, court order, or subpoena.[207] But it includes broad exemptions for foreign intelligence surveillance.[208] Moreover, the law is woefully outdated. It does not cover digital data brokers or

---

[198] *See* Sara Morrison, *A surprising number of government agencies buy cellphone data records. Lawmakers want to know why*, VOX (Dec. 2, 2020), https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.

[199] *See* Ashley Belanger, *FBI finally admits to buying location data on Americans, horrifying experts*, ARS TECHNICA (Mar. 9, 2023), https://arstechnica.com/tech-policy/2023/03/fbi-finally-admits-to-buying-location-data-on-americans-horrifying-experts/.

[200] *See* Morrison, *supra* note 198.

[201] *See* Paul Blest, *ICE Is Using Location Data From Games and Apps to Track and Arrest Immigrants, Report Says*, VICE, (Feb. 7, 2020), https://www.vice.com/en/article/v7479m/ice-is-using-location-data-from-games-and-apps-to-track-and-arrest-immigrants-report-says.

[202] *See* Blest, *supra* note 201.

[203] *See* Joseph Cox, *Secret Service Bought Phone Location Data from Apps, Contract Confirms*, MOTHERBOARD (VICE) (Aug. 17, 2020), https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.

[204] *See* Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 22, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

[205] Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J. (Jun. 19, 2020), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815. Although more is known about the practice at the federal level, state and local law enforcement also have been caught buying information about social media users from data vendors. *See* Kristina Cooke, *U.S. police used Facebook, Twitter data to track protestors: ACLU*, REUTERS (Oct. 11, 2016), https://www.reuters.com/article/us-social-media-data-idUSKCN12B2L7.

[206] *See* Savage, *Intelligence Analysts*, *supra* note 204; Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People*, BUZZFEED NEWS (Oct. 30, 2020), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[207] 18 U.S.C. § 2702.

[208] 50 U.S.C. § 2511(2)(a)(ii), (e), & (f).

many app developers, for the simple reason that they did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections. Companies that are prohibited from selling their data to the government can simply sell it to a data broker — a disturbingly common practice[209] — and the data broker can resell the same information to the government, at a handsome profit. The information is effectively laundered through a middleman.

These combined gaps — in FISA, in the government's reading of Fourth Amendment case law, and in ECPA — leave the government free to collect some of the most sensitive information Americans generate, and to do so inside or outside the United States, without statutory authorization or judicial oversight. That is presumably how the CIA came to operate a bulk collection program that pulls in Americans' data, to be retrieved through backdoor searches and used for unknown purposes.

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

But Congress should go further and use the opportunity presented by the Section 702 sunset to close the data broker loophole completely — i.e., not just for foreign intelligence investigations. Congress should make clear that the government may not purchase Americans' personal information if compelled disclosure of that information would require a warrant, court order, or subpoena. The Fourth Amendment Is Not For Sale Act,[210] a bill introduced in the last Congress by Senators Ron Wyden and Rand Paul and by Representatives Jerrold Nadler and Zoe Lofgren, would go a long way toward accomplishing this goal.[211]

### 2. Update the Law to Reflect the Supreme Court's Decision in *Carpenter v. United States*

Since 1967, the Fourth Amendment has been understood to apply whenever the government intrudes on a "reasonable expectation of privacy."[212] For decades, however, the protections that flowed from this analysis were artificially constrained by the "third-party doctrine." First articulated in *United States v. Miller* (1976)[213] and reiterated in *Smith v.*

---

[209] In 2020, for example, Federal Communications Commission Chairman Ajit Pai proposed fines totaling $208 million after major mobile phone carriers like T-Mobile, Verizon, and Sprint were caught selling their consumers' real-time location data to data brokers without their knowledge or consent. *See* Jon Brodkin, *Senate Bill Would Ban Data Brokers from Selling Location and Health Data*, ARS TECHNICA (Jun. 15, 2022), https://arstechnica.com/tech-policy/2022/06/senate-bill-would-ban-data-brokers-from-selling-location-and-health-data/.
[210] H.R. 2738, 117th Cong. (2021); S. 1265, 117th Cong. (2021).
[211] *See* Elizabeth Goitein, *The government can't seize your digital data. Except by buying it.*, WASH. PO. (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.
[212] *See* Katz v. United States, 389 U.S. 347 (1967).
[213] 425 U.S. 435 (1976).

*Maryland* (1978),[214] the doctrine holds that a person loses any expectation of privacy in information that he or she voluntarily discloses to another — no matter how limited or necessary the disclosure.

Arguably, this doctrine never made much sense. Most of us do not understand "private" to mean "secret"; we don't assume that information is private only if we never share it with another living soul. Rather, we understand privacy to be about controlling when and with whom we share information. The fact that a person might choose to confide in a spouse, relative, or even a group of trusted friends does not mean that she wants or expects the information to be widely available to the public.

Nonetheless, whatever sense the third-party doctrine might have made in the 1970s when it was established, it is wholly untenable today. Documents once stored in a desk at home are now frequently backed up to the cloud, accessible to the cloud service provider. Letters once sealed against inspection by the U.S. Post Office have become texts or emails, sent and stored by the companies that provide those services. Searches through card catalogues in the local library have turned into internet searches, generating search and web browsing records stored by internet service providers. And while it was once possible to pay a private visit, our cell phones — and therefore, our cell phone service providers — know where we are at all times, whether we are visiting a public park, a therapist, or Alcoholics Anonymous. In short, it is effectively impossible to go 24 hours without disclosing highly sensitive information to the multitude of third parties that manage life in the digital world.

The Supreme Court has begun the long process of bringing the Fourth Amendment in line with these new realities. In 2018, in *Carpenter v. United States*,[215] the Court held that police officers need a warrant to compel cell phone companies to turn over historical cell site information for a seven-day period. The Court concluded that individuals retain a reasonable expectation of privacy in that information despite "sharing" it with a third party (their cell phone companies). Its reasoning was essentially twofold. First, comprehensive geolocation information, unlike the items of information at issue in *Miller* (bank deposit slips) and *Smith* (phone numbers transmitted over a particular line), can reveal the most intimate details of a person's associations and activities — what the Court referred to as "the privacies of life."[216] Second, disclosure of one's location though the use of a cell phone cannot fairly be described as "voluntary," given that the only alternative is to forego cell phone use and — along with it — participation in modern life.

Unfortunately, the holding in *Carpenter* is limited to the facts of that case. The Court expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party. There is no way to predict when cases involving other instances of third-party collection might come before the Court. We might well have to wait many years to discover how the Court will apply the principles articulated in *Carpenter* to comprehensive communications metadata, internet search and web browsing

---

[214] 442 U.S. 735 (1979).
[215] 138 S. Ct. 2206 (2018).
[216] *Carpenter*, 138 S. Ct. 2210 (quoting Riley v. California, 573 U.S. 373, 403 (2014) (internal quotation marks omitted)).

histories, DNA analyses, and multiple other categories of highly sensitive data. The Court also refrained from opining on whether warrants would be required to obtain cell site location information in national security or foreign intelligence investigations. To the extent this data collection takes place under Executive Order 12333, courts might never have the opportunity to weigh in on this question.

Americans' Fourth Amendment rights should not hang in the balance for years or longer while each use-case scenario wends its way through the courts. When the Supreme Court held in 1967 that the government needed a warrant to wiretap calls made from a phone booth, Congress moved swiftly to codify the principles articulated in that decision through Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[217] Congress should take similar action now, using the principles set forth in *Carpenter* to identify additional categories of highly sensitive information that merit the protection of a warrant regardless of whether they are held by third parties. In addition to communications content and geolocation data, those categories should include:

- *Communications metadata*. As noted above, accumulated communications metadata can reveal intimate associations, habits, and even beliefs; indeed, it can be every bit as revealing as communications content.
- *Internet search and web browsing records*. These records can provide a window into the most private thoughts of Internet users. In 2020, the Senate voted 59-37 in favor of a bipartisan amendment offered by Senators Steve Daines and Ron Wyden that would have imposed a warrant requirement for such records.[218]
- *Biometric information*. Governmental access to biometric information (including fingerprints, retinal scans, DNA, etc.) carries extreme risks to privacy and associational rights, and has become a tool of persecution in countries like China and Iran.[219]

---

[217] Pub. L. 90-351 (1968) (codified at 34 U.S.C. § 10101 *et seq.*).

[218] *See* Niels Lesniewski, *Senate amends surveillance bill to add new oversight*, ROLL CALL (May 13, 2020), https://rollcall.com/2020/05/13/senate-may-have-the-votes-to-limit-surveillance-of-browser-history/.

[219] Isabelle Qian et al., *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*, N.Y. TIMES (updated Jul. 26, 2022), https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html; Charlie Campbell, *'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World*, TIME (Nov. 21, 2019), https://time.com/5735411/china-surveillance-privacy-issues/; STEVEN FELDSTEIN, THE GLOBAL EXPANSION OF AI SURVEILLANCE (Carnegie Endowment for Int'l Peace 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847; Frank Hersey, *Surveillance states: life in the facial recognition spotlight in China, Iran, and India*, BIOMETRIC UPDATE (Jan. 12, 2023), https://www.biometricupdate.com/202301/surveillance-states-life-in-the-facial-recognition-spotlight-in-china-iran-and-india; Shrutika Gandhi, *Biometric Identity Cards, Surveillance and Discrimination of Religious Minorities in Iran*, IRAN PRESS WATCH (Mar. 24, 2021), https://iranpresswatch.org/post/22195/biometric-identity-cards-surveillance-discrimination-religious-minorities-iran/. Facial recognition technology is even more problematic, given its inaccuracy when used to identify women and persons of color. *See* Steve Lohr, *Facial Recognition Is Accurate, if You're a White* Guy, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html. For that reason, many advocates and lawmakers have called for a moratorium or even a total ban on the use of this technology. *See* Facial Recognition and Biometric Technology Moratorium Act of 2021, H.R. 3907, 117th Cong. (2021); S. 2052, 117th Cong. (2021); American Civil Liberties Union, *Coalition Letter Calling for a Federal Moratorium on Face Recognition* (Jun. 3, 2019), https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition.

- *Health information*. Records pertaining to an individual's mental and physical health are among the most sensitive records that we entrust to third parties, and we reasonably expect the contents of those records to remain private.

In short, there is no reason why Americans' privacy should be held hostage to the slow pace of litigation. Congress should fill in the contours of the picture the Supreme Court began to paint in *Carpenter*, applying the principles the Court set forth to create statutory warrant protections where they are most clearly needed.

**Conclusion**

Since Section 702 was last reauthorized, it has become increasingly apparent that its impact on Americans is anything but "incidental." Intelligence agencies are leveraging this authority on a systemic basis to gain warrantless access to Americans' communications and other personal information in ways that circumvent FISA and the Constitution and violate court-ordered policies. At the same time, anachronistic limitations on FISA's reach and other gaps in the law are rendering Americans' personal information vulnerable to warrantless surveillance outside of any statutory framework and without judicial oversight. With the scheduled expiration of Section 702 this year, Congress has the opportunity — and the responsibility — to bring the law in line with Americans' constitutional rights and legitimate privacy expectations.



