OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

WEDNESDAY, SEPTEMBER 18, 2019

Serial No. 116–47

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PUBLISHING OFFICE
44–884 WASHINGTON : 2021

COMMITTEE ON THE JUDICIARY

JERROLD NADLER, New York, *Chair*
MARY GAY SCANLON, Pennsylvania, *Vice-Chair*

ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
THEODORE E. DEUTCH, Florida
KAREN BASS, California
CEDRIC L. RICHMOND, Louisiana
HAKEEM S. JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
ERIC SWALWELL, California
TED LIEU, California
JAMIE RASKIN, Maryland
PRAMILA JAYAPAL, Washington
VAL BUTLER DEMINGS, Florida
J. LUIS CORREA, California
SYLVIA R. GARCIA, Texas
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
GREG STANTON, Arizona
MADELEINE DEAN, Pennsylvania
DEBBIE MUCARSEL-POWELL, Florida
VERONICA ESCOBAR, Texas

DOUG COLLINS, Georgia, *Ranking Member*
F. JAMES SENSENBRENNER, JR., Wisconsin
STEVE CHABOT, Ohio
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
KEN BUCK, Colorado
MARTHA ROBY, Alabama
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
DEBBIE LESKO, Arizona
GUY RESCHENTHALER, Pennsylvania
BEN CLINE, Virginia
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

PERRY APELBAUM, *Majority Staff Director & Chief of Staff*
BRENDAN BELAIR, *Minority Staff Director*

C O N T E N T S

WEDNESDAY, SEPTEMBER 18, 2019

OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Wednesday, September 18, 2019

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY
Washington, DC

The Committee met, pursuant to call, at 10:13 a.m., in Room 2141, Rayburn House Office Building, Hon. Jerrold Nadler [chairman of the committee] presiding.

Present: Representatives Nadler, Lofgren, Jackson Lee, Cohen, Johnson of Georgia, Cicilline, Lieu, Raskin, Jayapal, Demings, Correa, Scanlon, Garcia, Stanton, Escobar, Collins, Chabot, Gohmert, Jordan, Buck, Ratcliffe, Roby, Gaetz, Johnson of Louisiana, Biggs, Lesko, Reschenthaler, Cline, Armstrong, and Steube.

Staff Present: Aaron Hiller, Deputy Chief Counsel; Arya Hariharan, Deputy Chief Oversight Counsel; David Greengrass, Senior Counsel; John Doty, Senior Adviser; Madeline Strasser, Chief Clerk; Moh Sharma, Member Services and Outreach Adviser; Susan Jensen, Parliamentarian/Senior Counsel; Sarah Istel, Oversight Counsel; Julian Gerson, Staff Assistant; Priyanka Mara, Professional Staff Member; Sophie Brill, Counsel; Brendan Belair, Minority Staff Director; Bobby Parmiter, Minority Deputy Staff Director/Chief Counsel; Jon Ferro, Minority Parliamentarian/General Counsel; Ryan Breitenbach, Minority Chief Counsel, National Security; and Erica Barker, Minority Chief Legislative Clerk.

Chairman NADLER. The House Committee on the Judiciary will come to order.

Without objection, the chair is authorized to declare recesses of the Committee at any time.

We welcome everyone to this morning's hearing on Oversight of the Foreign Intelligence Surveillance Act. I will now recognize myself for an opening statement.

The Judiciary Committee is holding today's hearing to carry out one of its most important tasks, to ensure that the tools used by our Government to keep us safe are consistent with our values and with the freedoms guaranteed by the Constitution. This Committee has long exercised its responsibility to shape the legal framework under which intelligence and law enforcement agencies investigate threats and collect evidence of crimes.

Although we do not conduct day-to-day oversight of intelligence agencies, it falls to us in hearings like this to conduct a broad re-

view of how our Government exercises its legal authorities and whether that conduct accords with our values as Americans.

At the outset, I want to acknowledge two things. First, the men and women in our Nation's law enforcement and intelligence communities, including our witnesses today, work tirelessly to keep us safe from attacks and other threats by hostile adversaries. Those efforts include working rigorously to comply with our laws.

Second, there are countless Americans in the privacy and civil liberties communities who are dedicated to keeping us safe from other kinds of threats—threats to privacy, freedom of speech, and due process—that take hold when the Government's surveillance authorities extend too far.

Those who criticize and question the laws we will be discussing today are part of this Nation's proud and robust tradition of holding our Government to account, questioning the Government's reasons for its actions and jealously safeguarding the freedoms guaranteed to us by the Constitution. It is in that spirit that I hope to have a serious and substantive discussion today about the Foreign Intelligence Surveillance Act, or FISA, and the provisions that are set to expire at the end of this year.

In response to substantial concerns that the intelligence community had exceeded its authority under FISA, Congress, in 2015, enacted the USA FREEDOM Act, which contained several important reforms. Notably, we put an end to the NSA's program under which it collected the phone records of millions of law-abiding Americans using a highly strained interpretation of a provision in the 2001 USA PATRIOT Act.

We reformed that provision, known as section 215, to prohibit both the collection of phone records and other types of records. Instead, to collect certain kinds of phone records, we required the NSA to apply to the FISA court for an order based on individualized facts and on a specific selection term.

We also created an important mechanism to ensure that the FISA court hears both sides of the legal arguments in cases presenting novel and important issues. And we enacted several measures to enhance transparency in the FISA court and in other types of reporting.

At the end of this year, section 215 and two other FISA authorities, known as the "roving wiretap provision" and the "lone wolf provision," are set to expire unless they are reauthorized by Congress. Because these three provisions give the Government powerful and controversial intelligence authorities, Congress attached them to sunsetting provisions when they were first enacted and has reauthorized them for limited periods of time ever since.

These periodic reauthorizations provide this Committee and other committees an important opportunity to review how these laws are used and to conduct the kind of oversight that we are doing here today. Last month, however, former Director of National Intelligence Daniel Coats sent a letter to the leadership of this Committee and other committees in the House and Senate asking that we reauthorize all three provisions permanently.

At the same time, former Director Coats' letter acknowledged that the NSA has dismantled the call records program that it had been conducting under section 215, as amended by the USA FREE-

DOM Act. Simply put, the NSA dismantled the program because it was a serious failure.

The NSA used it to collect hundreds of millions of phone records, but in 2018, it discovered that it had no authority to collect some of the records it was receiving. Worse, it had no way of separating out which records were wrongly acquired from the ones that were collected lawfully. So, it started deleting them all. This has all been publicly reported by the intelligence community.

To be clear, it is not a bad thing that the NSA identified a problem, told us about it, and tried to fix it. It is also fine that they decided the program was not worth running. As former Director Coats put it, the decision to end the program was made after balancing its "relative intelligence value," which was evidently minimal, against "compliance and data integrity concerns."

The NSA decided that the costs outweighed the benefits, and it pulled the plug. That kind of candor should be applauded. It is baffling to me that the Administration announced that it had shuttered the program and then, in the very same breath, asked Congress to extend it permanently.

The Administration has offered almost no reason for this striking position, except the vague suggestion that we might need the program sometime in the future as technology changes and as our adversaries' capabilities evolve and adapt.

When Congress enacted the USA FREEDOM Act, we made a good faith effort to give the intelligence community the capability that it said it needed to collect call records. That experiment has run its course. If the Administration really wants to keep this provision on the books, it is going to have to justify it with more than a vague promise that it might come in handy one day in the future somehow.

I look forward to discussing the other authorities that are set to sunset, including aspects of section 215 and FISA's roving wiretap and lone wolf provisions. I also look forward to discussing, as well, the important reforms that we enacted in the USA FREEDOM Act and whether any of those reforms should be strengthened.

As I noted earlier, this Committee has an important and long-running responsibility to have these candid and rigorous discussions as we consider how best to ensure that our laws are in line with our values.

I thank today's witnesses for being here today and for their service to our Nation.

I now recognize the Ranking Member of the Judiciary Committee, the gentleman from Georgia, Mr. Collins, for his opening statement.

Mr. COLLINS. Last week, we once again commemorated the lives of all the innocent victims lost on 9/11, the brave first responders, and dedicated recovery workers. The 9/11 anniversary reminds us each year of the shock, sadness, and anger we all felt that morning.

Our unity and strength following the attacks were palpable and encouraging also. Nothing the terrorists inflicted could defeat our Nation as a worldwide beacon of freedom and liberty.

As part of our resolve, it is critical that tools to defeat terrorism remain available to the men and women of our national security

and intelligence community, who work tirelessly to protect our country and to secure the freedoms that we cherish.

Several of these tools are set to expire on December the 15th. It is our duty to reauthorize these authorities. Otherwise, the authorities revert back to our national security posture before 9/11. I don't think anyone wants that.

I am actually kind of glad we are actually having this hearing. It expires on December 15th, we could have been working on this a long time. I guess we have been busy with other things. We are at least having this hearing today.

The Foreign Intelligence Surveillance Act was originally passed to protect Americans from surveillance abuses. Our national security apparatus surveillance regime offers the access to critical foreign intelligence that we need, but we must ensure that there is a balance in both protecting our security and our civil liberties. FISA was created to do that.

In 2016, during and after the Presidential election, this balance appears to have broken down. While Democrats accused Republicans of simply trying to divert attention for political purposes, it is now clear that those at the pinnacle of our national security community lost all the objectivity that they were required by law to exercise. That is coming out now as we see a FISA report coming out soon.

A necessary component for Americans' trust in the intelligence community is the perception of fairness, particularly when implementing surveillance against Americans. Like many Americans, I await the Inspector General Horowitz's report on potential FISA abuse from the Presidential election period. However, it is a fact that multiple individuals at the top of the FBI have either been fired, terminated, or even referred for and reported to be under criminal investigation, although that has seemed to escape the notice of the majority on this committee.

Oversight and deterrence are clearly needed when the top-level officials in our intelligence and law enforcement community are officially criticized and potentially even indicted for divulging sensitive information and lying. That said, today we face the reauthorization of authorities passed in 2015 as part of the USA FREEDOM Act focused on battling terrorism. Three provisions—Sections 215, Business Records; lone wolf; and roving wiretaps—must be reauthorized. It is admittedly difficult to separate our concerns on FISA abuse from reauthorization facing us, but we need to protect valuable tools in combating violent extremists and their evil goals.

Two of the authorities are fairly straightforward, the lone wolf and roving wiretap provisions. The lone wolf provision essentially permits surveillance of terrorists seeking to harm us, even if there is no proof of the terrorist being directly connected to ISIS or al-Qaeda.

Why? We know this has been a trajectory of terrorist attack where the perpetrators are not "Members" of these particular terrorist organizations but are inspired by their medieval ideologies.

The roving wiretap provision allows the intelligence community to follow terrorists and spies who attempt to thwart or evade surveillance by dumping and switching phones. If we can do this for drug dealers, we should be able to do it for suspected terrorists.

Regarding section 215, I look forward to hearing more from the FBI on their use of this authority. The ability to obtain business records, particularly in terrorist and foreign intelligence investigations, but also of suspected spies, is not something whose authority we can afford to let expire. However, section 215, as used for collecting call data records, however, has been significant and seemingly insurmountable technical problems in its implementation.

We would like to hear from the NSA on their thoughts and the continuing validity of 215 for collecting CDRs.

I would like to thank each of the agencies who are here this morning. I wish that more had been able to come this morning. I wish that we could do this, but in the spirit of 9–1–1 and the countless other senseless terrorist attacks illustrate the need for our Nation to always be on guard. The authorities are set to expire in December. We have gotten to it now, thankfully. Despite the apparent misuse and abuse of other FISA authorities, are not the ones we should be removing from our counterterrorism toolbelt.

I look forward to the witnesses' testimony, and I yield back.

Chairman NADLER. I thank the gentleman.

I will now introduce today's witnesses. Brad Wiegmann—and I pronounced that correctly? Brad Wiegmann is the Deputy Assistant Attorney General at the Department of Justice, National Security Division. Previously, he served in legal positions at the Department of Defense and State and at the National Security Council.

He also served as a law clerk for Judge Patrick Higginbotham on the United States Court of Appeals for the Fifth Circuit. Mr. Wiegmann received his B.A. from Duke University and his J.D. from Harvard Law School.

Michael Orlando is the Deputy Assistant Director at the Federal Bureau of Investigation's Counterterrorism Division. He entered duty as a special agent in the Pittsburgh field office in 2003 and has since worked on counterintelligence matters at the Honolulu, Baltimore, and Washington field offices. Previously, Mr. Orlando worked as the Assistant section Chief of East Asia Counterintelligence Investigations.

Prior to working for the FBI, Mr. Orlando served in the U.S. Army. He received his B.A. from the State University of New York College at Cortland and received a Master's in Leadership from Georgetown University's McDonough School of Business.

Susan Morgan has worked in NSA operations for 18 years.

We welcome all our distinguished witnesses, and we thank them for participating in today's hearing.

Now, if you would please rise, I will begin by swearing you in. Raise your right hand unless you are a lefty.

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

[Response.]

Chairman NADLER. Thank you.

Let the record show the witnesses answered in the affirmative. Thank you, and please be seated.

Please note that each of your written statements will be entered into the record in its entirety. Accordingly, I ask that you summarize your testimony in 5 minutes. To help you stay within that

time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, it signals your 5 minutes have expired.

Mr. Wiegmann, you may begin.

TESTIMONY OF BRAD WIEGMANN

Mr. WIEGMANN. Chairman Nadler, Ranking Member Collins, Members of the committee, thank you for the opportunity to testify today about four important provisions of the Foreign Intelligence Surveillance Act, or FISA.

These are authorities that will expire at the end of this year unless reauthorized by Congress. The Administration strongly supports permanent reauthorization of these provisions.

Three of the authorities—the roving wiretap, business records, and lone wolf provisions—have been part of FISA for well over a decade. They have been renewed by Congress multiple times, most recently in the USA FREEDOM Act of 2015. Before that, these same authorities were reauthorized multiple times between 2005 and 2011, and each renewal gained bipartisan support.

Today, I will give you a brief overview of these three legal authorities and then turn it over to my colleague from FBI to address how they have been used in practice and their value to national security. Then my colleague from NSA will address the fourth authority, the call detail records, or CDR authority, under which NSA can engage in targeted collection of telephony metadata in counterterrorism investigations.

First, the roving wiretap authority. This enables the Government to continue surveilling a FISA court-approved national security target when the target is taking affirmative steps to thwart the surveillance. These are individuals who rapidly and repeatedly change communication service providers to evade Government monitoring.

The roving provision allows us to continue surveillance without having to go back to the FISA court for a new order each time the target switches his phone. The Government has used this authority in a relatively small number of cases each year. The cases tend to involve highly trained foreign intelligence officers operating within the United States or other important investigative targets, including terrorism targets.

The Wiretap Act has for decades contained a similar roving provision for ordinary criminal investigations of, say, drug dealers or organized crime figures.

Second, the business records authority. This allows the Government to apply to the FISA court for an order to collect records, papers, and other tangible things that are relevant to a national security investigation. It allows the Government to obtain many of the same types of records that it can obtain through a grand jury subpoena in an ordinary criminal case.

For example, it can be used to obtain driver's license records, hotel records, car rental records, shipping records, and the like. In most cases, these are records for the Government can be obtain in ordinary criminal or civil investigation without any court order.

A FISA business records order is typically sought because national security interests preclude the use of the less secure criminal

authorities or because there may be no criminal investigation underway in the intelligence context. This authority has been used several dozen times a year, on average, over the last several years.

Now, the business records provision is also the mechanism for the targeted collection of CDRs from U.S. telecommunication service providers. As my colleague from NSA will discuss in a few minutes, this provision provides a way for the Government, pursuant again to a FISA court order, to identify telephone contacts of suspected terrorists who may be within the United States.

Finally, the lone wolf provision. This enables the Government to surveil a foreign person who is engaged in international terrorism, but who lacks traditional connections to a terrorist group. It also applies to foreign persons engaged in international proliferation of weapons of mass destruction.

Although the Government has not used the lone wolf authority to date, it fills an important potential gap in collection capabilities where isolated actors are concerned. It allows for the surveillance of a foreign terrorist who might be inspired by a foreign terrorist group, but who is not technically an agent of that group.

So, for example, it would allow for surveillance of a foreign person who has self-radicalized through viewing propaganda of a foreign terrorist organization like ISIS or al-Qaeda on the Internet or a known international terrorist who severs his connection with a foreign terrorist group.

Use of any of these three authorities requires approval from the FISA court under standards prescribed in law. Each also requires strict rules governing how the Government must handle any information that is obtained concerning U.S. persons. Each also is subject to extensive executive branch oversight, as well as congressional reporting requirements and oversight. As I have said, each has been renewed by Congress multiple times in the past.

With that, I will stop and turn it over to my colleagues.

TESTIMONY OF MICHAEL ORLANDO

Mr. ORLANDO. Good morning, Chairman Nadler, Ranking Member Collins and Members of the committee.

Chairman NADLER. Good morning.

Mr. ORLANDO. Thank you for the opportunity to testify today about important provisions of the USA FREEDOM Act that will expire later this year unless reauthorized by Congress.

These provisions have been integral to the FBI's success in many national security investigations. While I will likely not be able to get into specific examples of our use of these provisions in an open setting, I will do my best to provide you with thorough hypothetical use situations.

I have seen these provisions throughout my time as both a counterintelligence agent and a counterterrorism agent. I am looking forward to answering your questions today.

National security threats have evolved significantly in the last 20 years. From the proliferation of mobile smartphones to the expanded use of end-to-end encryption, new technology has allowed our threat actors to work increasingly in the shadows. Today, we have nearly universal access to the Internet, and anyone with a cell phone can view and become radicalized by extremist content.

Our subjects are no longer forced to travel to other countries to communicate with other extremists who threaten the security of the United States. Instead, they can do this from their home. Because of this, we are also witnessing a shift toward individuals acting alone, with multiple ideologies and without clear ties to any one foreign adversary.

Our window for identification and disruption is getting smaller. Our subjects are quickly moving from radicalization to mobilization.

As these threats have evolved, Congress has helped us ensure we are prepared with the appropriate tools to continue to protect the U.S. and its interests. I am here today to talk about the expiring provisions, which the FBI uses with FISA court approval and oversight.

As my colleague from the Department of Justice explained, we use the business records provision to obtain records or other tangible things for use in a national security investigation. We often describe the business records provision as a "building block" authority. That means we use it during the early stages of an investigation to build our case against national security threats.

It is important to note the responses to the business records order do not contain content. If we see that the suspect is communicating with a known bomb maker in another country, for example, that is incredibly important information.

As in this case, the information we get from business record orders often help us establish the legal threshold we need to reach to get an order from the FISA court for more advanced investigative techniques, such as a wiretap. For example, once we receive the business record returns that the suspected terrorist is communicating with a known bomb maker, we would have relevant information to help establish probable cause for a wiretap.

Similarly, if we received business record returns showing that the suspect, the terrorist, is buying bomb-making materials like nitrogen-based fertilizer and large amounts of ball-bearings, that information can also help us establish probable cause.

The roving authority detailed in the USA FREEDOM Act is also an important provision that counteracts efforts by various national security threats, including terrorists and intelligence officers, to avoid court-authorized surveillance. These individuals often employ tactics such as using multiple burner phones or regularly creating new email accounts.

Without this roving authority, we would struggle to keep awareness of our targets as they purposely take action to thwart surveillance. We use this authority regularly in our national security investigations as a tool to avoid missing critical intelligence that would be lost if our ability to initiate surveillance was delayed.

It is worth noting that the FBI only seeks roving authority when the requirements of the statute are met. That means we must provide information to show that the target's actions can have the effect of thwarting surveillance.

The last authority the FBI requests you reauthorize is the lone wolf provision. While it has not been used since authorization, we believe it is important to have available.

Homegrown violent extremists are among the FBI's top threats to the homeland. These individuals are, by definition, not in direct collaboration with foreign terrorist organizations. Homegrown violent extremists are often self-radicalized online through terrorist propaganda and are motivated to attack with no direction from individuals associated with a foreign terrorist organization.

The lone wolf provision is narrowly tailored to only allow use against non-U.S. persons, which gives the FBI an additional tool without impacting the rights of any U.S. person.

These authorities are critically important in our fight to keep the American public safe. The FBI urges Congress to reauthorize these authorities because they will continue to play an important role in the FBI's national security investigations as our adversaries continue to advance.

Thank you for the opportunity to appear before you today. I am happy to answer any questions related to these authorities.

Chairman NADLER. Thank you very much. Ms. Morgan?

TESTIMONY OF SUSAN MORGAN

Ms. MORGAN. Good morning, Chairman, Ranking Member, distinguished Members of the committee.

Thank you for the opportunity to testify today about the National Security Agency's Call Detail Records Program.

The authority for the Call Detail Records, or CDR, Program is among the important provisions of the Foreign Intelligence Surveillance Act that will expire at the end of this year unless reauthorized by Congress.

Congress added this authority to the Foreign Intelligence Surveillance Act 4 years ago in the USA FREEDOM Act, as one of several significant reforms designed to enhance privacy and civil liberties. It replaced NSA's bulk telephony metadata collection program with a new legal authority whereby the bulk metadata would remain with the telecommunication service providers.

As this committee's 2015 report described, the CDR authority provides a "narrowly tailored mechanism for the targeted collection of telephone metadata for possible connections between foreign powers or agents of foreign powers and others as part of an authorized investigation to protect against international terrorism."

Critically, the provision authorizes the collection of certain metadata associated with telephone calls, such as the originating or terminating telephone number and date and time of a call, but does not authorize collecting the content of any communication, the name, address, or financial information of a subscriber or customer, or locational information.

As this Committee is aware, the NSA recently discontinued the CDR program and deleted the records acquired under the CDR authority after balancing the program's intelligence value, associated costs, and compliance and data integrity concerns.

NSA's decision to suspend the CDR program does not mean that Congress should allow the CDR authority to expire. Rather, that decision shows that the executive branch is a responsible steward of the authority Congress affords it.

As technology changes, our adversaries' tradecraft and communication habits continue to evolve and adapt. In light of this dy-

namic environment, NSA supports reauthorization of the CDR provision so that the Government will retain this potentially valuable tool, should it prove useful in the future.

Thank you again for the opportunity to testify today. I look forward to your questions.

[The joint statement of Mr. Wiegmann, Mr. Orlando, and Ms. Morgan follows:]

JOINT STATEMENT OF BRAD WIEGMANN, MICHAEL ORLANDO, AND SUSAN MORGAN

Introduction

Chairman Nadler, Ranking Member Collins, distinguished Members of the Committee, thank you for the opportunity to testify today about four important provisions of the Foreign Intelligence Surveillance Act ("FISA") that will expire at the end of this year unless reauthorized by Congress. As indicated in the Director of National Intelligence's letter to this Committee, the Administration strongly supports permanent reauthorization of these provisions.

Three of the authorities—the roving wiretap, business records, and lone wolf provisions—have been part of FISA for well over a decade and have been renewed by Congress multiple times, most recently in the USA FREEDOM Act of 2015 ("FREEDOM Act"). Before that, these same authorities were reauthorized multiple times between 2005 and 2011, each time following extensive congressional review and deliberation. Each renewal gained bipartisan support.

Two of the authorities, the "roving wiretap" and "business records" provisions, have been part of FISA since 2001. These provisions are important in national security investigations and are comparable to provisions available in ordinary criminal investigations. The roving wiretap authority enables the Government to continue surveilling a court-approved national security target when the target takes steps to thwart the surveillance. The business records authority allows the Government to collect records, papers, and other documents that are relevant to a national security investigation. The Government has used these important national security authorities judiciously, with the approval of the Foreign Intelligence Surveillance Court ("FISC"), and in the interest of national security.

The "lone wolf" provision was added to FISA in 2004 to close a gap in the Government's ability to surveil a foreign person who is engaged in international terrorism or international proliferation of weapons of mass destruction, but who lacks traditional connections to a terrorist group or other foreign power. Without the authority, the Government could not rely on FISA to respond to those kinds of threats. Although the Government has not used the lone wolf provision to date, it is critical this authority remain in the Government's toolkit for the future, as international terrorist groups increasingly seek to inspire individuals to carry out attacks, without necessarily providing the kind of coordination or support that would authorize traditional FISA surveillance.

The fourth authority—the Call Detail Records ("CDR") provision—permits the targeted collection of telephony metadata but not the content of any communications. Congress added this authority to FISA four years ago in the FREEDOM Act as one of several significant FISA reforms designed to enhance privacy and civil liberties. It replaced the National Security Agency's ("NSA") bulk telephony metadata collection program with a new legal authority whereby the bulk metadata would remain with the telecommunications service providers. As this Committee's 2015 report described, the CDR authority provides a "narrowly-tailored mechanism for the targeted collection of telephone metadata for possible connections between foreign powers or agents of foreign powers and others as part of an authorized investigation to protect against international terrorism." H. Rep. 114–109, at 17 (2015). The FREEDOM Act also permanently banned bulk collection under FISA's business records and pen-trap provisions and under the National Security Letter statutes. As this Committee is aware, the NSA recently discontinued the CDR program for technical and operational reasons. But the CDR program retains the potential to be a source of valuable foreign intelligence information. The CDR program may be needed again in the future, should circumstances change. NSA's careful approach to the program, and the legal obligations imposed by the FREEDOM Act in the form of judicial oversight, legislative oversight, and transparency, support the reauthorization of the CDR program.

We urge the Committee to consider permanently reauthorizing these authorities based not only on the Government's demonstrated record and the importance of the authorities to national security, but also on the significant reforms contained in the FREEDOM Act. These include authorizing the FISC to appoint *amici curiae* to address privacy and civil liberties concerns and enhancing public transparency and reporting requirements under FISA. Four years ago, the FREEDOM Act was passed after extensive oversight and comprehensive hearings, and it was reported out of this Committee with unanimous support. In the wake of repeated reviews and bipartisan authorizations over nearly two decades, the Administration's view is that the time has come for Congress to extend these authorities permanently.

Roving Wiretap

First, Congress should permanently reauthorize the "roving wiretap" provision. The authority outlined in this provision is similar to the roving wiretap authority that has been available since 1986 in criminal investigations, under the Wiretap Act, and which has repeatedly been upheld in the courts.

The "roving wiretap" provision provides the Government an effective tool to use in response to adversaries attempting to thwart detection. To understand the importance of this authority, the Committee must consider how FISA functions in ordinary, non-roving cases, and how roving authority is necessary for targets who try to avoid surveillance. Under both regular and roving FISA authority, the Government's application for a court order must identify the target of the surveillance with particularity and must establish probable cause that the target is a foreign power or an agent of a foreign power. If the Court approves the application, it issues one order to the Government and a "secondary" order to a third-party—such as a telephone company—directing it to assist the Government in conducting the wiretap. *See* 50 U.S.C. 1805(c)(1–2). The secondary order is necessary because, in most cases, the Government needs the assistance of a company to implement the surveillance. In an ordinary case, if the target switches to a new communications service provider, the Government must submit a new application and obtain a new set of FISA orders. However, where the Government can demonstrate in advance to the FISA Court that the target's actions may have the effect of thwarting surveillance, such as by rapidly and repeatedly changing providers, FISA's roving wiretap provision allows the FISC to issue a generic secondary order that the Government can serve on the new provider to commence surveillance without first going back to the Court. *See* 50 U.S.C. 1805(c)(2)(B). The Government's probable cause showing that the target is an agent of a foreign power remains the same, and the Government must also demonstrate to the FISC, normally within 10 days of initiating surveillance of the new facility, probable cause that the specific target is using, or is about to use, the new facility. *See* 50 U.S.C. 1805(c)(3).

The roving wiretap authority has proven to be an important intelligence-gathering tool. The Government has used the authority in a relatively small number of cases each year. Those cases tend to involve highly-trained foreign intelligence officers operating within the United States, or other important investigative targets, including terrorism-related targets, who have shown a propensity to engage in activities deliberately designed to thwart surveillance. Similar authority designed to prevent suspects from thwarting surveillance has been a permanent part of our criminal law for over thirty years, and this provision has been renewed as part of FISA repeatedly since 2001 without controversy or evidence of abuse. It remains an important tool, and we strongly support permanent reauthorization.

Business Records

Second, we also support permanent reauthorization of the so-called "business records" provision, which was enacted as section 215 of the USA PATRIOT Act in 2001. This provision authorizes the Government to apply to the FISC for an order directing the production of business records or other tangible things that are relevant to an authorized national security investigation. It allows the Government to obtain in a national security investigation many of the same types of records and other tangible things that the Government can obtain through a grand jury subpoena in an ordinary criminal investigation. The Government has used the business records provision to obtain, for example, driver's license records, hotel records, car rental records, apartment leasing records, and the like. An application for such records, and other sensitive records, must come from the FBI Director, Deputy Director, or Executive Assistant Director. *See* 50 U.S.C. 1861(a)(3).

Importantly, the business records provision contains several statutory safeguards. To obtain a FISC order approving a business records application, the Government

must make a showing to the FISC that (1) it is seeking information in an authorized national security investigation conducted pursuant to guidelines approved by the Attorney General; (2) where the investigative target is a U.S. person, the Government has demonstrated that the investigation is not based solely on activities protected by the First Amendment; and (3) the Government must demonstrate that the information sought is relevant to the authorized investigation. *See* 50 U.S.C. 1861(a)(1–2). The Government must also adhere to Attorney General guidelines and minimization procedures that limit the retention and dissemination of any information collected concerning U.S. persons. *Id.* 1861(a)(2)(A) & (g). Recipients of an order seeking business records also have the opportunity to challenge the legality of the order in court, although, to date, no recipient has done so.

Some criticize the business records provisions as running afoul of the Fourth amendment because business records orders are not issued under a "probable cause" standard. But an order issued under the business records provision does not authorize the Government to enter premises, or to search for or seize records or other tangible things. Thus, the Fourth Amendment's probable cause standard generally does not apply. Rather, the records the Government is authorized to obtain—pursuant to a FISC order—are similar to those that the Government could obtain in ordinary criminal or civil investigations—without *any* court order in most instances—pursuant to a grand jury subpoena in an ordinary criminal case, or pursuant to an administrative subpoena in a civil case. Like a grand jury subpoena or an administrative subpoena, a business records order merely requires the recipient to identify and produce responsive records or other tangible things.

Critics have also questioned the need for the business records provision in view of the Government's ability to seek similar records pursuant to a grand jury subpoena. But not every national security investigation involves criminal activity; thus, a grand jury subpoena is not always available to the Government. Additionally, business records orders issued by the FISC are often supported by classified information that cannot be disclosed to the grand jury and cannot be declassified without compromising important national security interests. Thus, reauthorization of this provision remains critically important.

To be sure, this authority has generated substantial controversy because it was employed, with FISC approval, to support NSA's bulk telephony metadata collection program. However, that program has been terminated and replaced by the more targeted collection of telephony metadata authorized under the CDR provisions of the FREEDOM Act, as discussed below. The FREEDOM Act permanently banned bulk collection altogether under the business records authority and required the use of a "specific selection term" to justify an application for a business records order. The law defines "specific selection term" as a term that "specifically identifies a person, account, address, or personal device, or any other specific identifier [that] is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought, consistent with the purpose for seeking the tangible things." 50 U.S.C. 1861(k)(4)(A)(i). It does not include terms, or a combination of terms, that are not so limited. *See id.* 1861(k)(4)(A)(ii). Moreover, the FREEDOM Act provided that the FISC may evaluate the adequacy of minimization procedures issued under the business records provisions, and may require additional, particularized minimization procedures beyond those otherwise required, with regard to the production, retention, or dissemination of certain business records, including requiring the destruction of such records within a reasonable period of time. *See id.* 1861(g)(3).

The Government has used the business records authority judiciously. On average, between 2015 and 2018, the Government sought and obtained records under this provision less than 76 times per year. The number of business records applications approved has decreased every year since 2012. Many of these investigations seek records that are outside the scope of the National Security Letter statutes, and often a business records order is sought because national security interests preclude the use of less secure criminal authorities, or because there may be no criminal investigation underway. Given the importance of the authority, the absence of any evidence of abuse, and the additional safeguards Congress imposed in 2015, we urge the Committee to support permanent reauthorization of this provision.

Lone Wolf

The third expiring provision is the so-called "lone wolf" provision of FISA. It allows the FISC to authorize surveillance of *non-United States* persons engaged in international terrorism or the international proliferation of weapons of mass destruction, without the need to show that the target is acting on behalf of a particular terrorist group or other foreign power.

The "lone wolf" provision is contained within the definition of an "agent of a foreign power" in FISA. Electronic surveillance under FISA can only be directed at a "foreign power" or "agent of a foreign power," as defined in the statute. *See* 50 U.S.C. 1804(a)(3)(A). A foreign power under FISA is defined for counterterrorism purposes to include a group engaged in international terrorism. Accordingly, without the lone wolf provision, the Government would need to establish that a terrorism-related surveillance target was an *agent of an international terrorist group*. The lone wolf provision specifies that a foreign individual is also considered an "agent of a foreign power" under FISA if the individual is engaged in international terrorism—even if the individual is not directly connected to a foreign terrorist group.

There are two key points to understand about this provision. First, it applies only to non-U.S. persons (not to American citizens or aliens lawfully admitted for permanent residence), *see* 50 U.S.C. 1801(b)(1)(C), and second, only when they engage or prepare to engage in "international terrorism," *see id.* 1801(c). In practice, to establish the probable cause necessary to secure a FISC order under the lone wolf provision, the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity, to satisfy the definition of "international terrorism."

Although the Government has not used the lone wolf authority to date, it fills an important gap in the Government's collection capabilities. The provision allows for the surveillance of a foreign terrorist who might be *inspired* by a foreign group, but who is not technically an agent of that group. For example, the provision would allow for surveillance of a foreign person who has self-radicalized through internet propaganda of a foreign terrorist organization, or a known international terrorist who severs his connection with a terrorist group. The Government's decision not to employ this authority to date does not mean that it should be abandoned. To the contrary, it shows that the Government will use this provision only where necessary and legally available. Terrorist groups like ISIS and al-Qaida actively seek to encourage lone wolf attacks. The continued availability of the lone wolf provision ensures the Government retains the authority to surveil isolated foreign terrorist actors who are inspired, but not directed by, foreign terrorist groups.

Call Detail Records

Finally, as we have explained, in addition to reauthorizing these longstanding provisions of FISA in 2015, the FREEDOM Act banned bulk collection and established a new, narrowly-tailored mechanism for the targeted collection of CDRs from U.S. telecommunications service providers. The new provisions were enacted after comprehensive oversight, including hearings addressing recommendations of a presidentially-appointed group of outside experts and the Privacy and Civil Liberties Oversight Board, which weighed in on the privacy and civil liberties effects of the authorities and their importance to national security.

The CDR provision represents a carefully tailored balance between the interest in individual privacy and the need to protect against the activities of international terrorist groups. In support of an authorized counterterrorism investigation, the CDR authority provides a way for Government investigators, pursuant to a FISC order, to identify contacts of suspected terrorists who may be within the United States. It permits the Government to seek an order from the FISC compelling the production on an ongoing basis of CDR information based on a specific selection term, such as a telephone number. The Government must demonstrate to the FISC that (1) there are reasonable grounds to believe that the data sought is relevant to an authorized counterterrorism investigation; and (2) there is a reasonable, articulable suspicion that the specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation of international terrorism. *See* 50 U.S.C. 1861(b)(2)(C). Critically, the provision authorizes the collection of certain metadata associated with telephone calls, such as the originating or terminating telephone number and date and time of a call, but *does not authorize* collecting the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. *See id.* 1861(k)(3). With FISC approval, the Government may require the production of CDRs two "hops" from the seed term—*i.e.*, the CDR's associated with the initial specific selection term and those associated with the CDRs identified in the initial "hop." *See id.* 1861(c)(2)(F).

The Government has used this authority responsibly. In 2018, the NSA identified certain technical irregularities in data it received from telecommunications service providers under the CDR provision. Because it was not feasible for NSA to resolve the issue technologically, in May of 2018, NSA began the process of deleting all CDR data that it had received since 2015. Then, after balancing the program's intel-

ligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes, NSA suspended the CDR program.

NSA's decision to suspend the CDR program does not mean that Congress should allow the CDR authority to expire. Rather, that decision shows that the Executive Branch is a responsible steward of the authority Congress afforded it, and that the numerous constraints on the Government imposed by the FREEDOM Act, including oversight by the FISC, are demanding and effective. As technology changes, our adversaries' tradecraft and communications habits continue to evolve and adapt. In light of this dynamic environment, the Administration supports reauthorization of the CDR provision so that the Government will retain this potentially valuable tool should it prove useful in the future.

The Administration looks forward to working with this Committee and the rest of the Congress to reauthorize on a permanent basis these important national security provisions.

Chairman NADLER. Thank you very much for your testimony.

We will now proceed under the 5-minute Rule with questions. I will begin by recognizing myself for 5 minutes.

Ms. Morgan, I want to ask you about the Call Detail Records Program. In 2014, prior to the passage of the USA FREEDOM Act, the Privacy and Civil Liberties Oversight Board reviewed the efficacy of the NSA's use of section 215 to collect "detail records."

The board concluded rather starkly, and I quote, "We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."

The board continued, "Even in those instances where telephone records collected under section 215 offered additional information about the contacts of a known terrorism suspect, in nearly all cases, the benefits provided have been minimal, generally limited to corroborating information that was obtained independently by the FBI."

In short, the board found this very complicated program to be of very little use to the intelligence community.

Ms. Morgan, is there any reason to doubt the accuracy of the board's conclusions in 2014?

Ms. MORGAN. Sir, thank you. Thank you for your question.

So, I just want to start out by saying I think a metric in terms of determining the value of a particular intelligence program, the number of attacks it has prevented, is but one metric, or the number of attacks it has contributed to identifying is but one metric that you could consider, but it is certainly not the only metric.

I came into the agency in the summer of 2001 as an intelligence analyst, and I could tell you that as an intelligence analyst, you are typically dealing with disparate pieces of information, and you are trying to pull them together in different ways to create a picture to understand what your target or adversary might be doing in response to a valid foreign intelligence requirement.

So, when we looked at the CDR program, as it existed up until we suspended it, we did look and evaluate the foreign intelligence value that the program did provide. It did certainly provide value.

However, you have to weigh that in the context of everything else that we are doing, and you have to weigh that against not only

the data integrity and compliance concerns that we face, but you also have to weigh that against the resources and the costs that we are expending, as we want to be a good steward of the taxpayers' dollars and resources.

So, I would say that it is very difficult to—it is not ever a black-and-white answer when you are trying to analyze the value of a particular activity. There is a lot of factors that go into that, and I could get a piece of information today that 7 or 10 or 11 steps down the line later might actually prove to be really valuable.

Chairman NADLER. The CDR program was reconstituted under the USA FREEDOM Act after its passage in 2015. Now please help me update the board's findings. Sitting here today, can the NSA cite any instance involving a threat to the United States in which the CDR program made a concrete difference in the outcome of a counterterrorist investigation?

Ms. MORGAN. Sir, as I alluded to earlier, the measure of value isn't necessarily—

Chairman NADLER. The—

Ms. MORGAN. Yes, sir?

Chairman NADLER. I heard that. You don't have to repeat it. My time is limited. So, the answer is no or yes?

Ms. MORGAN. In an open setting, I am really leery to get into specific examples of the value that the program—

Chairman NADLER. I asked you a specific question.

Ms. MORGAN. Yes, sir.

Chairman NADLER. Can the NSA cite any instance involving a threat to the U.S. in which the CDR program made a concrete difference in the outcome of a counterterrorist investigation?

Ms. MORGAN. Sir, respectfully, I would say that is a complicated question that to effectively answer it, I need to go into classified information.

Chairman NADLER. Okay. Is the NSA aware of any instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack? Same answer?

Ms. MORGAN. Again, sir. I would like to, if I may?

Chairman NADLER. Go ahead.

Ms. MORGAN. I would like to say that I don't think a metric of a program in terms of its value should be really necessarily focused on whether or not it prevented or stopped a terrorist attack.

Chairman NADLER. Okay. After the CDR program was reconstituted under the USA FREEDOM Act, the NSA realized it had two problems on its hands. First, it was pulling in phone records that it should not have received, and second, it had no way of untangling the good data from the bad. Is that a fair assessment of the problem?

Ms. MORGAN. Yes, sir.

Chairman NADLER. On June 28th of last year, the NSA decided to purge its entire database, nearly 3 years of call detail records. Is that correct?

Ms. MORGAN. Yes, sir.

Chairman NADLER. In the press release announcing the destruction of those records, the NSA stated that it had contacted the appropriate congressional committees of its intent to do so. Do you

happen to know if the NSA contacted the House Judiciary Committee in advance of that press release?

Ms. MORGAN. Sir, I apologize. I have to take that back. I don't have those specifics.

Chairman NADLER. Okay. On August 16, 2019, the NSA decommissioned the CDR program altogether. According to former Director Coats, the intelligence community weighed the costs against the benefits, saw that the benefits are minimal, and decided to discontinue the program. Is that correct?

Ms. MORGAN. Yes, sir.

Chairman NADLER. Okay. To sum up, the CDR program had its origins in an extralegal, Bush-era spying program. From the moment it was brought under FISA—from the moment it was brought under FISA in 2006 to the moment it was discontinued in 2019, it did not once make a material difference to a single counterterrorism investigation, at least that you can tell us about.

One last question, Ms. Morgan. Why has the Trump Administration asked us to reorganize—I am sorry. In light of this record, why has the Administration asked us to reauthorize this program?

Ms. MORGAN. Sir, as an intelligence professional, I will tell you that I want to have every tool available in my toolbox. I am not able to, although I wish I could, predict what the future situation is going to hold. Should I confront a situation where this tool would valuable to protect international security, protect us against terrorist activities, I would like the tool to remain available.

Chairman NADLER. Okay. Let me just say that is a very good effort, but I think the Administration will have to do a little better than that, than to say that we have a perhaps useless program, but we want to reauthorize it because maybe some day it will do some good. Have to give it some more basis to believe, in fact, that it has a future utility.

My time is expired. The gentleman from Georgia, Mr. Collins.

Mr. COLLINS. Take as much time as you need there, Mr. Chairman. You did yesterday.

One of the things I want to point out, Ms. Morgan, is normally we have had the secure—or exec session or a classified briefing after this. We don't have that today. So, I understand your questions here. I don't know why we didn't, but we are choosing not to do that today.

We have done this in the past, and it would have been good to have. I think you would probably have been able to answer questions in classified briefings much better.

I do appreciate Chairman actually acknowledging me for my 5 minutes today, and I appreciate that.

What the session—Ms. Morgan, what session-identifying information collected under the Call Detail Records Program, if we terminate that and allow the program to fast-forward expire, a terrorist decides to communicate over encrypted app, is the ability to collect session-identifying information lost with respect to encrypted communications?

Ms. MORGAN. Sir, I apologize. In an open hearing, I can't get into capabilities—

Mr. COLLINS. Thus, the reason it would have been nice to have had a classified hearing after this as well, which we could have gotten into this.

Ms. MORGAN. Sir, I am absolutely willing to arrange for a time that is convenient for you and the rest of the Committee to talk about this in a classified—

Mr. COLLINS. Now that is fine. We have had all year, and we are here now. You know, I guess we just have to deal with it. So that is fine.

Mr. Wiegmann, does the criminal Brady requirement imposed on prosecutors to divulge exculpatory evidence favorable to the defendant also apply when practicing before a FISA court? In other words, even though the proceedings are *ex parte*, is there any requirement from the Department to inform the court of evidence favorable to the target of the FISA surveillance that could Act to initiate a probable cause that the person is an agent of a foreign power?

Mr. WIEGMANN. I believe we do provide the full picture in terms of what the information is available when we are applying you are saying regular Title I FISA. For example, we provide the full picture, and that would include it is not really Brady as a principle. Because that is a principle of applicability in a criminal case, not in a FISA application.

We do disclose, I think as an ordinary course, to the court the information that would suggest the person is an agent and any information that suggests the contrary. I believe that is our practice.

Mr. COLLINS. So, if you didn't disclose exculpatory information, you chose to keep it as beginning to be more, this is a very real concern because that is lying to the court. Correct?

Mr. WIEGMANN. Really, you would have to know the facts of that particular case to—

Mr. COLLINS. Well, if you had exculpatory information, you didn't, as you just said, provide a full picture to the court. If you don't provide a full picture, would that not be a problem?

Mr. WIEGMANN. I think the effort is to provide a full picture to the court, but not to conceal any information from the court.

Mr. COLLINS. Not my question. Not my question. Not the effort. If it happened, is that a problem? Is that something that you would not say should happen?

Mr. WIEGMANN. In general, I think we would want to provide all the information, all the relevant information to the court. Absolutely, sir.

Mr. COLLINS. Okay. So, in general, you say it is okay. In cases where you don't want to disclose it, you say it is okay?

Mr. WIEGMANN. No, sir. No, sir. Maybe I misspoke in saying in general. I do believe we should disclose all relevant information to the court in applying for a FISA.

Mr. COLLINS. If that is not, that is abuse of the court process?

Mr. WIEGMANN. I don't know if I would use those exact terms, but it is something that we work—

Mr. COLLINS. What would you call it?

Mr. WIEGMANN. Well, it is something that we work hard to do at DOJ, to provide all the information relevant to the court.

Mr. COLLINS. If it did not happen and to any court, even this court as well, if it did not happen, that is a failure. Correct?

Mr. WIEGMANN. It is something that we don't want to happen.

Mr. COLLINS. A failure. The elephant in the room is the Carter Page FISA, the surveillance sought and obtained by both the FBI and DOJ on the Presidential campaign volunteer. Have you conducted a Woods review of the Carter Page FISA to determine whether each and every fact was verified by some underlying evidence? And has anyone ever been held accountable for unlawful disclosure of the Carter Page FISA application to the media?

Mr. WIEGMANN. Sir, I really can't comment on that in any way. Among other reasons, I don't know anything about that particular case. So, I can't comment on it today.

Mr. COLLINS. You are not saying that my question just prior to this also hits at this very issue as well? This is an issue that is now not a secret court issue. This is not some—this has actually been put into the realm of the public and the media, if you are not using the information completely in a file.

Mr. WIEGMANN. I am not sure what your question is.

Mr. COLLINS. I understand you are not going to answer it either way. The problem is, though, and I think Chairman and I both do agree on some things, and this is one of the areas we agree, that there is a problem with the FISA. We have just not talked about it this year because it is not in the political narrative we are talking about.

There is a problem here that needs to be addressed. There has to be all and complete evidence brought to the FISA court, not just in general, as you said. I appreciate your concern of misspeaking.

The issue here is that we have got to make sure that this is a process which is open for everybody. Because there is not a person listening to this hearing today, whether apolitical or very political, this is not something we need to have the probability at the highest level of our intelligence communities and DOJ to have a political agenda or leave out stuff when they go to a court in which there is *ex parte* proceedings and not anybody available to correct that or to correct the record.

Then to actually have it leaked later in a sense in which no accountability has taken place so far. I think this is the issue.

I will go back. Hopefully, at some point, we will get a classified briefing, but my time has expired. I yield back.

Chairman NADLER. Let me just say that the minority staff worked with the majority staff in setting up this hearing, and the minority staff has been working with the majority staff in setting up a classified briefing, which will be scheduled.

Mr. COLLINS. Again, Mr. Chairman, I appreciate that. Also at a certain time, it has always been scheduled together, where we could have all of our stuff together and the witnesses here. I was just pointing out a simple fact.

I appreciate Chairman feeling he had the need to discuss the bipartisanship, which was so evident on this, but so lacking yesterday.

Chairman NADLER. Well, I have also commented I am not aware of any terrible problem with the FISA court and specifically not with the Carter Page application.

Mr. COLLINS. Because we have not talked about it until today. I would move on.

Chairman NADLER. Yes. The gentlelady from California?

Ms. LOFGREN. Thank you, Mr. Chairman.

You know, being in this room reminds me of after 9/11, and we actually came in on the weekend, and we sat around the table that you are—the witness table, and Mr. Sensenbrenner was chair of the committee. It was a bipartisan group, trying to figure out what are we going to put together.

I participated in that, and we came up with a bill. We didn't know how it would work at the time, but we knew we needed to do some things, and we did as a bipartisan group. It is entirely appropriate that we review what we did so long ago to make sure that it is working as we had hoped. It is obviously an important balance.

I mean, we need to keep our country safe. Everyone agrees with that. We also have strong incentive to make sure that the rights of Americans are fully protected and respected. I know that all of you would agree with that.

One of the questions that I have on these proceedings is how the court rulings having to do with privacy are integrated, if at all, into your proceedings. For example, the recent Supreme Court decision in Carpenter really challenged and overturned the predigital age notions of the kinds of information that Americans have a Fourth amendment right to privacy in.

Prior to Carpenter, law enforcement considered cell site geolocation data to be a business record and stored under the Communications Act. It didn't require a probable cause warrant. Now Carpenter, you need a probable cause warrant.

Has that been translated into the same kind of records as 215 would allow? Do you need probable cause to get geolocation records, as we do in the criminal matter? Who can answer that?

Mr. WIEGMANN. Yes, I can take that. So, you are absolutely right. The Carpenter decision, an important decision that in the context of a criminal case held that you needed a warrant in order to obtain historic cell site location information. So, that is not the same as GPS.

Ms. LOFGREN. Correct.

Mr. WIEGMANN. Iformation concerning a cell tower and so forth. So, they specifically in that Supreme Court case distinguished the national security context and said the ruling was only applicable in the context of a criminal case.

Ms. LOFGREN. I understand that. I understand.

Mr. WIEGMANN. We have given some thought to the issue of, okay, how does the Carpenter case apply in, let us say, the business records context? To really go into the detail, unfortunately, as to how we are applying it in that context, I would have to get into classified information, but I am happy to do that and provide that information to you as to what our policy is with respect to business records and how Carpenter applies to it.

So, again, I am happy to do that for you, simply.

Ms. LOFGREN. So, if I can just probe, what you are saying is you are looking at it. It is not the belief of the Department that Carpenter actually applies to what you are doing, but that you are con-

sidering the Fourth amendment implications for what—how you are proceeding. Would that be accurate?

Mr. WIEGMANN. I think it is a fair summary to say it is not controlling, but certainly something that we are giving serious—have given serious thought to in terms of how we apply it to our national security authorities, even though it is not controlling.

Ms. LOFGREN. You know, one of the things that I have had concern about is the collection of content under various provisions of our FISA efforts, and I do think it is important to note that if you get enough information, even if it is not called content, it actually provides tremendous insight into the details of privacy rights of Americans.

Can you, Ms. Morgan, talk about how much content that you obtain through this program?

Ms. MORGAN. Thank you for the question, ma'am.

So, I just want to emphasize that under NSA's program, the Call Detail Records Program, we don't receive any content at all. We receive things like "Telephone number A called telephone number B at this date and time for this duration."

That is—we are not receiving any content, and we are not receiving any locational information either.

Ms. LOFGREN. Let me ask in terms of—and maybe you can't answer this in a public session. In terms of text messages, pictures, emails, and the like, what is the universe of what you are collecting?

Ms. MORGAN. So, ma'am, again, under the CDR program, under the USA FREEDOM Act, we are not collecting any content. I am happy in a closed session to give you more insight into—

Ms. LOFGREN. Right. Under 215, none of that would be collected?

Ms. MORGAN. I will speak to NSA CDR provision. We are not collecting any content.

Mr. WIEGMANN. It is a little bit trickier in the context of the traditional uses of 215 because whether you call something content, like so is a driver's license record content or not? It is certainly substantive information. It is a third-party business record.

Ms. LOFGREN. Yes.

Mr. WIEGMANN. It has the information about the individual, or that a terrorist or suspected terrorist stayed at particular hotel on a particular night, that is the type of information that we may get.

Ms. LOFGREN. So under business records, you would get all of that?

Mr. WIEGMANN. That is right. We would get that information. It is not that it is not communications content, if that is what you are thinking.

Ms. LOFGREN. I understand.

Mr. WIEGMANN. We can't get substance of telephone calls or anything like that.

Ms. LOFGREN. My time has expired, Mr. Chairman. I thank you.

Hopefully, as we will when we originally crafted these measures, we all care about civil liberties. We will craft together amendments to it.

I yield back.

Chairman NADLER. The gentlelady yields back. The gentleman from Ohio?

Mr. CHABOT. Thank you, Mr. Chairman. Thank you for holding this oversight hearing so that we can get a better understanding of FISA provisions and procedures, some of which expire in a few months on December 15th.

For nearly a year since the start of this Congress, the majority has had this Committee and the American public endure their issuance of subpoena after subpoena, holding hearing after hearing, and passing resolution after resolution regarding an investigation that has long been completed by Special Counsel Robert Mueller.

Yesterday, Corey Lewandowski appeared before our Committee for several hours and again answered questions. He has already testified before Congress a number of times, but the result remains the same. The President neither conspired nor colluded with the Russians to impact or influence the 2016 presidential election.

Now the Russians did try to interfere. They set up fake Facebook accounts, *et cetera*, but that was under the Obama Administration's watch, not Trump's. So if there was insufficient effort to protect America from the Russians, it was Obama's fault, not Trump's.

Today, the American people might finally get some insight on how the original FISA application that then-FBI Director Jim Comey and other senior FBI officials obtained at the behest of the Democratic Committee and the Hillary Clinton campaign, how that began.

Mr. Orlando, let me begin with you. Could you please tell us under what circumstances the FBI might seek a FISA warrant to investigate an American citizen?

Mr. ORLANDO. Before an FBI can seek a FISA warrant on an American person, we first need a case open on that individual, where we need specific and articulable facts that person poses a threat to national security, which he has to have some sort of tie to a foreign power, generally as an agent of a foreign power or tie to a foreign terrorist organization.

Mr. CHABOT. Thank you.

And in order to initiate such a counterintelligence investigation, senior FBI officials must apply for and obtain a FISA warrant to collect the information related to these allegations. Is that correct?

Mr. ORLANDO. You are seeking a FISA warrant. There is an internal process of how we do that, and it elevates up to the Department of Justice, then to go over to the court.

Mr. CHABOT. Would it be proper for FBI agents to attempt to obtain FISA warrants to investigate senior Trump campaign advisers simply because they hated Donald Trump?

Mr. ORLANDO. That would not be appropriate. As I have stated earlier, for us to open a case, there needs to be specific and articulable facts that the person poses a threat to national security.

Mr. CHABOT. Would it be proper for FBI agents to open a counterintelligence investigation based upon hyper-partisan memos that were written by individuals linked to the opponent's campaign, in this case, the Clinton campaign?

Mr. ORLANDO. Back to my same answer. Sure, we would have to show that you are an agent of a foreign power.

Mr. CHABOT. Thank you.

As far as you are aware, do the FBI and other intelligence officials verify the truthfulness of the allegations in this field dossier about then-candidate Donald Trump?

Mr. ORLANDO. Sir, this is outside my purview.

Mr. CHABOT. Okay. Even though the information was never verified, and most of it has been proven to be false, the intel community relied on it to get a FISA application to spy on the Trump campaign. Is that basically what happened?

Mr. ORLANDO. Again, sir, that is outside my purview.

Mr. CHABOT. Thanks.

Mr. Orlando, tell me, what sort of information should an agent use to open a counterintelligence investigation?

Mr. ORLANDO. Really, a wide variety of information that we can use. There just simply needs to be some sort of allegation that has specific and articulable facts that believes there is a national security investigation. When an agent does that, there is a supervisor that reviews that and approves that opening of the case. In sensitive matters, it elevates the approval.

Mr. CHABOT. Thank you.

I have got a lot more questions, but you know, it appears to me that faulty information was used to investigate the Trump campaign officials' bipartisan agents. I just think it is strange that just a few weeks ago, Inspector General Horowitz issued a scathing report regarding the mishandling of sensitive information by James Comey.

It appears that nothing will happen relative to Mr. Comey. He won't be brought before this Committee to answer for the allegations in his report, and Mr. Horowitz won't have an opportunity to further testify as to what was really happening at the FBI when senior officials decided to open the investigation.

That is really a shame because the American people deserve to learn the truth, the truth about how it was that the Democratic National Committee and the Clinton campaign were able to peddle a fake dossier to obtain a FISA warrant and turn it into an unnecessary, expensive, time-consuming investigation in order to undermine an American presidency. The American people deserve better.

I yield to the gentleman.

Mr. JORDAN. Mr. Chairman, could I actually ask a question? I know the gentleman's time has expired.

Chairman NADLER. The gentleman's time has expired. The—

Mr. JORDAN. Could I ask the chair a question, just on something the gentleman just mentioned?

Chairman NADLER. Is it a parliamentary inquiry?

Mr. JORDAN. It is a question for Chairman of the committee. So, Mr. Chairman, the Ranking Members and the chairmen of the Oversight and Judiciary Committees received a letter from Mr. Horowitz last week, indicating that he has now turned the FISA report over to Mr. Barr in the Justice Department.

Have you had any contact with Mr. Horowitz about when he might be in front of this Committee to answer questions about the very subject we are learning about today?

Chairman NADLER. We will review any such letter.

The gentleman from—the gentlelady from Texas?

Ms. JACKSON LEE. Good morning to the witnesses, and thank you very much.

Let me just ask a general question first, Mr. Wiegmann. Having been here on the day, being here in the Congress on 9/11/2001, just commemorating the aura of that day just about a week ago, is the FISA process an important process for national security, in your opinion?

Mr. WIEGMANN. Yes, ma'am.

Ms. JACKSON LEE. Mr. Orlando?

Mr. ORLANDO. Yes, ma'am. It is a critical tool for us to disrupt threats to the United States.

Ms. JACKSON LEE. Ms. Morgan?

Ms. MORGAN. Yes, ma'am.

Ms. JACKSON LEE. Now, let me start with Mr. Wiegmann on the FISA opinions. The USA FREEDOM Act directed the Government to make all significant or novel foreign intelligence surveillance court opinions publicly available to the greatest extent practical. It is clear from the written text and from statements from Members during floor debate that this was to include opinions written before the passage of the USA FREEDOM.

Nonetheless, only a handful of opinions from the court released following passage of the bill have been published. How does the ODNI or the DOJ determine which opinions are significant or novel enough to be published?

Mr. WIEGMANN. So, in terms of how we decide what is significant and novel, the way I think about it is there are plenty of opinions that are only going to be applying ordinary legal principles to the facts, so let us say as to a particular case, deciding whether a particular individual—whether there is probable cause that they are an agent of a foreign power. There is nothing particularly novel about that exercise. It is just very fact intensive.

Not much would be released anyway if we were to release the opinion because it would only be application of facts, which are classified. So there is not much benefit to the public. So that is the type of case where we would not consider it significant or novel.

If it was, instead, some new interpretation of the act, certainly anything that involved an amicus, something about how the law applies more broadly, we would consider that to be significant and novel. Those are the opinions that we provide to this Committee and that we have an obligation under the FREEDOM Act to review for declassification.

Ms. JACKSON LEE. Do you know how many opinions have remained completely secret because of the definitions you are using?

Mr. WIEGMANN. There are certainly opinions that we would not consider significant and novel, and those opinions would not have been declassified. That is right.

Ms. JACKSON LEE. Would there be a way of securing that inasmuch as they are not significant and novel for the information of either the American people or Members of Congress?

Mr. WIEGMANN. I am sorry. I missed your question.

Ms. JACKSON LEE. Would there be a way of releasing those, even those not significant or novel for the American people or Members of Congress?

Mr. WIEGMANN. So, if they are neither significant or novel, I think the judgment of the Congress was that those are ones that we would not provide to the committees and would have no obligation to review because there also would be limited public interest, I think, in those opinions.

Ms. JACKSON LEE. We could access them, if necessary, in a classified setting?

Mr. WIEGMANN. I imagine if there was a particular opinion that the Committee wanted to see, I imagine we could have a discussion about providing that to the committee. Absolutely.

Ms. JACKSON LEE. In addition, the Government should disclose Office of Legal Counsel opinions relevant to the Government's interpreting of section 215 of USA FREEDOM Act. Is that correct?

Mr. WIEGMANN. The Government has done what with the OLC?

Ms. JACKSON LEE. Disclose Office of Legal Counsel opinions relevant to the Government's interpreting of section 215 of the USA FREEDOM Act. Is that important?

Mr. WIEGMANN. Whether they should be disclosed?

Ms. JACKSON LEE. Yes.

Mr. WIEGMANN. Again, OLC opinions, some of them are made public. Others are not. It really depends on the facts of the case and OLC's policy in a particular case as to whether it is kind of privileged advice or whether it is something that they feel they can make public. Some opinions are public, and others are not.

Ms. JACKSON LEE. Thank you.

May I go to Ms. Morgan? The NSA announced in 2018 that it received large numbers of CDRs that it should not have and that these technical irregularities began in 2015. In response, the NSA deleted every single record it collected since 2015. The agency claims it solved the problem going forward, but failed to provide any evidence of any change.

As a result, NSA announced it would purge every single record it had collected since 2015. In 2019, the New York Times published a major story reporting that the NSA stopped using this authority entirely.

What exactly were the technical irregularities, and has the NSA actually stopped the CDR program at this time? If you could answer both of those?

Finally, to Mr. Orlando, if you could—I know where we are with respect to foreign operatives—explain the value of FISA in your work, but also the necessity of some form of that with respect to domestic terrorism.

Ms. Morgan?

Ms. MORGAN. Thank you, ma'am. I will start with your second question.

The CDR program has been stopped. Last month, all of the equipment was decommissioned. We are not leveraging the CDR authority and have currently no plans to leverage it.

In terms of the technical irregularities that we experienced, we got some information, and it was still all metadata. I would like to be really clear. It was still all things like "Phone number A called phone number B at this date and time for this duration."

Some of that information was inaccurate. As such, we determined that the best course of action was to delete the records we received from the telecommunication providers.

Ms. JACKSON LEE. Mr. Orlando?

Mr. ORLANDO. Ma'am, if I understood your question correctly—

Chairman NADLER. The time of the gentlelady is expired. The witness may answer the question.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Mr. ORLANDO. Ma'am, if I understood you correctly, you wanted to understand how FISA could be used on domestic terrorism subjects?

Ms. JACKSON LEE. Whether you need an expansion or a recharacterization, let us put it that way.

Mr. ORLANDO. We can only use FISA when there is a proof of agent of foreign—

Ms. JACKSON LEE. I understand.

Mr. ORLANDO. So, if the subject is not tied to an agent of foreign power, we could not use it on a domestic terrorism subject.

Ms. JACKSON LEE. I understand that, and I was just saying you need some kind of similar, comparable situation.

Mr. ORLANDO. I couldn't comment on FBI policy, but we have other tools on criminals matters like a title III for wire surveillance that we could use. Oftentimes in domestic terrorism cases, we look for the Act of Violence, already a violation of Federal law, and some ideology about social or hate.

Ms. JACKSON LEE. Thank you.

Chairman NADLER. The time of the gentlelady has expired.

Ms. JACKSON LEE. Thank you.

Chairman NADLER. The gentleman from Texas?

Mr. GOHMERT. Thank you, Mr. Chairman.

Thank you all for being here. Thank you for your work trying to keep America safe.

Did the DOJ, FBI, or NSA during the Obama Administration consider the Russian Ambassador to be a terrorist or an agent of a terrorist organization?

Mr. WIEGMANN. I couldn't comment on that. I don't know.

Mr. ORLANDO. I can't comment on anything outside the scope of the FREEDOM Act.

Mr. GOHMERT. All right. Ms. Morgan?

Ms. MORGAN. Sir, I don't have that information.

Mr. GOHMERT. Wow. Wow. That is amazing. Because it puts us in the position, having heard that Jeff Sessions was being surveilled when he met as a Senator with an Ambassador, there were reports that, gee, we have had the Israeli Ambassador under surveillance, people that he met with.

I don't know any of these things firsthand. It is what I read in here. It gives me great concern because in my freshman term, when we debated section 206, 215, when we debated the FISA court, and then recently seen massive abuses through the FISA court, we kept being assured, no, no, no, especially in a FISA court, things like 215, we are not abusing anybody. I heard here at this hearing that 215 allows surveillance of foreigners that are not normally associated with a terrorist organization.

I just wondered if that included nations of Israel or other folks like that, and your silence speaks volumes. Looking at this provision to get access to certain business records for foreign intelligence or international terrorism investigations, I still am concerned, as I was originally, with some of the language because it allows the pursuit—and this is normally going to be in front of a FISA court, apparently—that you can go after foreign intelligence information not concerning a U.S. person.

We know that is not true because U.S. persons are constantly caught up, masked, and then, as we saw in the Obama Administration, unmasked for no good reason. Then, also—or to protect against international terrorism. Okay, well, that is subject to a term of art or clandestine intelligence activities.

I asked years ago, what does that mean? Clandestine intelligence activities. Is that like if my neighbor kind of stands behind the curtains and watch what is going on in my yard, is that clandestine gathering intelligence? I mean, how broadly can this go?

I was never really assured by the part of the law that said these things will be done under the guidelines approved by the Attorney General. Gee, we may have the Acting Attorney General indicted here soon. I would rather have those done under the law instead of some guidelines we have nothing to do with.

Let me also mention with regard to FISA, I understand you have abandoned the gathering of metadata, but as long as there is a FISA court, there can be another application and affidavit that violates the Fourth Amendment's requirement of probable cause and supported by oath or affirmation, particularly describing things to be seized. When I looked at what was disclosed of the order regarding Verizon, apparently everybody got one. Everybody complied except Qwest, and I understand the head of Qwest may be in jail.

This just says give us everything you have got on an ongoing daily basis, all the call details. There was no probable cause of anything. There was no particularity.

So, even though we may have abandoned those programs, as long as there is a FISA Court and we do not have proper safeguards for people's civil rights in the United States, then you could go right back, and we can get into a constitutional discussion on meta data, pen registers, and that kind of thing. Still, as long as we do not have reforms in the FISA Court or do away with it and go back to the old way of protecting national security, then we are going to have these kind of things come up, and we will find out about them later, and then the program can be abandoned. It sounds like we are just going to keep reauthorizing.

So, I have significant concerns, and also, I am amazed here, you get an order that allows—it says meta data between U.S. and abroad and wholly within the United States, including local telephone calls, but nothing to do with all of those in foreign countries. So, in other words, the affidavit and application must have said we are not after anything where people aren't protected by our U.S. Constitution; we are only after the stuff that is protected by the Fourth amendment of our Constitution.

So that all causes me concern. I was delighted to hear my friend from California say she wanted to work with both sides. We definitely need reforms, so you don't have to be back here and squirm-

ing because of the abuses that have occurred in the system. I really do hope we will work together to have some reforms.

I yield back.

Chairman NADLER. The gentleman yields back.

The gentleman from Tennessee.

Mr. COHEN. Thank you, Mr. Chair. I appreciate the work all of you all are doing in your agencies. What the Department of Justice does, what the FBI does, what our intelligence groups does protects our country. It is sad that they have been attacked on a regular basis over the last 2 years and people have had to question the men and women who are doing such outstanding work for us on our behalf. I think that most Americans appreciate what you are doing, and I certainly do.

I am concerned about First amendment rights, and I just want some assurances, Mr. Wiegmann, if you can help me with this. The law makes clear that when the Government seeks business records for investigations involving American citizens or permanent residents, the investigation questions cannot be conducted solely upon the basis of activities protected by the First Amendment.

How does the Department look at this, the Justice Department? Is there any kind of review conducted internally to make sure that non-First amendment factors supporting the investigations aren't just pretextual?

Mr. WIEGMANN. Thank you for that question. So, absolutely, that is a core provision in various provisions of FISA that we cannot engage in investigative activity solely on the basis of First Amendment-protected activity. Let me give you an idea of what that means.

It is a First amendment right if you want to say, "I support terrorism" or "I support al Qaeda" or ISIS, or "I think that"—

Mr. COHEN. Or "I like beer."

Mr. WIEGMANN. Right, whatever. If you want to say those things, if you want to think those things, that is your right. So, we could not get a FISA warrant or use a business records application when—solely on the basis of that type of speech.

However, if we have more than that, if the person is saying those things and they are also in touch with people in ISIS in Syria or in touch with people in al Qaeda in Afghanistan, and they are having communications, we can still consider the fact that they have made these other statements, because that gives us context to evaluate whether this person is an agent of a foreign power.

So, you can see how speech in and of itself that might be First amendment protected can be combined with other speech or other conduct and paint an entire picture in which you come up with a conclusion that someone is an agent of a foreign power or is a valid target.

Does that answer your question?

Mr. COHEN. Sufficiently. Thank you. Thank you.

A lot of people have issues or concerns about minority communities being targeted. Have you or any of your colleagues here analyzed whether section 215 has disproportionately been used on specific minority groups, Muslims, in particular, Hispanics, border communities? How would you go about assessing that? Is anything being done to make sure there is not a disproportionate impact?

Mr. WIEGMANN. So, once again, it is very similar. We, the FBI—and I will let Mike also address this—cannot initiate any investigative activity, including under FISA, solely on the basis of someone's race, religion, gender, national origin, *et cetera*. It is the same kind of "solely" provision, though. So if, let us say, we had information indicating that someone of German nationality was coming to the United States to engage in a terrorist attack and that may be a bit of information that we consider together with other pieces of information to consider whether someone was properly targetable, if that explains it.

Mr. COHEN. Thank you, sir. Can you commit, one of your groups, that you will do a disproportionate impact audit for us?

Mr. WIEGMANN. I can certainly take that back.

Mr. ORLANDO. I could take that back to the FBI as well. Just to echo some of his comments, we can't open a case on anyone based on First Amendment-protected activity, race, ethnicity, or religious groups. We look at the activities of the individual, and that is how we make decisions about opening cases, and then the probable cause to move towards a FISA.

Mr. COHEN. Thank you. Can you tell us, when FISA was first passed, which I guess was right after 9/11, am I correct?

Mr. WIEGMANN. It was actually—

Mr. COHEN. There were changes after 9/11.

Mr. WIEGMANN. There were changes. It was enacted in 1978.

Mr. COHEN. Yeah, the changes were pretty strong. It had an acronym about—Bush gave it, whatever.

Mr. WIEGMANN. The PATRIOT Act.

Mr. COHEN. PATRIOT Act, yeah, thank you. A lot of people reacted adversely to it. Can you assure me and some of my liberal friends who had those concerns that there have been quite a few amendments to take care of some of the concerns that originally arose?

Mr. WIEGMANN. There have been certainly, with respect to the expiring authorities, a number of amendments over the years. There has been a lot of oversight over the years, both congressional oversight, the court, the executive branch. From my perspective, we have a very robust system for making sure these authorities are used properly.

Mr. COHEN. Thank you. Just let me close. It appears that some on the other side have got a problem with a lot of things that have gone on in law enforcement. I read all those FISA applications in the Carter Page case and saw nothing wrong with any of them. I think it was—all the information was given to the Court concerning the fact that the dossier that was there was not the Russian Government. It was a British official, so it was not Russia. It was started by the Republicans, I think. Regardless of that, that was only a small factor, and there was lots of information there to protect our country from Russian interference. I thank the Justice Department and the FBI for their work, and the security folk. Too much has been put on you, and the biggest threat to you is a President who does not tell the truth and has access to information and the ability to counteract the good work that you are doing. So keep doing your good work.

I yield back the balance of my time.

Chairman NADLER. The gentleman yields back.

The gentleman from Texas is recognized.

Mr. RATCLIFFE. Thank you, Chairman.

As a former U.S. Attorney, it was and still is my opinion that FISA is an important tool in the fight against international terrorism. I think it is estimated that 25 percent of our actionable intelligence on foreign terrorists comes from FISA authorities like section 702, which isn't up for reauthorization, but my point is that, properly used, reauthorization of certain FISA authorities should be noncontroversial and should be bipartisan.

The problem is that many of us, as has been pointed out, including those of us with access to classified information, have seen what appear to be egregious abuses and misuses of FISA authorities and corresponding misrepresentations before the Foreign Intelligence Surveillance Court itself, specifically as it pertains to Obama Administration DOJ and FBI officials in securing a FISA order on at least one U.S. citizen back in October of 2016 named Carter Page.

Many of us do believe that the Obama Justice Department verified an unverifiable dossier that was funded by the Democratic Party to secure an order allowing for the surveillance of that former Trump campaign associate, Mr. Page. Many of us also believe that the Obama Justice Department had exculpatory evidence on the issue of probable cause that was not provided to the FISA Court, at least not provided to the Court during the pendency of the FISA order itself.

Earlier this morning, Chairman said that he didn't see any evidence of FISA abuse as it pertains to Carter Page. You just heard Mr. Cohen say the same thing. Democrats generally have expressed that opinion. The former FBI Director, former Director Comey, says the idea of FISA abuse is nonsense as it pertains to Carter Page. I and many of my colleagues disagree with that. I will just leave it at the Inspector General has written a report, and we will see who is right, and we will see who is wrong. I am afraid, unfortunately, that the Inspector General is going to find that folks on my side of the aisle are right, that FISA procedures were abused and that they were not followed and will offer recommendations to correct that. Again, we will see.

So, I want to use my time to focus a little bit on process, and let me start out by just asking: Do any special rules exist when submitting a FISA application to surveil or spy upon a political campaign or one of its associates? Anyone.

Mr. ORLANDO. As I have stated earlier, we open cases based on specific and articulable facts that they are agents of foreign powers. I can't comment on anything outside the scope of the FREEDOM Act today.

Mr. RATCLIFFE. Anyone? Special rules for surveiling a political campaign?

Mr. WIEGMANN. I am not familiar with it, to be honest with you, sir. I can't say one way or the other.

Mr. RATCLIFFE. Okay. So let us then use the existing framework that we know of. When the Government is presenting a case with respect to a U.S. person like Carter Page, the FBI is required to

verify to the Foreign Intelligence Surveillance Court, or FISC, that that evidence is verified. Correct?

Mr. ORLANDO. When we draft an application, we have a Woods file that contains supporting documents to back up the facts.

Mr. RATCLIFFE. Does the Department of Justice—are they required to disclose to the Foreign Intelligence Surveillance Court any exculpatory evidence? In criminal cases, we have what is called the "Brady requirement" to disclose exculpatory information. Does that something Brady-like apply before the FISA Court?

Mr. WIEGMAN. Again, as I was saying earlier, it is not Brady because that is a principle in criminal law in that context. But, yes, my understanding at least, and subject to getting back to you on this question, but I think the answer is, yes, we do try to provide the full picture to the Court when applying for a FISA warrant. So that means evidence both indicting that the person—that there is probable cause that the person is an agent of a foreign power and information that would suggest to the contrary.

Mr. RATCLIFFE. Okay. So in the case of Carter Page, if all the Court heard was the arguments of the Government seeking a warrant, no counterarguments presented questioning the motivations of the funders of the Steele dossier, no cross-examination about the veracity of the dossier itself or about the credibility of the dossier's author, Mr. Christopher Steele, what safeguards are there in the FISA process currently to make sure that those obligations are met? What as a practical matter would prevent the appointment of an attorney ad litem to represent the interests of a target of a FISA application, provided you could meet the security clearance requirements, maybe by taking someone from the Justice Department's Civil Rights Division?

Mr. WIEGMANN. So, if I understand your question, I guess your question is whether we should—

Chairman NADLER. The gentleman's time has expired. The witness may answer the question.

Mr. WIEGMANN. Your question is whether we should have something like an amicus or something like to represent the targets of FISA applications? Is that the—is that your question?

Mr. RATCLIFFE. To be able to probe the arguments that the Government is making to take the extraordinary measure of surveiling a U.S. citizen.

Mr. WIEGMANN. So, I guess one thing I would say is we have to remember that FISA is really in the national security world the same thing, as I am sure you are familiar with as an ex-U.S. Attorney, as a title III wiretap, which is really the same type of thing, and we don't have any amicus or any other participation in that context. So, I am not sure why it would be necessary or appropriate to have an additional lawyer in this context. We do have *ex parte* proceedings in the ordinary course when we are doing wiretaps of a drug dealer or an organized crime figure, *et cetera*. I am not sure I see a need for having an amicus in the same situation when it is a spy or a terrorist.

Chairman NADLER. The time of the gentleman has expired.

The gentleman from Georgia.

Mr. JOHNSON of Georgia. Thank you, Mr. Chairman. I am ashamed that in an oversight hearing you all have to be subjected

to political fake news that is being trafficked in by Members of the Republican Caucus on this Committee.

Several days before President Trump was inaugurated, he compared intelligence officials such as yourselves as "Nazis." Then the day after he was inaugurated, he paid a visit to CIA headquarters out in Langley, Virginia, and he stood in front of the hallowed ground of the memorial wall where the names of CIA operatives, men and women, American citizens, have given—are commemorated. Those are people who have given their lives, the untold numbers. We do not know how many. That is what that wall commemorates, and it is hallowed ground out there. Instead of, while he was there, speaking about the sacrifice of those brave men and women who have given their lives to protect us, the President talked about his crowd size at the Inauguration, and he bragged about winning the election. Since then, he has continued to do everything he can to destabilize public opinion about our intelligence professionals and the work that you do, and you have had to work through that. So, I appreciate you coming here today. I appreciate you continuing to do your work without political bent of mind but strictly and single-mindedly for the protection of the American people, and I thank you for that. This hearing is about oversight and should not be about politics. As a member of the legislative branch, I am sorry. I want to apologize to all of you all, all of your professionals who are here today, for having to sit through this tirade that comes from the other side.

Now, Ms. Morgan, you mentioned that the CDR Program has been suspended, and NSA is tasked with execution of the CDR Program. Correct?

Ms. MORGAN. NSA operated the CDR Program.

Mr. JOHNSON of Georgia. Has the CDR Program or that authority under the program been used in any way, the meta data collected under the program, has it been accessed for any purpose since the program was suspended?

Ms. MORGAN. Sir, we deleted the records associated—that we got from the telecommunication providers, so those records no longer are there to be accessed.

Mr. JOHNSON of Georgia. All right. Thank you. And while it was being collected, was that information subject to being shared with immigration enforcement authorities?

Ms. MORGAN. Sir, the information that we collected under the CDR provision was accessible to analysts who are trained in how to handle that particular data and the rules associated with that data. Those analysts would look at the data, and if they had foreign intelligence insights to share based on that, they would report it through authorized channels to authorize personnel.

Mr. JOHNSON of Georgia. That would have been officials also involved in immigration enforcement?

Ms. MORGAN. Sir, I am not certain about that. They would report it to an authorized distro, to individuals who were authorized to receive that foreign intelligence information.

Mr. JOHNSON of Georgia. Thank you.

Now, Mr. Orlando, the call detail records provision says that these records cannot include cell sites or GPS information, but other parts of the law governing the types of business record don't

have that express prohibition. So what I want to know is: Does the Government collect geolocation information under section 215?

Mr. ORLANDO. I am going to defer that question over to my colleague at DOJ. He is better suited to answer legal and authority questions.

Mr. JOHNSON of Georgia. Yes, sir. Mr. Wiegmann?

Mr. WIEGMANN. So, as I think I mentioned earlier, there are some—there can be some Fourth amendment issues in that area, and to really answer your question, I think I would prefer to answer that in classified session.

Mr. JOHNSON of Georgia. Thank you. With that, I will yield back.

Chairman NADLER. The gentleman yields back.

The gentleman from Arizona.

Mr. BIGGS. Thank you, Mr. Chairman.

So, I know this has been discussed this morning to some extent and I want to approach this maybe from a slightly different angle. In light of Carpenter, do you believe you have the authority under 215 to obtain cell site location information from providers?

Mr. WIEGMANN. So, again, I would prefer to get into that—I am happy to give you that information, Congressman. I would just like to do that in a classified briefing.

Mr. BIGGS. Okay. This may elicit the same response, but has NSA or DOJ issued any guidance interpreting section 215 in light of Carpenter?

Mr. WIEGMANN. No.

Mr. BIGGS. No guidance, NSA?

Ms. MORGAN. Not to my knowledge.

Mr. BIGGS. Okay. Has DOJ ever notified a criminal defendant that information in his or her case was obtained through a section 215 order?

Mr. WIEGMANN. No. It is not required by law. There is no provision for that.

Mr. BIGGS. Why is the number of accounts impacted so substantial given the number of targets? In 2018, the Government collected information, 214,816 unique accounts, if it had only 60 surveillance targets?

Ms. MORGAN. Sir, just to clarify, I assume you are referring to the numbers that were reported in the—for the NSA CDR?

Mr. BIGGS. Yes.

Ms. MORGAN. Okay, sir. So, I think it is—two things I think are important when you think about those numbers. One is putting those numbers into context. So, every day in the United States, there is billions of telephone calls made a day, which can generate multiple records. We had about 500 million over the course of a year.

The other thing I would want to highlight is that when we get data, when we were getting data under the program that is now suspended, we were authorized to get historical data that the telecommunication providers held in addition to ongoing data for the period of the court order.

Additionally, I would like to highlight that under the CDR Program, which, again, we are no longer using, we are authorized to get up to two hops from the—

Mr. BIGGS. Right.

Ms. MORGAN. So that, as you would imagine, will expand your numbers exponentially.

Mr. BIGGS. So, does the NSA believe it has the authority to restart the program?

Ms. MORGAN. Sir, currently we believe that authority exists.

Mr. BIGGS. Okay. Do you have the authority, collection authority that is replicated under any authorization or any other authority? In other words, is there some other legal authority that you think that allows you to get the same information?

Ms. MORGAN. We don't have another legal authority that would allow us to reinstate this existing—the program as it existed.

Mr. BIGGS. I am not following that. So, let me get this back. If I understand, the answer to the first question is you believe that you do have the authority to restart the program; you don't need new authority to restart.

Ms. MORGAN. Yes, sir.

Mr. BIGGS. If you don't restart that program, is there some other legal authority that you can use to garner the same information?

Ms. MORGAN. There is no other legal authority whereby we could establish the program that we recently shut down.

Mr. BIGGS. Okay. Very good. Thank you.

So, a FISA order on a U.S. citizen, Carter Page, was divulged to the Washington Post, and I think you answered this earlier. Has anyone been held accountable for this illegal disclosure? There has been no Woods review? You don't know whether there has or not?

Mr. WIEGMANN. I can't comment on that in any way. I don't know the answer.

Mr. BIGGS. Okay. So, I want to make sure I understand something. Mr. Orlando, I thought you said—and I jotted it down. I am not going to quote it because I am sure I messed it up, and I am just asking for clarification here. I thought you might have said something to the effect that you use FISA authority to cultivate obtaining probable cause. Is that a fair characterization, or did you say anything like that at all?

Mr. ORLANDO. We use some of the business records and other authorities to develop probable cause to support a FISA.

Mr. BIGGS. All right. So, you are using business record authority, okay. We have indicated that you can't—you don't know whether a Woods review was performed on the Carter Page FISA application to determine whether each alleged fact was substantiated. Can a regular news article server as—serve as underlying evidence in a Woods file to verify the accuracy of a FISA application?

Mr. ORLANDO. If I understand your question correctly, you are asking is a news article appropriate to be used? If information was pulled from the newspaper article, it would have to be included in the Woods file.

Mr. BIGGS. So, the answer is yes?

Mr. ORLANDO. Yes. There is often a lot of other facts that are put into that file that builds up the totality of your probable cause.

Mr. BIGGS. Okay. With that, my time has expired. Thank you, Mr. Chairman. Thank you, Members of the panel.

Chairman NADLER. The gentleman yields back.

The gentleman from Rhode Island.

Mr. CICILLINE. Thank you, Mr. Chairman. Thank you to our witnesses for your testimony and for your service to our country.

I think we are all trying to balance the very important constitutional values that are the bedrock of our democracy with, of course, your important responsibilities to keep Americans safe, and FISA attempts to strike that balance.

I would like to focus my questions on the role of an adversarial process in that particular—and, Mr. Wiegmann, I will begin with you. Significant reform in the USA FREEDOM Act was a requirement that the FISA Court appoint an *amicus curiae* to argue the other side of the case as presenting novel or significant interpretations of law. The annual report on the FISA Court's activities for 2018 issued by the Administrative Office of U.S. Courts states that an amicus was appointed on nine occasions last year. Is that right?

Mr. WIEGMANN. I don't know that exact number, but it sounds in the right ballpark anyway.

Mr. CICILLINE. Then the report for 2017 states that no amicus were appointed at all that year, but it also says something kind of odd. It says on three occasions the FISA Court told the Government that it was considering appointing an amicus because the proposed application raised novel or significant questions. Then the Government either withdrew the applications or modified them in a way that apparently convinced the Court not to appoint an amicus.

Understanding that this is an unclassified setting, can you explain as best you can what happened in those three incidents?

Mr. WIEGMANN. So, I don't know in those particular three incidents, but I can tell you that there is a process where—it is a little bit unusual, that you wouldn't see in a regular criminal matter—where we provide read copies to the Court in advance. So, this is essentially a draft application, and there is a give-and-take sometimes between the judges and their assistants, their staff, and attorneys. In light of the exchanges that occur in that process, sometimes applications are withdrawn altogether. Other times they can be modified in ways that, again, may mean that the case is less significant or novel and the Court might—

Mr. CICILLINE. Can you share maybe in writing what the particular circumstances were of those three? There was also, I believe, in 2018 something similar happened. I am wondering if you could give a little more context of what the actual circumstances were?

Mr. WIEGMANN. I can certainly take that back and see if we can get you that information.

Mr. CICILLINE. Thank you.

The law also requires the FISA Court and the Government to give those who file *amicus curiae* access to all materials deemed relevant to their duties, such as legal precedents, applications, or other supporting materials. As far as you are aware, have any amici ever been denied access to information they thought was relevant to their duties?

Mr. WIEGMANN. Not that I am aware of.

Mr. CICILLINE. Have they ever been denied the ability to consult with other individuals for assistance in preparing their cases?

Mr. WIEGMANN. Again, not that I am aware of.

Mr. CICILLINE. If the *amicus curiae* believes the FISA Court has made a decision in error, do they have the ability to appeal or otherwise notify the FISA Court of review?

Mr. WIEGMANN. You are asking a good question. I would have to look back at the law on that. There is an appellate mechanism. My only hesitation is I am not sure if the amicus, the way that we constructed the law, actually has standing to bring the appeal or whether it is done in a different fashion. I could get you—it is written in—there is an appeal mechanism, and so I would just have to get into that issue. They certainly can participate in appeals when an appeal is brought, so I would have to get back to you as to how it works exactly. It is a slightly different mechanism than that, but there is a mechanism—there is a mechanism for appeal.

Mr. CICILLINE. It is my understanding that only a handful of opinions from the Court have been published. How does the NSA or the DOJ determine which opinions are significant or novel enough to be published?

Mr. WIEGMANN. Again, as I mentioned earlier, it is an evaluation—it is a case-by-case evaluation. There are many—the vast bulk of FISA matters are routine. You are applying the law to the facts and determining whether there is probable cause to target a particular individual. Those would be routine. There is a much smaller number that raise new significant issues of whether, let us say, a particular type of data could be collected or new issues, new expansions of an authority. And so we are evaluating that on a case-by-case basis and determining which—

Mr. CICILLINE. Yeah, what I am interested to know is how many opinions that fit that definition of "significant or novel" but are not published.

Mr. WIEGMANN. Well, we have to provide all of those to the committee. Under the FREEDOM Act, all of those must be provided. Then we also have to undertake, I believe, a declassification review to determine whether we can redact and release any of those significant or novel opinions. So, that is in the law since 2015 that we have to do that.

Mr. CICILLINE. All of those declassification reviews are current?

Mr. WIEGMANN. Yeah, I mean, there may be some that are a work in progress. In other words, there may be some that are ongoing, that haven't been done yet, but that they would be under review.

Mr. CICILLINE. My final question, Mr. Wiegmann, is: Has the Department of Justice notified all criminal defendants who are being prosecuted based on evidence derived from the use of section 215? You are required to do it, obviously, for prosecutions with evidence from 702. But, I would like to know whether you do it with respect to 215—if you do not, why not? —and whether you will commit to such notification. Finally, would there be a problem if Congress were to amend section 215 to require notice to a criminal defendant in the same way we do under section 702?

Mr. WIEGMANN. Yeah, so we don't provide notice to criminal defendants but for use of information under 215. Other provisions of FISA, title I, title III, 702, Congress has built in a mechanism whereby we would give notice if we intend to use information that is obtained or derived from that authority in a criminal case

against an aggrieved person. So, there is no such provision currently in the law for section 215. The reason for that, again, I think is that 215 is, again, essentially like a grand jury subpoena. It is just an authority to allow us to collect third-party business records in which there is no Fourth amendment protected interest. Generally, we associate notice and suppression mechanisms with your ability to challenge, the invasion of a constitutionally protected privacy interest. That is generally not done in the law in other contexts with respect to third-party business records. There is no ability, for example, to challenge information derived from a grand jury subpoena either, and so that is the model that is incorporated into FISA modeled on the criminal authorities.

Mr. CICILLINE. Thank you. I yield back, Mr. Chairman.

Chairman NADLER. The gentleman yields back.

The gentleman from Louisiana.

Mr. JOHNSON of Louisiana. Thank you, Mr. Chairman. Thanks to each of you for being here and for your service to the country.

Mr. Wiegmann, just a few questions for you regarding the constitutional implications of all this. Does the Fourth Amendment's protection against unreasonable search and seizure apply to business records that could be obtained under section 215 of the PATRIOT Act?

Mr. WIEGMANN. No.

Mr. JOHNSON of Louisiana. So, a person does not have a reasonable expectation of privacy in third-party business records then. Is that right?,

Mr. WIEGMANN. Yes.

Mr. JOHNSON of Louisiana. Is it true that a 215 order provides greater privacy protection than a grand jury or administrative subpoena which can be used to obtain the same types of business records in a criminal investigation without prior court approval?

Mr. WIEGMANN. That is correct. Insofar as, for example, most grand jury subpoenas can be issued by an Assistant U.S. Attorney, here we have to go through court and make a specific showing and so forth, which we would not have to do in a criminal case. So, it is more protection, not less.

Mr. JOHNSON of Louisiana. I got it. If the Fourth amendment applies to foreign countries, do other American protections under the Bill of Rights apply, like, for example, the Second Amendment? Or what about the Due Process Clause?

Mr. WIEGMANN. I am not sure if I understand your question.

Mr. JOHNSON of Louisiana. Well, strike that. Let me give you some foundation for it.

In a domestic title III wiretap, an individual who is not under suspicion may be monitored because they receive a phone call from someone who is the target of the title II wiretap. Traditionally, those calls are subject to minimization procedures. Is the same true for the collection of content under FISA?

Mr. WIEGMANN. Yes. It operates differently under title III. In the criminal context, it is real-time minimization, and by that I mean they are turning on and off the wiretap during the conversation, depending on whether they are collecting information that is relevant to their investigation or not.

In FISA, it is done after the fact. Okay? So, if you receive that U.S. person information, if it is a foreign target, they are in communication with a U.S. person, then the minimization process—there are procedures that are in place to try to minimize the collection, retention, *et cetera*, of U.S. person information. That process is done post hoc. When you are thinking about the information that you have and you are disseminating it within the intelligence community, that is the stage at which they are doing the minimization in the FISA context. So, that is the big difference between title III and FISA in that regard.

Mr. JOHNSON of Louisiana. In that process, the on-off procedure, as you describe it, there is obviously an inevitable amount of subjectivity that goes into thate is the kind of thing that makes people nervous, I guess. We have to at the end of the day, trust that those who have that authority are flipping the switch at the right times. But, I know that is an impossible thing to—I do not how to speak to that.

Mr. WIEGMANN. Again, just to be clear, that is in an ordinary criminal wiretap. That is what they are doing every day and have done for many years.

Mr. JOHNSON of Louisiana. Right. Is legally obtained information eligible for use in other intelligence activities? So, can evidence obtained through intelligence collection be used in a criminal prosecution and under what circumstance?

Mr. WIEGMANN. Yes, it can be, assuming that they get approval from the Attorney General to use it, we get the approval from the intelligence community. It can as a general matter be used in a criminal case.

Mr. JOHNSON of Louisiana. All right. I am going to yield back, Mr. Chairman.

Chairman NADLER. The gentleman yields back.

The gentleman from California, Mr. Lieu.

Mr. LIEU. Thank you, Mr. Chair. Thank you all for your public service.

I am going to start by simply correcting some misstatements of my Republican colleagues related to the FBI's counterterrorism investigation and the Carter Page warrants. Here are the facts.

The FBI's counterterrorism investigation included in part the Carter Page FISA warrants. That entire investigation helped lead to the Mueller Special Counsel investigation. Special Counsel Mueller's investigation resulted in 34 individuals being indicted or companies being indicted, of which 8 have been convicted or pled guilty of violating American criminal laws. Volume I of the Mueller report showed that the Russians engaged in a sweeping and systematic attack on elections. It showed that the Trump campaign knew about this attack. They welcomed it. They gave internal polling data to the Russians, and then they planned their campaign strategy around that Russian attack. We should be thanking the FBI, not trashing them for getting this information out to the American people. Those are the facts.

Now, I have questions about the Call Detail Records Program, and my first question is: Unlike FISA warrants and so on, none of this goes through a warrant process. Is that correct?

Ms. MORGAN. Sir, if I might just explain how the program worked when we—

Mr. LIEU. Sure.

Ms. MORGAN. So just as an example, an NSA analyst, they have a phone number, say, and they have a reasonable, articulable suspicion that that phone number is used by a foreign power engaged in international terrorism. We work at the NSA with our DOJ and our FBI colleagues to draft an application to the FISA Court or the Attorney General in an emergency situation. The FISA Court reviews that information we present to see if we have met the standard, reasonable, articulable suspicion. If the FISA Court approves that application, then the telecommunication providers are compelled to provide us with the meta data associated with that phone number.

So there is a court—

Mr. LIEU. Before that—before the purge, you had all these records collected without a warrant. Correct?

Ms. MORGAN. Sir, before the purge, the records that we did collect were a result of going through that FISA process. However, some of the records that we received had technical irregularities with them which resulted in the purge.

Mr. LIEU. So, you had hundreds of thousands of records that went through the FISA process?

Ms. MORGAN. The FISA Court approved the specific selection term. The records that we get that are associated with that term come from the telecommunication providers.

Mr. LIEU. So, one term could result in a lot of records.

Ms. MORGAN. Yes, sir, because as you likely know, we are able to get historical records associated with that phone number and prospective records for as long as the order is in place. We are also authorized to get what we call "two hops out" from that original phone number.

Mr. LIEU. Can you explain what that means to the American people?

Ms. MORGAN. Absolutely, sir. So, if the Court approves a phone—say my phone number is associated with international terrorism, and agent of a foreign power, going through the court process, they are approved, I am authorized to get meta data records of other phone numbers that have been in contact with my phone number. So, for example, if I am in contact with Mr. Orlando, I am authorized to get that. I am also authorized to get the phone numbers that were in contact with Mr. Orlando's phone number. So, if Mr. Orlando was in contact with Mr. Wiegmann, I would be authorized to get that, and we call that "two hops." I am authorized to get retrospectively as well as ongoing for the duration of the court order.

Mr. LIEU. All right. Thank you.

Earlier it was stated that part of that also would include driver's license information?

Mr. WIEGMANN. So, again, to be clear, that is traditional use of 215. What was just being described is the CDR Program, so the CDR Program has nothing to do with driver's licenses, *et cetera*. So, there is a separate—the regular, ordinary uses of business records allows you to get things like driver's license records, hotel records.

That is more targeted. That is based on the relevance of those particular records in a particular investigation.

Mr. LIEU. Would that also include images, like the picture on the driver's license as well?

Mr. ORLANDO. I am not sure. We can go back and—

Mr. LIEU. You will let us know?

Mr. ORLANDO. We will let you know.

Mr. WIEGMANN. I don't actually know.

Mr. LIEU. So, thank you for your answers. My personal view is that this CDR Program, also known as the meta data program, to me it does violate the privacy. The Government could tell, for example, just from meta data whether a person called a suicide prevention hotline or Alcoholics Anonymous or a sex chat line or a bankruptcy lawyer or a divorce lawyer. So to me, that is just too much information for the Government to have. In addition, with the two hops, I think it captures too many people. So, without a greater showing of why this system is efficient or has resulted in actual, concrete advantage to the Government, I am unlikely to support its reauthorization.

With that, I yield back.

Chairman NADLER. The gentleman yields back.

The gentleman from North Dakota.

Mr. ARMSTRONG. Thank you, Mr. Chairman. I just want to say I have never worked with the NSA because I was a lawyer in North Dakota, but I have worked with DOJ and FBI a lot in my private career, and I appreciate everything you all do. What I have always found is the very best agents, the very best lawyers are very cognizant of where the line is and what they can do and what they can't do. They also, the best and most aggressive ones, particularly, I am assuming in this area, will push the envelope in order to do something because that is your job. I don't discount that. I think that is actually appropriate. I think that is why it is our job and the Court's job to set where that wall is. So you can keep running into brick walls and doing what you are doing to keep our country safe.

I do want to go back to something that Mr. Ratcliffe was talking about, and we were doing the context between this gathering—or this type of information and criminal cases, and one of the things that was stated was that this happens a lot in criminal cases, *ex parte*, wiretaps, all of that. I think one of the fundamental differences that we have is eventually I get it all as the defense attorney. In a straightforward criminal case, I get it all. I get to go to Brady. I get to go to Carpenter. I get to go to all of those things. That is what I think we miss sometimes in this and how we deal with it.

I know the difference between Carpenter and essential real-time tracking of your actual location versus business record exceptions, and this is a perfect example of where we get to that.

Do you know how many FISA-derived informations have been used in criminal—or how many criminal prosecutions have come out of FISA warrants?

Mr. WIEGMANN. I am not sure what you mean by "come out of" the FISA warrant. If you mean how many cases have we used FISA information in a criminal case, including title I FISA, title III

FISA? So there have been many of those cases since the late 1970s when FISA was first adopted. I mean, it is not a massive number, but I couldn't—I wouldn't have an exact count of how many there have been, but there have been over the years many different cases.

Mr. ARMSTRONG. I would just like—outside of everything, I have never wanted a half-hour longer in my life to ask questions, but so—and how do you transition the intelligence gathering? I mean, we have talked about Brady, and it is not the same, and I understand all of those things. When you get into a criminal case—we always have a saying, right? Hard cases make bad law. There is back-and-forth going on about the Carter Page case and all of that. The problem with a lot of this is we only hear about the hard cases. We don't hear about a lot of other things. So, I am all over the place because I have so many questions I want to ask.

How does the Woods review work?

Mr. WIEGMANN. I will let Mike answer that.

Mr. ORLANDO. Sir, if I could go back to your original question and answer that.

Mr. ARMSTRONG. Yeah.

Mr. ORLANDO. So, an espionage case is a good example—oftentimes we use FISA to build that case, and then we bring that to a criminal conclusion. As we build that case, we make sure that the FISA, the information that is there that we have to turn over that is relevant to that case, gets declassified to be turned over to the defendant.

Mr. ARMSTRONG. I have a question. Have you ever found existing criminal activity unrelated to what you were dealing with that has been turned over to law enforcement?

Mr. ORLANDO. I don't recall.

Mr. ARMSTRONG. A terrorist talking to a drug dealer would be how I would—I mean, just that specific fact pattern.

Mr. ORLANDO. I don't have any specific background on that. Mr. Wiegmann might have some on that.

Mr. WIEGMANN. I would have to get back to you and see how often that has come up.

Mr. ARMSTRONG. That is where I think the conflict comes in for people who are not naive and understand how we want to keep our country safe but actually really do care about how the Due Process Clause and civil liberties apply once we end up in those situations.

Mr. WIEGMANN. Just to be clear, again, if we are using that FISA, the product of that FISA in a criminal case, we have an obligation to give notice to the criminal defendant. They have then the ability to challenge the use of that FISA information in court. There is a process that is all set up in the statute, and that has been done many times, again, in these cases, typically terrorism cases, espionage cases, and the like.

Mr. ORLANDO. In regards to the Woods process, the agent starts drafting an application. Once he is complete, he sits down with the supervisor. They review it together, and every fact he has to be able to show the supervisor where he got that information from. All that material goes into a book for review.

Mr. ARMSTRONG. This goes back to what several people—Mr. Cicilline and Mr. Ratcliffe were talking about. We had said the

amicus attorneys get all relevant legal information. I think some of us would be more—I don't care if they have the top classified clearance that exists in the world, but what would be the problem with having somebody in—an amicus lawyer in all of these hearings at their onset?

Mr. WIEGMANN. So, this was something that was considered back in 2015, and our judgment at that time, and I think it remains our judgment today, is that that would really slow down and bog down the process in the FISA Court. If you had an amicus participating and every FISA application was an adversary proceeding, certainly if we had that in the title III context where we are doing ordinary criminal wiretaps, having an adversary proceeding in every application would make the process untenable.

Mr. ARMSTRONG. A follow-up? Thank you. I don't necessarily see the oversight part of this that I would be looking at is I don't even—I don't want them to have all relevant information. I want them to have it all and be able to review it and deal with those. I don't necessarily think it would potentially have to be adversarial in the hearing. I would just want them to be able to deal with that, because the consequences for withholding information on those types of issues really only come to bear if somebody finds it out, which is typically very challenging when there is only one part of this process being presented. So, there are potential ways to do this that doesn't slow it down, that also holds people accountable for making sure it is being done correctly.

With that, I yield back.

Chairman NADLER. The gentleman yields back.

The gentlelady from Washington.

Ms. JAYAPAL. Thank you, Mr. Chairman. Thank you all for being here.

You have heard on a bipartisan basis that we all have concerns about how mass surveillance is used in the United States, and particularly after the PATRIOT Act, we tried to address some of those things. There are still issues that remain on the table as we look at reauthorization.

So, I wanted to go to the CDRs, and just so that the American people understand this, while the program has been suspended, my understanding is that the Administration has asked for that to continue to be part of the reauthorization. Is that correct, Ms. Morgan?

Ms. MORGAN. Yes, ma'am.

Ms. JAYAPAL. So, just so people understand how much information is being collected, according to the Office of the Director of National Intelligence 2019 Statistical Transparency Report, the NSA collected call records based on 11 targets in calendar year 2018. Is that correct?

Ms. MORGAN. Ma'am, I don't have the report in front of me, but—

Ms. JAYAPAL. It is page 28 of the report. According to that same report, with just 11 targets—just 11 targets—the NSA collected 434,238,500—excuse me, 434,238,543 call records. Does that sound—I know you don't have the report in front of you. It is quoted from the report.

Ms. MORGAN. Ma'am, that sounds accurate to me.

Ms. JAYAPAL. Okay. So, I think the American people need to understand that when one record is collected, one target is collected, that means you are collecting enormous amounts of call records with just that one target. It is a shocking amount of records, and I don't think that the vast majority of the American people understand that.

So now going to section 215, as part of the broader surveillance authorized by section 215, can the NSA obtain people's medical records?

Ms. MORGAN. Ma'am, if I could just clarify.

Ms. JAYAPAL. Of course.

Ms. MORGAN. So, the components that we use that we are talking about today is really the CDR provision from an NSA perspective. So, I would defer to my colleagues to speak to traditional uses of the—

Ms. JAYAPAL. Sure. We are moving to broader 215, so, Mr. Wiegmann, if you want to address that?

Mr. WIEGMANN. I don't know if—I am not aware of it having been used ever to get medical records. I mean—

Ms. JAYAPAL. But, it could be? The way the provision is written, the way that section 215 is written, could it be used to obtain medical records? It can be used to obtain driver's licenses.

Mr. ORLANDO. I am not aware of us ever seeking it for medical records. I would say the circumstances that I can think of us wanting that would be very limited—

Ms. JAYAPAL. But, there is nothing in 215 currently that prevents us from doing that. You are just saying it hasn't been used before. It could be. Is that correct?

Mr. ORLANDO. I think we would have to look at the version closely to give you a—

Ms. JAYAPAL. Okay. How about tax returns? Do you collect tax returns from millions of—hundreds of millions of Americans?

Mr. WIEGMANN. We certainly couldn't get it for hundreds of millions. You have to show in each case with the statement of facts that these individual records are relevant to an authorized investigation of counterterrorism or for counterintelligence purposes for a U.S. person. So, that is going to limit it dramatically. You are not going to be able to do that. You also have to use a specific selection term now because Congress put that in in 2015. So, you can't do bulk collection under 2015 at this stage. There is no possibility of collecting hundreds of millions of health records. Tax records, I know, is—

Ms. JAYAPAL. Thank you. Thank you for that clarification. You can collect—you could potentially collect it, though, but perhaps not with the scale that I mentioned with—

Mr. WIEGMANN. Right. So, the law specifically mentions tax records and says in the case of an application for an order requiring, let us say, book sale records, firearms sales, and then tax return records—or medical records, so medical records are also contemplated in the statute—then that application has to go to a higher-level review. So, that is the Director of the FBI, the Deputy Director, and I think the EAD, the Executive Assistant Director.

So, to answer your question, the statute does contemplate the possibility of getting medical records or tax records, but recognizing

the sensitivity, particularly of those types of records, they are elevated for particularly senior review. I am just saying that I personally am not aware of whether we have ever done that in a—the connection of a medical or tax record to a terrorism investigation or counterintelligence is, I guess, unlikely, but it is possible.

Ms. JAYAPAL. Then you might be supportive of excluding those kinds of records?

Mr. WIEGMANN. I don't think that we like to exclude because you never know whether—if those records meet the standard and they are relevant in an authorized counterterrorism or counterintelligence investigation, then—

Ms. JAYAPAL. Well, let me just say, I am hearing you, but I am deeply concerned about the kinds of information that we collect. And Ms. Morgan, you mentioned earlier that Chairman's questions were not the right standard to assess whether or not a program was effective. At some point, perhaps—I have another question to get through, so—and I see my time has expired, but maybe at some point you could provide us with what matrix are reasonable, because I think the problem that we are dealing with is we are trying to strike the right balance of maintaining security, of course, but we have to respect these bedrock values of privacy and civil liberties protections. When we authorized this and we see what happened with the CDRs, I think that is just an indication of the challenges that we face.

Thank you, Mr. Chairman. I yield back.

Chairman NADLER. The gentlelady yields back.

The gentlelady from Florida.

Ms. DEMINGS. Thank you so much, Mr. Chairman. And thank you all for what you do every day to help to keep us safe.

If we could just go back a little bit to follow up on my colleague's questions about whatever the information is, that it would have to be relevant, I believe. Could you talk a little bit about the checks and balances of the FISA Court application system that would maybe relieve some of the concerns there?

Mr. ORLANDO. To begin with, first we have to open a case, which has to have supervisor approval. As we move forward to do a business record and the agent drafts that up, it goes back to a supervisor review, all the way up the chain, over to our headquarters where there are a number of lawyers that look at that application to make sure that we have the right relevancy that is relevant to a national security investigation, and then it moves over to the Department of Justice for another series of attorneys who look at it before it goes over to the Court. So, there are a number of individuals and supervisors that are looking at these applications.

Ms. DEMINGS. Mr. Wiegmann.

Mr. WIEGMANN. You also have to have a statement of facts. You can't just assert that it is relevant. You have to have the factual showing that it is relevant to the investigation. Then you also have to be able to show that it is not based on First Amendment-protected activity. Then you have to present all of that to the FISA Court, and the FISA Court has to agree. So, there is a really elaborate process that Mike just described, and then it ends up with a judicial approval.

Ms. DEMINGS. Thank you. Moving on, Mr. Orlando, to roving wiretaps, when the Government applies to conduct electronic surveillance under FISA, it always—does not always necessarily have to identify the person being targeted. The law requires you to State the identity, if known, or a description of the specific target.

At a general or hypothetical level, can you describe why you might not know the identity of a particular target and would instead provide a description of the target? Or in most cases, do you know—

Mr. ORLANDO. I would say in all my experience, we have always known who that individual is. The roving authority gives us the ability, if they are using tradecraft to elude us so that we get secondary orders so we can go to multiple facilities. We still have to go back to the Court within 10 days to describe what we have done. The only circumstance hypothetically that I can think of is if there is a pending threat and we don't have a name, but we have a number of identifiers of what that individual is. If we can possibly present a case to the Court that we think it is this type of person because it meets all the identifiers might be that circumstance.

Mr. WIEGMANN. If I could just add on that, without getting into the classified detail, I think the cyber context is one in which you can imagine you might have a lot of information to be able to identify an individual that may not know that person's name. So, I can give you more information about that, but I think if that is what you are referring to, the cyber context would be the context in which that would most be applicable.

Ms. DEMINGS. So, with the roving wiretaps, could you just briefly describe why you feel this provision is so needed and why terrorists or national security threats have been detected or prevented as a result of it, and if it is classified, just please give us a hypothetical.

Mr. ORLANDO. Sure, I can talk about both counterterrorism and counterintelligence hypothetical situations. On the counterterrorism side, we have the threat of the homegrown violent extremists who are radicalizing very quickly and mobilizing very quickly. We have to disrupt them faster than we have had to disrupt them in the past 20 years. They are involving with their tradecraft. We have instances where they change their cell phones and emails and online profiles pretty quickly. That roving authority helps us keep pace with them. If we did not have that authority, we would have to repeatedly go back to the Court or seek emergency authority and get the order thereafter, which would cause delay.

On the counterintelligence side, we have foreign intelligence services that have highly trained intelligence officers who are trained to evade FBI surveillance, who are able to come into the country, change cell phones, change emails, change rented vehicles. This gives us the capability to keep pace with them.

Ms. DEMINGS. I believe it was said earlier that the lone-wolf provision has never been used.

Mr. ORLANDO. Yes.

Ms. DEMINGS. Could you give me—well, I find that surprising but—and the concern that just expressed, could you give me some examples of how it could be used to help decrease domestic terrorism?

Mr. ORLANDO. I don't believe it applies to domestic terrorism. What I will say, for the lone-wolf statute, with the homegrown violent extremists, these are individuals who are here in the United States. For that statute, they would have to be a non-U.S. person, but they have a global jihadist ideology. Homegrown violent extremists are not taking direction from a terrorist organization. To date, we have been able to thwart those activities by finding other ways of getting FISAs or making some sort of connection. With this evolution, I foresee the possibility of using that statute, possibly coming through with the way the threat is evolving, where people are using mixed ideologies.

Ms. DEMINGS. Okay. Thank you, Mr. Chairman. I yield back.

Chairman NADLER. The gentlelady yields back.

The gentleman from California.

Mr. CORREA. Thank you, Mr. Chairman. I would like to add my voice to the chorus of colleagues here that have expressed appreciation for your work, protecting our country, our citizens. I also wanted to add my concerns about civil liberties and privacy.

We are not a police state. Our security to a great extent relies on the trust of our population in our governmental institutions and our police, so to speak.

In my district, we probably speak 100 different languages. I think about my district as being the new Ellis Island of the United States. I have people from all over the world, literally from all over the world, living in my district. Trust in our police agencies is paramount.

To give you an example, a few years ago we—I didn't but neighbors arrested a rapist in the Act of raping a woman. He was convicted of 20 rapes. We think there were more victims, but yet those victims never presented themselves because they feared the authorities and many of them were undocumented.

I wanted to follow up some of the questions Congressman Cohen touched on, which was the impact of sections 215 on minority communities. Specifically, your information that you gather, is it shared with immigration enforcement authorities?

Mr. ORLANDO. There would have to be some crime that relates to them before we would share any information with them.

Mr. CORREA. So, let me help you clarify for me, it is not shared with immigration authorities unless it is relevant to some specific crime, some national interest of specific criminal acts of terrorism or otherwise? Is that what I am hearing?

Mr. ORLANDO. It would have to be done on a specific case by case where there is relevancy for us to pass it to them.

Mr. CORREA. So specifically wiretap, you suspect somebody on one end or the other, the U.S. is—may have a question of immigration status, that information is not automatically turned over to immigration enforcement authorities?

Mr. ORLANDO. It would have to be relevant. For instance, if we had determined that we have a terrorist threat that is possibly coming through the border, we would turn it over to our partners in CBP to assist us in neutralizing that threat.

Mr. CORREA. That terrorist threat is not one defined as merely immigration status but, rather, they are here to do serious violent acts to our population?

Mr. ORLANDO. They would have to meet the definition of an international terrorism case.

Mr. CORREA. Ms. Morgan?

Ms. MORGAN. Yes, sir, as I stated before, we have used the CDR Program specifically to focus on mitigating threats from international terrorism. If we find information related to international terrorism, we will report it out to entities authorized to get that information.

Mr. CORREA. Mr. Wiegmann?

Mr. WIEGMANN. Again, there are minimization procedures under all FISA authorities that specify the rules for when you can disseminate information. The general standard is it has to be foreign intelligence information, necessary to understand foreign intelligence information, or evidence of a crime. Those are, generally speaking—

Mr. CORREA. That crime would not be immigration status in this country?

Mr. WIEGMANN. That is a good question as to whether someone had illegally entered. Would that be a crime? So, if you had evidence that was bearing on that as a crime, I don't know. Maybe that is possible if the actual information was evidence of that crime.

Mr. CORREA. Could you get me more information on that, under what circumstances that may be possible or not?

Mr. WIEGMANN. Sure, absolutely.

Mr. CORREA. Again, my question is your information is shared with immigration authorities on the fact that maybe somebody here—their immigration status is not correct, so to speak.

Mr. WIEGMANN. I will get back to you on that.

Mr. CORREA. I can envision a situation—you have a very powerful tool at your disposal, information, wiretapping. You could very easily turn that around and say we are going to use this for immigration purposes. I hope you do not get that—

Mr. ORLANDO. That would not be correct, sir. We only use these authorities to counter foreign intelligence services and foreign terrorism organizations and international terrorists, lone-wolf international terrorists.

Mr. CORREA. I would like something in writing from each of you on that specific. I don't want a treatise, but just something clear.

Mr. CORREA. Finally, the last 20 seconds, I also would like to know what tools you need to fight domestic terrorism. You mentioned that the lone-wolf provision has not been applied. Maybe it can be—it only applies to maybe international, not domestic. I want to know what tools you need to keep our population safe in the U.S. from emerging domestic terrorism threats.

With that, Mr. Chair, I yield.

Chairman NADLER. The gentleman yields.

The gentlelady from Texas.

Ms. GARCIA. Thank you, Mr. Chairman. Thank you for holding this very important hearing.

I, too, want to first start by thanking all of you for the good work that you do in your respective agencies and to all the people that work in your agencies, not only in your offices here in DC, but obviously in the field, where the real work happens.

I, too, have worked with at least the DOJ and the FBI on a number of cases in my capacity as a judge and a lawyer, never with NSA. So, I just want to make sure that you know that there are many of us out there who do support you and do so without shame. However, when we look at the whole picture, I know that it is all about the balances, and the national security or threats versus the privacy of individuals versus some of the other things that we have got to balance.

I wanted to start with you, Ms. Morgan, to clarify even for the audience that is watching at home perhaps. We get a letter from your agency that says that NSA has suspended the Call Detail Records Program and has deleted the call details record. This decision was made after balancing the program's relative intelligence value, associated costs and compliance.

If we have suspended it, and you keep saying you need the tool in your toolbox, obviously in my toolbox, if I have a broken hammer, I just throw it out. I mean, why is it that you suspended it and now you think that you need it? I know you said that emphatically as a professional, that you thought you needed it. So, I want to be clear as to why we really do need it.

Ms. MORGAN. Thank you for your question, ma'am. I really do appreciate it. So, as we have stated and as was stated in the letter, we made the decision to suspend the program after we balanced the intelligence value that did exist in the program when it was—

Ms. GARCIA. Yeah, but you said there was a lot of matrix, but you only referenced two, the ones Chairman talked about.

Ms. MORGAN. I am sorry?

Ms. GARCIA. I said you talked about a lot matrix that go into making that decision, but you only mentioned the two that I believe Chairman mentioned. So, what other matrix do you all consider?

Ms. MORGAN. So, when we evaluate our intelligence programs, we are going to look at them across the panoply of all the different programs that we have.

Ms. GARCIA. I know, but we talked about two. What others do you look at?

Ms. MORGAN. What others do I look at?

Ms. GARCIA. Mm-hmm.

Ms. MORGAN. In terms of making decisions as—on value. Is that what you mean?

Ms. GARCIA. Yeah, and why we should reinstate the program—reauthorize it.

Ms. MORGAN. So, what I would say is that, as I sit here as an intelligence professional, and I started my career in 2001 as an intelligence analyst. I can tell you that you can't—you never know what you are going to confront in the future—

Ms. GARCIA. I know, but you have told us all that. I want specific matrix that you all look at to determine whether or not did you want the program reauthorized after you have already suspended it.

Ms. MORGAN. Ma'am, can you help me understand what you mean by "matrix"?

Ms. GARCIA. Well, you used—I am using your own words.

Chairman NADLER. I think you mean "metrics."

Ms. MORGAN. Oh, metrics.
Ms. GARCIA. Metrics.
Ms. MORGAN. I am sorry, ma'am. I thought you said—
Ms. GARCIA. I did say "matrix." I misspoke. I apologize.
Ms. MORGAN. I apologize for that.
Ms. GARCIA. It has been a rough week already.
Ms. MORGAN. I am sorry?
Ms. GARCIA. It has been a rough week already.
Ms. MORGAN. It has been a long day. But metrics. So, what I would say is a couple things. One is you are not always necessarily going to have metrics because the intelligence profession is not always something that can be specifically measured, and you can't necessarily measure the information, the lead information that I got over, ultimately, weeks, months, years from now, actually led me to have this significant picture that provides me with critical insights from a foreign intelligence perspective. So, it is not always that you are going to have like a data point, like this amount of this particular thing happened to happen. You are not always going to have a number.

In some instances, it is going to be intelligence professionals, discussions with our colleagues, to say, "Hey, we reported this information out from this program. Has it been of value to you? How has it been of value to you?" Then you are going to take that information and make a decision based on different factors that you can consider. You are not necessarily going to have, "Well, this program I rate a 5 and this program I rate a 3, and here is all my data."

Ms. GARCIA. Well, it sounds like you want to keep it just in case you might want to use it, and I am not sure that I agree with that. So, I am going to have to cut you off because I quickly want to ask a question from the FBI folks. A number of companies offer genetic testing services to test for genealogical research, for detection of carrier status for inherited conditions. Is any of that also subject to the FISA 215 activity?

Mr. ORLANDO. This might be one of those where we need to refer back to the book again. I am not familiar of any time we have asked for that type of information.

Ms. GARCIA. Okay.

Mr. WIEGMANN. So, again, the 215 authority is just a grand jury subpoena. You can really request any type of tangible thing, any type of record, provided you have established that it is relevant to an authorized investigation and you have specific facts that show that. It seems unlikely, again, as I said earlier with respect to medical records that would be the case—

Ms. GARCIA. Well, there is a lot of—what about—

Mr. WIEGMANN. It is not ruled out because it—I don't know what the fact pattern might be, but could there be a fact pattern in which that was relevant to an investigation? I don't know.

Ms. GARCIA. What about the videos from the new door bells that you go to the door and there is a video camera or the video surveillance at the front door that you are videoing—

Mr. WIEGMANN. That most certainly could be relevant in an investigation. I am sure that could be—I can easily envision scenarios where that could be relevant to an investigation.

Mr. ORLANDO. Ma'am, if I could add on the business records provision, mostly what we use it for is a building block. We open a case; we identify a subject, his telephone numbers, his email addresses. We will go to the Court for a business record to identify the transactional records, not the content, to see who he is talking to, to see if we can build a connection to the terrorist organization to identify the network. And then we have our analysts look at that, and then we use that to aid us to building the probable cause to move to a FISA Court-authorized surveillance.

Ms. GARCIA. All right. Thank you, Mr. Chairman. My time has run out, I believe. I yield back.

Chairman NADLER. The gentlelady yields back.

This concludes today's hearing. We thank all of our witnesses for participating.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witnesses or additional materials for the record.

Without objection, the hearing is adjourned.

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

APPENDIX

September 17, 2019

Chairman Jerrold Nadler
U.S. House Judiciary Committee
2138 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Doug Collins
U.S. Judiciary Committee
2142 Rayburn House Office Building
Washington, D.C. 20515

Re: FISA Oversight Hearing

AMERICAN CIVIL LIBERTIES UNION

National Political
Advocacy Department
915 15th St. NW, 6th FL
Washington, D.C. 20005
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
National Political Director

Dear Chairman Nadler, Ranking Member Collins, and Members of the Committee:

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter for the record in connection with the House Judiciary Committee's hearing, "Oversight of the Foreign Intelligence Surveillance Act," which is scheduled to take place on September 18, 2019.

In 2015, in response to revelations that the NSA and FBI abused their surveillance powers, members of this committee worked on a bipartisan basis to pass the *USA Freedom Act.*[1] The goal of this legislation was to stop large-scale surveillance under the Patriot Act, increase transparency, and institute other reforms to ensure that Americans' constitutional rights were protected. Since passage of this Act, two things have become apparent. One, the reforms in the *USA Freedom Act* did not go far enough to protect Americans' rights. And, two, many of the reforms in the *USA Freedom Act* are not working as intended.

On December 15, 2019, Section 215 and other provisions of the Patriot Act extended by *the USA Freedom Act* are once again set to expire. **We urge Congress to use this opportunity to pass comprehensive surveillance reform that remedies the deficiencies in the 2015 legislation. Absent meaningful reform, the ACLU urges Congress to sunset Section 215 and the other expiring Patriot Act provisions.**

There are many issues that must be addressed in any meaningful surveillance reform legislation. However, we want to highlight several key reforms that should be included in any legislation:

[1] H.R. 2048, USA FREEDOM Act of 2015, Pub. L. No. 114-23.

- **Ending Section 215's call detail record authority,** which has been used to collect over 1 billion call records[2], has no proven intelligence value, and has been suspended due to persistent compliance violations;

- **Limiting the types of records that can be obtained under Section 215** to exclude location information health information, tax records, and sensitive data that the government generally cannot obtain without a probable cause warrant;

- **Preventing discrimination and strengthening existing First Amendment protections,** including by prohibiting the government from targeting individuals based on First Amendment conduct or discriminating against Americans on the basis of race, religion, nationality, or other protected class status;

- **Requiring notice to criminal defendants and others** who have Section 215 information used against them;

- **Closing the Section 702 backdoor search loophole**, which the government uses to search for information about Americans, thereby circumventing Section 702's prohibition against reverse targeting Americans;

- **Limiting large-scale collection and dissemination of information** under Section 215 and other Patriot Act authorities; and

- **Increasing transparency and oversight**, including by requiring the government to fully disclose the number of individuals whose information is collected under Section 215, requiring additional information be made public about the government's use of other surveillance tools, and making clear that existing law requires the government to promptly declassify novel or significant Foreign Intelligence Surveillance Court (FISC) opinions issued prior to 2015.

1. Ending the call detail record program

It is now apparent that the NSA's call detail record program is unsalvageable. Despite reforms in 2015, the NSA continued to collect an immense amount of Americans' information under the program – amassing over 1 billion records from 2016 to 2018 alone.[3] It has also consistently operated the program in violation of the law. While the NSA has reportedly shuttered the call detail record program, Congress must end this authority to ensure that it can never be restarted.

---

[2] Office of the Director of National Intelligence, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES, CALENDAR YEAR 2018, at 30 (Apr. 2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.
[3] *Id.* at 30.

The call detail program has been beset with compliance problems. Documents obtained by the ACLU revealed compliance incidents in November 2017 and February 2018, with the latter resulting in the collection of records that the agency did not have the authority to collect.[4] The Office of Civil Liberties, Privacy, and Transparency (CLPT) assessed that this incident had a "significant impact on civil liberties and privacy."[5] In addition, the NSA reportedly "relied" on this inaccurate information in targeting requests that were approved by the FISC, which may have resulted in improper surveillance.[6]

Following the discovery of the compliance violation, in June 2018, the NSA disclosed that it began deleting *all call detail records* collected under the program because the unauthorized records could not be "identified and isolated." However, the NSA stated that the "root cause of the problem has since been addressed for future CDR acquisitions."[7] Despite these promises, on or around October 2018, it appears that the NSA again received erroneous call records.[8]

In the wake of these persistent problems, the NSA has suspended the program. According to the ODNI, this decision was made after "balancing the program's relative intelligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes." In other words, even the ODNI has concluded the value of the intelligence value of the call detail record program does not outweigh its significant costs. This is perhaps unsurprising given that the Privacy and Civil Liberties Oversight Board concluded in 2014 that the call record program had never played a substantial role in stopping a terrorist attack or identifying a terrorist suspect.[9]

It is abundantly clear the call detail records program cannot be operated in a way that does not threaten Americans' rights. Congress should end this authority and should reject ODNI efforts to make the authority permanent so that the program can be restarted in the future.

2. Limiting the types of records that can be obtained under Section 215

---

[4] National Security Agency, REPORT TO THE INTELLIGENCE OVERSIGHT BOARD ON NSA ACTIVITIES, SECOND QUARTER, CALENDAR YEAR 2018—INFORMATION MEMORANDUM, approved for Release by NSA on Jun. 17, 2019, FOIA Case No. 105767 (litigation), at 049-051, available at https://www.aclu.org/legal-document/nsa-foia-documents-quarterly-reports-intelligence-oversight-board-nsa-activities.

[5] *Id.* at 050.

[6] *Id.* at 050-051.

[7] Press Release, National Security Agency, NSA Reports Data Deletion, (Jun. 28, 2018), https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/.

[8] NSA FOIA Case No. 105767, s*upra* note 4, at 032-033.

[9] Privacy and Civil Liberties Oversight Board, 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 (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

Under Section 215, the government asserts the authority to request a broad array of records from third parties, merely if they are considered "relevant" to a counterterrorism or counterintelligence investigation.[10] Though the government has not disclosed a complete list of the types of records it obtains under Section 215, this includes phone records, tax returns, health information, gun records, call records, and a host of other sensitive information.[11]

The government has justified this expansive power by arguing that individuals do not have a privacy interest in personal information held by third parties – an argument the Supreme Court rejected last term in *Carpenter* when it held that the government was required to obtain a warrant when demanding individual's location information.[12] Despite this ruling, as of March of this year, the ODNI had still failed to issue guidance or respond to Congressional inquiries regarding how *Carpenter* should be implemented.[13] Moreover, the ODNI has failed to respond to Congressional requests about whether it believes it can use Section 215 to collect location information[14], which would be contrary to the *Carpenter* ruling.

Given this, it is imperative that Congress amend Section 215 to make clear that it cannot be used to obtain sensitive information, including location information, health records, financial information, and sensitive data that that the government can generally not obtain without a search warrant.

3. Preventing Discrimination and Strengthening First Amendment Protections

Existing law fails to include enough protection against surveillance that is discriminatory or targeted based on First Amendment-protected activity. Section 215 and other Patriot Act authorities prohibit surveillance based "solely" on First Amendment-protected activities.[15] However, opinions that have been partially released by the FISC suggest that these safeguards have been interpreted narrowly.[16] These opinions suggest that the government is not foreclosed from surveilling an individual in cases where all or a substantial portion of the facts relied on in a surveillance application involve First Amendment-protected conduct.

Similarly, Presidential Policy Directive-28 states that the U.S. "shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or

---

[10] See 50 USC § 1861.
[11] See 50 USC § 1861(a).
[12] *Carpenter v. United States,* 138 S.Ct. 2206 (2018).
[13] Letter from Senator Ron Wyden to DNI Director Daniel Coats (Jul. 30, 2019), available at https://int.nyt.com/data/documenthelper/1528-wyden-letter-to-dni-re-215-and/6e12df714de6eb7df542/optimized/full.pdf#page=1.
[14] *Id.*
[15] *See* 50 USC § 1861(a).
[16] *In Re. Orders of this Court Interpreting Section 215 of the Patriot Act,* Docket No. Misc 13-02 (FISC Aug. 24, 2017), https://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Opinion-1.pdf

religion."[17] However, existing law and policies that are publicly available do not make clear that Patriot Act authorities cannot be used to target individuals based on race, religion, ethnicity, nationality, and other protected classes, and that the government cannot use selection terms that can serve as proxies for membership in a protected class.

To address these deficiencies, Congress should clarify and strengthen existing First Amendment protections to prohibit surveillance in cases where either the purpose of the investigation or the factual predicate for the surveillance is First Amendment protected activities. In addition, Congress should prohibit targeting of Americans or use of selection terms that are based on or serve as proxies for race, religion, nationality, or other protected classes.

4. Notice

Unlike other surveillance authorities, including Section 702 of the Foreign Intelligence Surveillance Act (FISA), Section 215 does not have a statutory provision requiring notice to individuals in cases where information obtained or derived from the authority is used in a criminal, civil, or administrative proceeding. In court filings,[18] the government has denied that it has any obligation to inform defendants when information obtained or derived from Section 215 is used in a criminal case. This position not only violates the Constitution, it also largely forecloses individuals from challenging unconstitutional surveillance in court.

To remedy this, Congress should add a statutory notice provision to Section 215, which makes clear that the government must provide notice in any case that it is using or disclosing evidence that would not have been obtained but for surveillance under Section 215 and regardless of any claim that the evidence would inevitably have been discovered.

5. Closing the Section 702 backdoor search loophole

Section 702 explicitly prohibits the government from targeting U.S. persons. The government nevertheless searches Section 702 data looking specifically for information about U.S. persons, a practice often referred to as a "backdoor search." This permits Section 702 to be exploited as a tool against Americans in foreign intelligence and domestic criminal investigations alike. The NSA performs over 30,000 backdoor searches annually. While the FBI refuses to report the number of backdoor searches it performs, the Privacy and Civil Liberties Oversight Board reports that the number of these searches is

[17] Presidential Policy Directive-28 of Jan. 17, 2014 (Signals Intelligence Activities), available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[18] Gov't Response at 6, *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo. Feb. 26, 2015) (ECF No. 711).

"substantial," in part because it is "routine practice" for the FBI to conduct a query when an agent initiates a criminal assessment or investigation related to any type of crime.[19]

The original version of the *USA Freedom Act* would have closed the backdoor search loophole by requiring the government to obtain a warrant when querying the Section 702 database to obtain information about Americans. Unfortunately, this reform was not included in the final version of the bill, despite the fact that the House has twice passed appropriations amendments that would close the backdoor search loophole.[20] We urge Congress to ensure that this reform is included in any surveillance reform measure.

6. Limiting Large-Scale Collection and Dissemination

Statistics released by the NSA suggest that the USA Freedom Act has not achieved its goal of preventing bulk and large-scale collection under the Patriot Act. For example, in 2018, using the pen register and trap and trace authority, the government collected information of 132,690 unique accounts, despite the fact that there were only 34 surveillance targets.[21] Similarly, under the Section 215 business records provision, the government collected information of 214,860 unique accounts, yet had only 60 surveillance targets.[22] The NSA and FBI have not disclosed how often this information is searched, and whether any of this information is routinely searched when the FBI initiates an assessment or criminal investigation.

To address these deficiencies, Congress should further limit large-scale collection under the authorities reformed by the USA Freedom Act. In addition, it should prohibit information collected under the Patriot Act from being disseminated and searched for purposes unrelated to the reasons for which it was collected.

7. Increasing Transparency

The transparency provisions in the USA Freedom Act have failed to ensure that the public and Congress have sufficient information about U.S. surveillance practices – in part because the government has failed to fully comply with them. Section 402 of the USA Freedom Act required the government to declassify novel and significant FISA court opinions – yet the government has wrongly interpreted this to only apply to opinions issued after passage of the Act. In addition, there have not been any FISC opinions declassified pursuant to the statute for at least a year, calling into question whether the government is fully complying with this requirement. Similarly, though the *USA Freedom Act* required the government to report information regarding the number of unique accounts impacted under Section 215 surveillance and other authorities, the government has only partially

---

[19] Privacy and Civil Liberties Oversight Board, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC.702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Jul. 2, 2014) https://www.pclob.gov/library/702-Report.pdf. [Hereinafter "PCLOB Report on 702"]
[20] H.R. 4870, Roll Call Vote 327, http://clerk.house.gov/evs/2014/roll327.xml; H.R. 2685, Roll Call Vote 356, http://clerk.house.gov/evs/2015/roll356.xml.
[21] Office of the Dir. of Nat'l Intelligence, STATISTICAL TRANSPARENCY REPORT, *supra* note 2, at 24.
[22] *Id.* at 26.

released these statistics. Government statistics appear to exclude information from non-communications records, or records that were received through hard-copy or portable media.[23]

To address this, Congress should make clear that the government is obligated to promptly disclose novel and significant FISA court opinions, including those that were issued prior to 2015. In addition, they should strengthen existing transparency provisions to ensure that the government is providing a complete picture of surveillance under Section 702 and Patriot Act authorities.

The expiring Patriot Act provisions are an opportunity for Congress to enact meaningful surveillance reform. In addition to the issues highlighted above, Congress should also consider reforms to further enhance transparency, limit dissemination of information, ensure information collection is targeted, increase oversight, and strengthen the FISA court amici. Furthermore, it must address concerns with the "lone wolf" and "roving wiretap" authorities, which are also set to expire in December. Absent meaningful reform, we urge Congress to allow the expiring Patriot Act provisions to sunset.

If you have questions, please contact Senior Legislative Counsel, Neema Singh Guliani at nguliani@aclu.org.

Sincerely,

Ronald Newman
National Political Director

Neema Singh Guliani
Senior Legislative Counsel

cc: Members of the U.S. House Judiciary Committee

[23] *Id.* at 23, 26.

Questions for the Record of Congressman Ted W. Lieu

House Judiciary Committee

Hearing on "Oversight of the Foreign Intelligence Surveillance Act"

September 18, 2019

1. Can the government use Section 215 orders to obtain biometric information, including but not limited to images of faces, fingerprints, or DNA?

2. What specific types of biometric information has the government used Section 215 orders to acquire?

3. Once obtained, could this information be subject to further analytical techniques, for instance facial recognition analysis?

RESPONSES OF
J. BRADFORD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

TO QUESTIONS FOR THE RECORD
ARISING FROM A SEPTEMBER 18, 2019, HEARING

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

CONCERNING
OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Questions from Representative Lieu

Question 1: Can the government use Section 215 orders to obtain biometric information, including but not limited to images of faces, fingerprints, or DNA?

Response: 50 U.S.C. §1861 authorizes the Government to apply to the Foreign Intelligence Surveillance Court ("FISC") for an order directing the production of business records or other tangible things that are relevant to an authorized national security investigation, provided that with respect to a United States person, such investigation is not conducted solely on the basis of First Amendment protected activities. An order issued by the FISC under section 1861 may require the production of a tangible thing only if such thing can be obtained via a grand jury subpoena or with any order issued by a court of the United States directing the production or records or tangible things. *See*, §1861(c)(2)(D). Accordingly, if biometric information (e.g., fingerprints or photographs) is included in records that, in context, are relevant to an authorized national security investigation and obtainable via a grand jury subpoena or other court order (e.g., employment or Department of Motor Vehicle records), such information could be obtained by an order issued by the FISC under section 1861, much as they could with a grand jury subpoena or court order.

Question 2: What specific types of biometric information has the government used Section 215 orders to acquire?

Response: Based upon a finding that the tangible things requested were relevant to an authorized national security investigation and obtainable via a grand jury subpoena or other court

order, the FISC has issued orders under section 1861 for the production of records that likely contained certain images and/or biometric information such as security surveillance video footage, and records that include driver's license information, including license photographs. The FISC also has issued orders under section 1861 for employment records and educational records that may have included photographs and/or fingerprints.

Question 3: Once obtained, could this information be subject to further analytical techniques, for instance facial recognition analysis?

Response: The FBI's section 215 minimization procedures allow the FBI to analyze collection for the purpose of determining whether the material reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or to assess its importance, or evidence of a crime. However, there may be technological issues that limit what analytical techniques could be applied to section 215-acquired information. Similarly, there may be classification issues that limit the FBI's ability to use non-secure systems for analyzing classified information such as section 215-acquired information.

Questions for the Record to Mr. Orlando from Congresswoman Garcia

1. Q: Does the FBI have any current or developing policies regarding the use of Section 215 to acquire genetic records? If so, please describe them. If the government has used Section 215 to acquire such records, how many Section 215 orders have been issued to acquire them and how many genetic records have been delivered to the government in response to those orders?
2. Q: Does the FBI have any current or developing policies regarding the use of Section 215 to acquire video recordings produced by consumer products, such as Ring Video Doorbells? If so, please describe them. If the government has used Section 215 to acquire such video recordings, how many Section 215 orders have been issued to acquire them and how many video recordings have been delivered to the government in response to those orders?
3. Q: Has the FBI ever used Section 215 to acquire video recordings, for instance those that would be produced by a Ring doorbell or similar consumer product? Is the government's position that it may?

○