THE ADMINISTRATION'S USE OF FISA AUTHORITIES

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JULY 17, 2013

Serial No. 113–45

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
81–982 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
MARK AMODEI, Nevada
RAUL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
JASON T. SMITH, Missouri

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

CONTENTS

JULY 17, 2013

THE ADMINISTRATION'S USE OF FISA AUTHORITIES

WEDNESDAY, JULY 17, 2013

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to call, at 10:11 a.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Sensenbrenner, Coble, Smith of Texas, Chabot, Bachus, Forbes, King, Gohmert, Poe, Chaffetz, Gowdy, Labrador, Farenthold, Holding, Collins, DeSantis, Conyers, Nadler, Scott, Lofgren, Jackson Lee, Cohen, Johnson, Chu, Deutch, DelBene, Garcia, and Jeffries.

Staff Present: (Majority) Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Chief of Staff & Chief Counsel; Allison Halataei, Parliamentarian & General Counsel; Caroline Lynch, ; Sam Ramer, Majority Counsel; Kelsey Deterding, Clerk; (Minority) Perry Apelbaum, Minority Staff Director & Chief Counsel; Danielle Brown, Parliamentarian; and Aaron Hiller, Counsel.

Mr. GOODLATTE. Good morning. The Judiciary Committee will come to order. And 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 Administration's use of FISA Authorities, and I will begin by recognizing myself for an opening statement.

Today's hearing will examine the statutory authorities that govern certain programs operated under the Foreign Intelligence Surveillance Act, or FISA. Since the unauthorized public release of these programs, many Members of Congress and their constituents have expressed concern about how these programs are operated and whether they pose a threat to Americans' civil liberties and privacy. We have assembled two panels of witnesses today to help us explore these important issues.

Last month, Edward Snowden, an unknown former NSA contractor and CIA employee, released classified material on top secret NSA data collection programs. On June 5th, the Guardian released a classified order issued by the Foreign Intelligence Surveillance Court requested by the FBI to compel the ongoing production for a 3-month period of call detail records, or telephony metadata. Telephony metadata includes the numbers of both parties on a call, unique identifiers, and the time and duration of all calls.

On June 6th, classified information regarding a second program, the PRISM program, was reported by the Guardian and the Washington Post. News reports described the program as allowing the NSA to obtain data from electronic service providers on customers who reside outside the United States, including email, chat, photos, videos, stored data, and file transfers.

Both of these programs are operated pursuant to statutory provisions in FISA or the FISA Amendments Act. FISA was enacted to provide procedures for the domestic collection of foreign intelligence. When FISA was originally enacted in 1978, America was largely concerned with collecting intelligence from foreign nations, such as the Soviet Union, or terrorist groups like the FARC in Colombia. FISA set forth procedures for how the Government can gather foreign intelligence inside the United States about foreign powers and their agents.

The intelligence landscape has changed dramatically over the last 30 years. Today, we are confronted with ongoing threats from terrorist organizations, some of which are well structured, but most of which are loosely organized, as well as threats from individuals who may subscribe to certain beliefs but do not belong to a specific terrorist group. The FISA business record provision, often referred to as Section 215 of the PATRIOT Act, allows the FBI to access tangible items, including business records in foreign intelligence, international terrorism, and clandestine intelligence investigations.

Unlike grand jury or administrative subpoenas in criminal investigations, which can simply be issued by a prosecutor, a FISA business records order must first be approved by a Federal judge. Similar to grand jury or administrative subpoenas, a FISA business record order cannot be used to search a person's home, to acquire the content of emails, or listen to telephone calls. It can only be used to obtain third-party records.

Critics of the metadata program object to its breadth, namely the ongoing collection of all customers' telephony metadata, and question whether this program conforms to Congress' intent in enacting Section 215 of the PATRIOT Act. I hope to hear from today's witnesses about this, about how the collection of this metadata is relevant to a foreign intelligence or terrorism investigation and about whether a program of this size is valuable and cost effective in detecting and preventing terrorist plots.

In the 40 years since FISA enactment, communications technologies have changed dramatically and revolutionized the transmission of international communications. The shift from wireless satellite communications to fiber optic wire communications altered the manner in which foreign communications are transmitted.

The use of wire technology inside the United States to transmit a telephone call that takes place overseas had the unintended result of requiring the Government to obtain an individualized FISA court order to monitor foreign communications by non-U.S. persons. Congress enacted in 2008 and reauthorized just last year the bipartisan FISA Amendments Act to update our foreign intelligence laws.

The FAA permits the Attorney General and the Director of National Intelligence to target foreign persons reasonably believed to be located outside the United States to acquire foreign intelligence

information. The act requires for the first time in U.S. history prior court approval of all Government surveillance using these authorities, including court approval of the Government's targeting and minimization procedures.

The PRISM program derives its authority from Section 702 of the FAA. It involves the collection of foreign intelligence information about non-U.S. persons located outside the United States. To the extent the program captures information pertaining to U.S. citizens, such interception can only be incidental, and the handling of such information is governed by court-approved minimization procedures.

I look forward to hearing from our witnesses today in greater detail about how the Government limits its targeting under 702 to non-U.S. persons outside the U.S. and a description of the oversight performed by the Administration and the FISC of this program, including the effectiveness of the current auditing of Section 702.

The terrorist threat is real and ongoing. The Boston bombing reminded us all of that. I am confident that everyone in this room wishes that tragedy could have been prevented. We cannot prevent terrorist attacks unless we can first identify and then intercept the terrorist.

However, Congress must ensure that the laws we have enacted are executed in a manner that is consistent with congressional intent and that protects both our national security and our civil liberties. We must ensure that America's intelligence gathering system has the trust of the American people.

It is now my pleasure to recognize the Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

Mr. CONYERS. Thank you, Chairman Goodlatte and Members of the Committee.

We are on Judiciary, which is the Committee of primary jurisdiction for both of the authorities we are here to discuss today, Section 215 of the PATRIOT Act and Section 702 of the FISA Amendments Act. Over the past decade, the Members of this Committee have vigorously debated the proper balance between our safety and our constitutional right to privacy.

And so, I join in welcoming the two panels—four each, very fairly made up—to this discussion today. I think it is an important one.

But we never at any point during this debate have approved the type of unchecked sweeping surveillance of United States citizens employed by our Government in the name of fighting the war on terrorism. Section 215 authorizes the Government to obtain certain business records only if it can show to the FISA court that the records are relevant to an ongoing national security investigation.

Now what we think we have here is a situation in which if the Government cannot provide a clear public explanation for how its program is consistent with the statute, then it must stop collecting this information immediately. And so, this metadata problem to me has gotten quite far out of hand, even given the seriousness of the problems that surround it and created its need.

Now I have another concern that pertains to the Administration's track record of responding to the criticisms of these programs. We

know Director Clapper's misstatements and others. National Security Agency Director General Keith Alexander had to make retractions. Even FBI Director Robert Mueller is not empowered to rewrite history.

But what we have is our conversation, which requires focusing on improving both more public scrutiny and congressional oversight of these programs. Over the last few weeks, the Administration has asserted that its conduct of this surveillance with congressional support because they have briefed some Members of these programs in the past. But that is not sufficient since we are in a catch-22 situation in a classified briefing in a secure setting, and we cannot discuss it publicly, certainly not even with our constituents. But if we skip the briefing, we risk being uninformed and unprepared.

One simple solution to this problem would be to publicly release significant FISA court opinions or, at the very least, unclassified summaries of these opinions. This solution would have the added benefit of subjecting the Government's legal claims to much-needed public scrutiny.

Over the past decade, the court has developed a body of law that instructs the Government about what it may do with the information it collects. There is no legitimate reason to keep this legal analysis from public interest any longer. And if we are to strike the right balance with these surveillance authorities, which I think is an important purpose of the hearing today, then we must bring the public into the conversation as soon as it is appropriate and without delay.

And I am not talking about releasing any classified information. Instead of simply asking our constituents to trust us, I am asking you and the executive branch to trust them. And the need for more declassification I think is very dominant, in my opinion, as to how we should move this today.

And I thank the Chair.

Mr. GOODLATTE. I thank the Ranking Member for his comments and would say in regard I share his concern about some classified information that does not need to be classified.

I also would say that because of the nature of the questions that we would like to ask, some of which cannot be asked or answered here in an open hearing, we will definitely be planning a second hearing on this subject, where we can ask those questions in a classified setting to, again, assure ourselves of the answers that we need.

Before we begin with questions for our witnesses, I want to stress that the—oh, first of all, without objection, all our Members' opening statements will be made a part of the record.

Before we begin with questions for our witnesses, I must stress that the programs this hearing is addressing remain classified. I expect the witnesses appearing before us today, particularly on our first panel, to answer questions from Members with as much candor as possible, given the unclassified setting.

But I also wish to caution Members of the Committee that they should be cognizant of this unique dynamic when phrasing their questions. The simple fact that certain programs have been leaked does not mean that they have been declassified, and Members and

witnesses alike would be violating the law were they to disclose classified information during this hearing.

I would also like to note that the Committee intends to hold a subsequent classified briefing for Members so that we have an opportunity to more closely examine those programs and pose questions to our witnesses that are not appropriate in this open setting.

We welcome our first panel today. And if you would all please rise, we will begin by swearing in the witnesses.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you very much.

Let the record reflect that all of the witnesses responded in the affirmative, and we will now proceed to introduce our witnesses.

Our first witness is Mr. James Cole, the Deputy Attorney General of the United States at the Department of Justice. Mr. Cole first joined the agency in 1979 as part of the Attorney General's Honors Program and served the department for 13 years as a trial lawyer in the Criminal Division.

He entered private practice in 1992 and was a partner at Bryan Cave, LLP, from 1995 to 2010, specializing in white-collar defense. Mr. Cole has also served as chair of the American Bar Association White Collar Crime Committee and as chair-elect of the ABA Criminal Justice Section.

Mr. Cole received his bachelor's degree from the University of Colorado and his juris doctor from the University of California at Hastings. We are fortunate to have him and his expertise with us today.

Our second witness is Mr. Robert S. Litt, the second general counsel of the Office of the Director of National Intelligence. Previously, Mr. Litt was a partner at Arnold & Porter, LLP, and served as a member of the Advisory Committee to the Standing Committee on Law and National Security at the American Bar Association. From 1994 to 1999, he served as Deputy Assistant Attorney General at the U.S. Department of Justice, where he worked on issues of national security, including FISA applications.

He began his legal career as a clerk for Judge Edward Weinfeld of the Southern District of New York and Justice Potter Stewart of the United States Supreme Court. Mr. Litt earned his bachelor's degree from Harvard University and his law degree from Yale. We welcome his experience and expertise.

The third member of our first witness panel is Mr. John C. Inglis, the Deputy Director and senior civilian leader of the National Security Agency, acting as the agency's Chief of Operations. Mr. Inglis began his career at NSA as a computer scientist within the National Computer Security Center.

Promoted to NSA's Senior Executive Service in 1997, he subsequently served in a variety of senior leadership assignments and twice served away from NSA headquarters, first as a visiting professor of computer science at the United States Military Academy and later as the U.S. special liaison to the United Kingdom.

Mr. Inglis is a graduate of the United States Air Force Academy, subsequently completing 9 years of active service and 21 years as a member of the Air National Guard. He holds advanced degrees in engineering and computer science from Columbia University,

Johns Hopkins University, and the George Washington University. And we thank him for joining us and sharing his expertise as well.

And finally on the first panel, Ms. Stephanie Douglas, Executive Assistant Director of National Security Branch of the Federal Bureau of Investigations. Ms. Douglas began as a special agent with the FBI in November 1989. She first reported to the Washington Field Office, where she worked violent crime, public corruption, and national security matters.

Before returning to the FBI headquarters in 2007, she served as an FBI detailee to the CIA's Counterintelligence Center, as well as supervisory special agent for a counterintelligence squad at the Washington Field Office, directing sensitive national security investigations. Before assuming her current post, Ms. Douglas was special agent-in-charge of the San Francisco Division.

Ms. Douglas earned her bachelor's degree in history at the University of Tennessee, and we are pleased to have her share her expertise with us today as well.

We thank all of you for joining us, and we will turn first to Mr. Cole for his testimony.

TESTIMONY OF JAMES COLE,
UNITED STATES DEPARTMENT OF JUSTICE

Mr. COLE. Thank you, Mr. Chairman, Mr. Ranking Member, and Members of the Committee, for inviting us here to speak about the 215 business records program and Section 702 of FISA.

With these programs and other intelligence activities, we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties. We believe these two programs have achieved the right balance.

First of all, both programs are conducted under laws passed by Congress. Neither is a program that has been hidden away or off the books. In fact, all three branches of Government play a significant role in the oversight of these programs.

The judiciary, through the Foreign Intelligence Surveillance Court, plays a role in authorizing the programs and overseeing compliance. The executive branch conducts extensive internal reviews to ensure compliance. And Congress passes the laws and oversees our implementation of those laws and determines whether or not the current law should be reauthorized and in what form. I would like to explain in more detail how this works with respect to each of the two programs.

The 215 program, as many of you have already heard, involves the collection of metadata from telephone calls. These are telephone records maintained by the phone companies.

They include the number that was dialed, the date and time of the call, and the length of the call. They do not include names or other personal identifying information. They do not include cell site or other location information, and they do not include the content of any phone calls.

These are the kinds of records that under longstanding Supreme Court precedent are not protected by the Fourth Amendment. The short court order that you have seen published in the newspapers only allows the Government to acquire these phone records. It does

not allow the Government to access or use them. That is covered by another, more detailed court order.

That court order provides that the Government can only search the data if it has a reasonable, articulable suspicion that the phone number being searched is associated with certain terrorist organizations. Deputy Director Inglis will explain in more detail how this process works.

But suffice it to say that there are many restrictions imposed on NSA to ensure that only properly trained analysts may access the data and that they can only access it with reasonable, articulable suspicion as a predicate and when it has been met and documented. The documentation of the analysts' justification is important. It exists so that it can be reviewed by supervisors before the search is done and audited afterwards to ensure compliance with the court's orders.

In the criminal context, the Government could obtain these types of records with a grand jury subpoena without going to court. But here, we go to court every 90 days to seek the court's authorization to collect the records. As part of the renewal process, we inform the court whether there have been any compliance problems. And if there have been, the court will take a very hard look and make sure we have corrected these problems.

As we have explained before, the 11 judges on the FISA court are far from rubber stamps. Instead, they review all of our pleadings thoroughly. They question us, and they don't sign off until they are satisfied that we have met all statutory and constitutional requirements.

The 702 program is different. Under that program, the Government does collect content of communications. Under 702, the Government applies to the FISA court for an order allowing it to collect the communications of non-U.S. persons reasonably believed to be overseas. This order lasts for 1 year.

The statute does not allow us to collect—or excuse me, does allow us to collect—communications even if the person on the other end of that phone call or email is in the United States or a U.S. person, but only if that is the result of a non-U.S. person outside the United States having initiated the call.

Importantly, the statute explicitly prohibits us from what is known as "reverse targeting." We can't use Section 702 indirectly to obtain the communications of U.S. persons anywhere or any persons located in the United States by targeting a non-U.S. person overseas.

Moreover, all U.S. person information collected is subject to what we call minimization rules. These rules are designed to restrict the dissemination, the use, and the retention of the information about U.S. persons collected. These rules are reviewed and approved by the court every year to ensure that we are handling U.S. person information in a manner consistent with the statute and the Fourth Amendment.

Both programs involve significant oversight by all three branches of Government. The FISA court reviews and approves the certifications and the Government's targeting and minimization rules, and it oversees the Government's compliance with these rules, the statute, and the Fourth Amendment.

Within the executive branch, multiple parts of the Government—NSA, its Inspector General, the Office of the Director of National Intelligence, and the Department of Justice—conduct robust compliance reviews and provide extensive reports on implementation and compliance to the FISA court and to the Intelligence and Judiciary Committees.

And Congress conducts oversight, decides whether to reauthorize the 702 authority, as it did in 2012 and as it did with 215 authority in 2011.

We take very seriously our responsibility to the American people to implement these programs in a manner that complies with all laws and the Constitution and strikes the right balance between protecting their safety and their privacy. I know others on the panel have brief statements to make, and then we are all ready to answer any questions you may have.

Thank you.

Mr. GOODLATTE. Thank you, Mr. Cole.

Mr. Litt, welcome.

TESTIMONY OF ROBERT S. LITT,
OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE

Mr. LITT. Thank you, Mr. Chairman, Mr. Ranking Member.

We appreciate your having this hearing. We think it is very important to correct some of the misimpressions that have been created about these activities, which, as the Deputy Attorney General explained, are entirely lawful and appropriate for protecting the Nation.

In my opening statement, I would like to make three related points about the Foreign Intelligence Surveillance Court. The first is that the activity that this court regulates, which is the acquisition of foreign intelligence for national security purposes, was historically outside of all judicial supervision. In fact, courts have held that the Fourth Amendment does not require a warrant at all for the conduct of surveillance for foreign intelligence purposes.

FISA was passed in 1978 and at that time established for the first time a requirement that we get a judicial order in order to conduct certain kinds of foreign intelligence or counterintelligence activities within the United States. But at the time FISA was passed, it was clear that the Congress did not intend that FISA would cover electronic surveillance directed at non-U.S. persons outside of the United States for foreign intelligence purposes.

And as you noted in your opening statement, because of technological changes in the way international communications are carried, over time more and more such surveillance—that is to say foreign intelligence surveillance directed at non-U.S. persons outside of the United States—more and more of that began to fall within the technical definitions that required FISA court approval, even though that was not what Congress had intended.

So, in the FISA Amendments Act, Congress set up the procedure of Section 702, which the Deputy Attorney General described, to provide a degree of judicial supervision over some kinds of foreign intelligence surveillance of foreigners outside the United States.

Properly viewed then, Section 702 is not a derogation of the authority of the FISA court, but an extension of the court's authority over a type of surveillance that Congress originally had not intended would be subject to the court at all.

The extent to which this Nation involves the courts in foreign intelligence surveillance goes well beyond what is required by the Fourth Amendment and I think beyond what other countries require of their intelligence services.

The second point I want to make is to forcefully rebut the notion that some have advanced that the FISA court is a rubber stamp. It is true that the court approves the vast majority of applications that the Government presents to it. But that does not reflect any lack of independence or lack of care on the part of the court.

Quite the contrary, the judges of the court and their full-time professional staff review each application carefully, ask questions, and can request changes or limitations. And an application is not signed unless and until the judge is satisfied that the application complies with the statute and the Fourth Amendment.

And these are some of the best and most experienced Federal judges in the country, and they take seriously their twin obligations to protect national security and to protect individual rights.

Finally, we agree with the Ranking Member and the Chairman that we should strive for the maximum possible transparency about the activities of the court, consistent with the need to protect sensitive sources and methods. We have been working for some time to declassify the court's opinions to the extent possible.

But legal discussions and court opinions don't take place in a vacuum. They derive from the facts of the particular case. And I want to quote here from Judge Walton, who is now chief judge of the FISA court, who said in a letter to the Senate Intelligence Committee.

"Most FISC opinions rest heavily on the facts presented in the particular matter before the court. Thus, in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC's analysis would result in a remnant void of much or any useful meaning."

That is an excellent and pithy summary of the challenge we face in trying to declassify these opinions. Of course, as you know, we do provide copies of all significant opinions of the FISC to the Judiciary and the Intelligence Committees of both houses. And I can tell you that in light of the recent disclosures, we are redoubling our efforts to try to provide meaningful public insight into the rulings of the FISA court, again to the extent we can do that consistent with the need to protect our intelligence activities.

With that, Mr. Chairman, I am glad to answer any questions that you have.

Thank you.

Mr. GOODLATTE. Thank you, Mr. Litt.

Mr. Inglis, welcome.

TESTIMONY OF JOHN C. INGLIS, NATIONAL SECURITY AGENCY

Mr. INGLIS. Good morning, sir.

Mr. Chairman, Mr. Ranking Member, Members of the Committee, thank you for the opportunity to join with my colleagues here today from the executive branch to brief and discuss with the Committee issues that you have identified in your opening remarks. I am privileged today to represent the work of thousands of NSA, intelligence community, and law enforcement personnel who employ the authorities provided by the combined efforts of the Congress, Federal courts, and the executive branch.

For its part, NSA is necessarily focused on the generation of foreign intelligence. But we have worked hard and long with counterparts across the U.S. Government and our allies to ensure that we discover and connect the dots, exercising only those authorities explicitly granted to us and taking care at once to ensure the protection of civil liberties and privacy.

In my opening remarks, I would like to briefly review the two NSA programs leaked to the media a little more than a month ago, their purpose, and the controls imposed on their use—the so-called 215 program authorizing the collection of telephone metadata and the so-called PRISM program authorized under Section 702 of the Foreign Intelligence Surveillance Act Amendment.

Let me first say that these programs are distinguished, but complementary tools with distinct purposes in oversight mechanisms. Neither of the programs was intended to stand alone, delivering singular results that tells the whole story about a particular threat to our Nation or its allies.

Useful intelligence, the kind decision-makers should use as the foundation of thoughtful action, is usually the product of many leads—some of which focus and sharpen the collection of additional data, some of which help connect and make sense of that data, and the sum of which is intended to yield the decisive and actionable conclusions that enable timely and precise employment of traditional instruments of national power, such as law enforcement and diplomacy.

The first program, which we undertake under Section 215 of the PATRIOT Act, as you heard described earlier today, authorizes the collection of telephone metadata only. It does not allow the Government to listen to anyone's phone calls.

The program was specifically developed to allow the U.S. Government to detect communications between terrorists who are operating outside the United States and who are communicating with potential operatives inside the United States, a gap highlighted by the attacks of 9/11. In a phrase, this program is designed and solely focused on the seam between foreign terrorist organizations and the U.S. homeland.

However useful the data might be that is acquired under this program for other purposes, its use for any other purpose is prohibited. The metadata acquired and stored under this program may be queried only when there is a reasonable, articulable suspicion, one that you can describe and write down, based on specific facts that a selector, which is typically a phone number, is associated with a specific foreign terrorist organization.

During 2012, we only initiated searches for information in this dataset using fewer than 300 unique identifiers. The information

returned from these searches only included phone numbers, not the content, the identity, or location of the called or calling party.

Under rules approved by the court, only 22 people at NSA are allowed to approve the selectors used to initiate the search in this database. All queries are audited. Only 7 positions at NSA, a total of 11 people, are authorized to release the query results believed to be associated with persons in the United States.

Reports are filed with the court every 30 days that specify the number of selectors that have been approved and the disseminations made to the FBI of reports that contain numbers believed to be in the U.S.

The Department of Justice conducts onsite review of the program every 90 days. The executive branch, the Department of Justice, reports to the court and the Congress on renewal orders every 90 days, with an update on types of records sought, received, or denied on an annual basis.

The second program, which we operate under Section 702 of the FISA—the Foreign Intelligence Surveillance Act—authorizes the collection of communications for the purpose of foreign intelligence with the compelled assistance of electronic communications service providers, sometimes called telecommunications providers. Under this authority, NSA can collect communications for foreign intelligence purposes only when the person who is the target of our collection is a foreigner who is at that moment outside the United States.

As you have heard earlier, we cannot use this authority to intentionally target any U.S. citizen or other U.S. person, any person known to be in the United States, a person outside the United States if our purpose in targeting that person is to acquire information from a person inside the United States. This program has been key to our counterterrorism efforts. More than 90 percent of information to support the 50 disruptions that you will hear my colleague from the FBI briefly describe came from Section 702 authorities.

A bit more about oversight. The oversight on these programs operates under controls both internal and external to NSA, including actions taken by the Department of Justice, the Office of the Director of National Intelligence. There are regular onsite inspections and audits. There are semi-annual reports provided to the Congress and the Foreign Intelligence Surveillance Court.

The men and women at NSA are not simply committed to compliance with the law and the protection of privacy and civil liberties, but they are actively trained and must be held accountable to standards for that performance. This is also true of contractors. The actions of one contractor should not tarnish all contractors because they also do great work for our Nation.

In concluding, I would note that our primary responsibility at the National Security Agency—not alone, but across the Federal Government—is to defend the Nation. These programs are a core part of those efforts. We use them to protect the lives of Americans and our allies and partners worldwide.

Over 100 Nations are capable of collecting signals intelligence or operating a lawful intercept capability like the one you are hearing

described today. I think our Nation is amongst the very best in protecting privacy and civil liberties.

We look forward to the discussions that you have encouraged today, but I also appreciate that this discussion takes place at an unclassified level. I especially appreciate that the Committee Chairman and the Committee have allowed for the possibility that we might have classified discussions in an appropriate setting because the leaks that have taken place of classified information have constituted an irresponsible and real damage to the capabilities that we will describe today.

Finally, whatever choices are made by this Nation on the matter before us, in consultation and collaboration across the three branches of Government, I assure you that NSA will faithfully implement those choices in both spirit and mechanism. To do otherwise would be to fail to take the only oath that we take, to support and defend the whole of the U.S. Constitution. That includes the protection both of national security and civil liberties.

And sir, I look forward to your questions.

Mr. GOODLATTE. Thank you, Mr. Inglis.

Ms. Douglas, welcome.

TESTIMONY OF STEPHANIE DOUGLAS,
FBI NATIONAL SECURITY BRANCH

Ms. DOUGLAS. Thank you, and good morning, Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee. And thank you for an opportunity to be here today.

As you know, NSA and FBI enjoy a unique relationship, one which has been invaluable since the events of 9/11. The authorized tools available under the business records 215 and FISA 702 complement many of the other investigative tools we apply to our national security cases.

Together with human sources, physical surveillance, and other logical investigation, 215 and 702 play a role in providing us a more full understanding of our risks and gives us an opportunity to proactively address national security threats. I would like to give you just a few examples of where these tools have played a significant role, specifically in counterterrorism investigations.

And the first case I want to note is one that is very familiar to this Committee, and that is of Najibullah Zazi. In early September 2009, NSA, using their authorities under 702, intercepted a communication between an al-Qaeda courier located in Pakistan and an unknown U.S. person—U.S.-based person. This U.S.-based person was inquiring about efforts to procure and use explosive materials, and there was some urgency in his communication.

NSA advised the FBI as to this communication, as it represented a potential imminent threat to the homeland. Based on the nature of the threat information, the FBI initiated a full investigation and submitted a national security letter to identify the subscriber. The subscriber came back to an individual named Najibullah Zazi located in Denver, Colorado.

Additionally, NSA ran a phone number identifiable with Mr. Zazi against the information captured under 215. NSA queried the

phone number and identified other Zazi associates. One of those numbers came back to Adis Medunjanin, an Islamic extremist located in Queens, New York.

The FBI was already aware of Mr. Medunjanin, but information derived from 215 assisted in defining Zazi's network and provided corroborating information relative to Medunjanin's connection to Zazi. Just a few weeks after the initial tip by NSA, both Zazi and Medunjanin were arrested, along with another co-conspirator. They were charged with terrorist acts and a plot to blow up the New York City subway system.

As you already know, the Zazi case was the most serious threat to the homeland since 9/11. The importance of the Zazi case is that it was initiated on information provided by NSA, which they acquired under 702, their coverage of an al-Qaeda operative overseas. Without this tip, we can only speculate as to what may have happened.

This was a fast-paced investigation and one in which time was of the essence. The combined tools of 702 and 215 enabled us to not only begin the investigation, but to better understand the possible network involved in an active plot to the homeland.

I would like to also represent one case to you specific to the business record 215 authority. In 2003, the FBI initiated a case on an individual identified as Basaaly Moalin. It was based on an anonymous tip that he was somehow connected to terrorism.

In 2004, the case was closed without sufficient information to move forward on the investigation. However, 3 years later, in October 2007, NSA provided a phone number to the FBI with an area code which came back to an area consistent with San Diego. NSA found this phone number was in contact with an al-Qaeda East African-affiliated person.

Once provided to the FBI, we initiated an investigation, submitted a national security letter for the subscriber of the phone number, and determined that it was Mr. Moalin, the subject of the previously closed case. Subsequent investigation led to the identification of others, and to date, Moalin and three others have been convicted of material support for terrorism.

The relevance of this case to 215 is that if that information had not been tipped to the FBI, it is unknown if we would have ever looked at Mr. Moalin again.

As you know, there are many other instances of the use of these authorities and their application to counterterrorism investigations.

Thank you, and I am happy to answer your questions

Mr. GOODLATTE. Thank you, Ms. Douglas.

And I will begin the questioning. With regard to the point raised by the Ranking Member with regard to declassification, I just want to say that with regard to the Section 702 surveillance of noncitizens of the United States outside the United States, I think there would be few Americans who would be surprised that our Government engages in intelligence gathering with regard to those individuals.

And they would know it even more clearly by looking at the statutes and the amendments to the statutes that have been passed

over the years, that this type of activity is clearly authorized in the law.

With regard to 215, there is some controversy about whether this particular program is authorized under the law. And you will hear more about that shortly, and I will have a question myself. But my first question to you is why would it not have made sense—given the magnitude of this program, I am, frankly, surprised it has remained secret until recently for the several years that it has.

Why not simply have told the American people that we are engaging in this type of activity in terms of gathering the information? It doesn't give away any national security secrets in terms of the particular information gathered that might lead to successes like the one just described by Ms. Douglas. But it might have engendered greater confidence in the public with regard to understanding how the program works and public support for it.

Mr. Cole, Mr. Litt, would you care to answer that?

Mr. LITT. Sure. The problem is that I think that a judgment was made that to disclose the existence of this program would, in fact, have provided information to people who were seeking to avoid our surveillance, that it would tell them that we are looking for the communications they are having with Americans, and we are using that as a basis of tracking them and identifying their confederates within the United States.

And so, the judgment was made a number of years ago when this program was started that it should be kept classified. It was not, of course, withheld from the oversight Committees in Congress. And as others have noted, briefings on it were offered to all Members of Congress before it was reauthorized. But the decision was made that this is the sort of sensitive source and method that we don't want to disclose.

Mr. GOODLATTE. Do you think a program of this magnitude, gathering information involving a large number of people involved with telephone companies and so on, could be indefinitely kept secret from the American people?

Mr. LITT. Well, we tried.

Mr. GOODLATTE. I understand. [Laughter.]

So let me ask a follow-up question to you and Mr. Cole, and that would be how exactly does Section 215's wording authorize the Government to operate a program for the collection of metadata? Can you walk the Committee through the Government's interpretation of the statute that lends itself to arguing that you can do metadata collection?

Mr. COLE. Certainly, Mr. Chairman. I think you have to start with the fact that when you look at 215 and the orders that the court issues under 215, there are two of them. You can't look at them separately. You have to look at how they interact and operate together.

And I think that is very, very important in understanding how this is relevant to an investigation concerning these terrorist organizations. You can't just wander through all of these records. There are very strict limitations on how you can access or how you can use these under what is called the primary order.

You have to have reasonable, articulable suspicion that a specific phone number, which they call a selector, is involved with one of

these specified terrorist organizations. And then, and only then, after you have documented that reasonable, articulable suspicion can you query this database to find out what other phone numbers that specific terrorist-related phone number has been in contact with.

Mr. GOODLATTE. Let me follow up on that question because how is the collection of all of a telephone company's telephone metadata relevant to a foreign intelligence or international terrorism investigation, an investigation?

Mr. COLE. It is only relevant to the extent that you need all of that information in order to do the query of the reasonably articulated suspicion.

Mr. GOODLATTE. Well, certainly, the acquisition of the type of information collected under this program is relevant to an investigation of an individual or group suspected of terrorism. But how do you and how does the FISC rationalize the collection of all of the data as being relevant to an investigation?

Mr. COLE. There are two main reasons. One is the length of time that these records are kept by the phone companies varies, and they may not keep them as long as we keep them under this program. The court allows us to keep them for a 5-year period.

The phone companies don't necessarily do that. The periods vary, and some can be as short as 15 or 18 months.

Mr. GOODLATTE. Mr. Inglis, with regard to Section 702, what happens if you incidentally collect information from a U.S. person? Can you explain how the minimization procedures apply to that, and what do you mean by minimization?

Mr. INGLIS. Yes, sir. There are court-approved rules that we call minimization procedures. What they do is they say that if in targeting a foreign person under 702 who you believe to be in a foreign location to derive foreign intelligence, and you discover that you have also collected a communication that involves a U.S. person. They might be the person who has received that communication from your person of interest. They might be the person who sent that communication. They might be referenced in that communication.

We have an obligation to first examine whether or not that communication is pertinent to foreign intelligence. If the communication is pertinent to foreign intelligence, then we must take further action to essentially protect the identity of that U.S. person unless knowledge of that identity is important pursuant to the foreign intelligence purpose.

We would, therefore, suppress the identity of that U.S. person in any report that we would make that focused on the target of our interest, and we would take action if that communication was not of foreign intelligence relevance to essentially destroy that communication in place.

Mr. GOODLATTE. How long do you retain information collected under 702? And you may have just answered it, but is the incidentally collected information about U.S. persons retained as well?

Mr. INGLIS. Yes. So the incidentally collected information, unless it is relevant to a foreign intelligence purpose or it is evidence of a crime or imminent death or injury to a person, you would destroy that on site at that time.

Mr. GOODLATTE. And other information, how long is that retained?

Mr. INGLIS. We would otherwise retain that for about 5 years. Typically in our holdings, under BR FISA, the information is mandatorily destroyed at 5 years. For most of the rest of our collection, 5 years is the reference frame. We found that over time at about the 5-year point, it loses its relevance simply in terms of its temporal nature.

Mr. GOODLATTE. Thank you.

My time is expired. The Chair recognizes the gentleman from Michigan, the Ranking Member Mr. Conyers, for 5 minutes.

Mr. CONYERS. Thank you, Chairman Goodlatte.

There are a couple of questions here that haven't come up, and I would like to direct them to Attorney Douglas. If only relevant conversations can be secured under Section 215 of the PATRIOT Act, then why on earth would we find now that we are collecting the names of everybody in the United States of America who made any calls for the last 6 years or more?

Ms. DOUGLAS. Sir, we are not collecting names. 215 only collects phone numbers, the time and date of the phone call, and the duration of the phone call.

Mr. CONYERS. Well, how do you consider that to be relevant to anything if there is just collecting only the names—I mean, look, if this is an innocent pastime that we just do to keep busy or for some other reason, why on earth would we be collecting just the names—just the numbers of everybody in the United States of America for at least 6 years?

Ms. DOUGLAS. I can speak to the application against investigations. And in this case, for 215, it would be specific to counterterrorism investigations. That information enables us to search against connections to other—if there is communication between a U.S.-based phone number and a phone number that is overseas that is related to terrorism.

And I know that Mr. Inglis explained to you the reasonable, articulable suspicion standard by which we have to actually search against those phone numbers.

Mr. CONYERS. Well, here we are faced with the fundamental problem in this hearing. We are not questioning access. We are talking about the collection in the first instance.

In the first instance, when you collect the phone numbers of everybody in the United States for over 6 years, there wasn't anything relevant in those conversations. Now you have them, and what I have been getting out of this is that they may—this access may become valuable, Mr. Ranking Member, and so that is why we do it this way.

But I maintain that the Fourth Amendment, to be free from unreasonable search and seizure, means that this metadata collected in such a super-aggregated fashion can amount to a Fourth Amendment violation before you do anything else. You have already violated the law, as far as I am concerned. And that is, in my view, the problem.

And of course, to help further document, the first question that the Chairman of this Committee asked is why didn't we just tell everybody about it is because the American people would be totally

outraged, as they are getting now as they become familiar with this, that every phone number that they have ever called is already a matter of record. And we skip over whether the collection was a Fourth Amendment violation. We just say that the access proved in one case or two that it was very important, and that is why we did it this way.

I see this as a complete failure to take and—you know, we changed the PATRIOT Act to add relevancy as a standard because of this very same problem that has now been revealed to be existing. And so, I feel very uncomfortable about using aggregated metadata on hundreds of millions of Americans, everybody, including every Member of Congress and every citizen who has a phone in the United States of America.

This is unsustainable. It is outrageous and must be stopped immediately.

Mr. INGLIS. Sir, if I may complement the answer that Ms. Douglas gave? With respect to the question of relevance, of course, it must be legally relevant, and it must, therefore, have operational relevance. I would like to address the operational relevance and then defer to my colleagues from——

Mr. CONYERS. Well, you don't—wait a minute. We are holding—we are handling this discussion.

I asked her. Maybe somebody else can do it, but my time has expired. And I appreciate your volunteering to help out here, but it is clear to me that we have a very serious violation of the law in which the Judiciary Committee deliberately put in the issue of relevance, and now you are going to help me out and defer to somebody else. Well——

Mr. INGLIS. No, sir. I meant to actually provide additional information. I would be happy to take the question for the record if time is not allowing that.

Mr. CONYERS. Well, in all fairness——

Mr. GOODLATTE. Without objection, the gentleman is recognized for an additional minute to allow another member of the panel to answer the question if he so chooses.

Mr. CONYERS. No, I don't so choose. I am satisfied exactly what I have gotten from the witness that I asked the question to.

Mr. GOODLATTE. The Chair thanks the gentleman.

Mr. CONYERS. You are welcome.

Mr. GOODLATTE. And now recognize the gentleman from Wisconsin, Mr. Sensenbrenner, for 5 minutes.

Mr. SENSENBRENNER. Well, Mr. Chairman, at the risk of having the flag thrown at me for piling on, I want to get at the whole business of who decides what is relevant. Both the Chairman and the Ranking Member have said that the PATRIOT Act was amended in 2006 to include a relevance standard.

Yesterday, I got a letter from the Justice Department, which was at great length explaining this, and I would ask unanimous consent that this letter be placed in the record at this time.

Mr. GOODLATTE. Without objection, it will be made a part of the record.

[The information referred to follows:]

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

JUL 16 2013

The Honorable F. James Sensenbrenner, Jr.
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Sensenbrenner:

This responds to your letter to the Attorney General date June 6, 2013, regarding the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted as section 215 of the USA PATRIOT Act.

As you know, on June 5, 2013, the media reported the unauthorized disclosure of a classified judicial order issued under this provision that has been used to support a sensitive intelligence collection program. Under this program, which has been briefed to Congress and repeatedly authorized by the Foreign Intelligence Surveillance Court (FISC), the Federal Bureau of Investigation (FBI) obtains authorization to collect telephony metadata, including the telephone numbers dialed and the date, time and duration of calls, from certain telecommunications service providers. The National Security Agency (NSA), in turn, archives and analyzes this information under carefully controlled circumstances and provides leads to the FBI or others in the Intelligence Community for counterterrorism purposes. Aspects of this program remain classified, and there are limits to what can be said about it in an unclassified letter. Department of Justice and Intelligence Community staff are available to provide you a briefing on the program at your request.

In your letter, you asked whether this intelligence collection program is consistent with the requirements of section 215 and the limits of that authority. Under section 215, the Director of the FBI may apply to the FISC for an order directing the production of any tangible things, including business records, for investigations to protect against international terrorism. To issue such an order, the FISC must determine that (1) there are reasonable grounds to believe that the things sought are relevant to an authorized investigation, other than a threat assessment; (2) the investigation is being conducted under guidelines approved by the Attorney General under Executive Order 12333; and (3) if a U.S. person is the subject of the investigation, the investigation is not being conducted solely upon the basis of First Amendment protected activities. In addition, the FISC may only require the production of items that can be obtained with a grand jury subpoena or any other court order directing the production of records or tangible things. Finally, the program must, of course, comport with the Constitution.

The telephony metadata program satisfies each of these requirements. The lawfulness of the telephony metadata collection program has repeatedly been affirmed by the FISC. In the years since its inception, multiple FISC judges have granted 90-day extensions of the program after concluding that it meets all applicable legal requirements.

Of particular significance to your question is the relevance to an authorized international terrorism investigation of the telephony metadata collected through this program. First, it is critical to understand the program in the context of the restrictions imposed by the court. Those restrictions strictly limit the extent to which the data is reviewed by the government. In particular, the FISC allows the data to be queried for intelligence purposes only when there is reasonable suspicion, based on specific facts, that a particular query term, such as a telephone number, is associated with a specific foreign terrorist organization that was previously identified to and approved by the court. NSA has reported that in 2012, fewer than 300 unique identifiers were used to query the data after meeting this standard. This means that only a very small fraction of the records is ever reviewed by any person, and only specially cleared counterterrorism personnel specifically trained in the court-approved procedures can access the records to conduct queries. The information generated in response to these limited queries is not only relevant to authorized investigations of international terrorism, but may be especially significant in helping the government identify and disrupt terrorist plots.

The large volume of telephony metadata is relevant to FBI investigations into specific foreign terrorist organizations because the intelligence tools that NSA uses to identify the existence of potential terrorist communications within the data require collecting and storing large volumes of the metadata to enable later analysis. If not collected and held by NSA, the metadata may not continue to be available for the period that NSA has deemed necessary for national security purposes because it need not be retained by telecommunications service providers. Moreover, unless the data is aggregated by NSA, it may not be possible to identify telephony metadata records that cross different telecommunications networks. The bulk collection of telephony metadata—i.e. the collection of a large volume and high percentage of information about unrelated communications—is therefore necessary to identify the much smaller subset of terrorist-related telephony metadata records contained within the data. It also allows NSA to make connections related to terrorist activities over time and can assist counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, including persons and activities inside the United States. Because the telephony metadata must be available in bulk to allow NSA to identify the records of terrorist communications, there are "reasonable grounds to believe" that the data is relevant to an authorized investigation to protect against international terrorism, as section 215 requires, even though most of the records in the dataset are not associated with terrorist activity.

The program is consistent with the Constitution as well as with the statute. As noted above, the only type of information acquired under the program is telephony metadata, not the content of any communications, not the identity, address or financial information of any party to

the communication, and not geolocational information. Under longstanding Supreme Court precedent, there is no reasonable expectation of privacy with respect to this kind of information that individuals have already provided to third-party businesses, and such information therefore is not protected by the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 739-42 (1979).

Moreover, it is important to bear in mind that activities carried out pursuant to FISA, including those conducted under this program, are subject to stringent limitations and robust oversight by all three branches of government. As noted above, by order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata it acquires. Instead, all information that is acquired is subject to strict, court-imposed restrictions on review and handling that provide significant and reasonable safeguards for U.S. persons. The basis for a query must be documented in writing in advance and must be approved by one of a limited number of highly trained analysts. The FISC reviews the program approximately every 90 days.

The Department of Justice conducts rigorous oversight to ensure the telephony metadata is being handled in strict compliance with the FISC's orders, and the Department of Justice and the Office of the Director of National Intelligence (ODNI) conduct thorough and regular reviews to ensure the program is implemented in compliance with the law.

The program is also subject to extensive congressional oversight. The classified details of the program have been briefed to the Judiciary and Intelligence Committees on many occasions. In addition, in December 2009, the Department of Justice worked with the Intelligence Community to provide a classified briefing paper to the House and Senate Intelligence Committees to be made available to all Members of Congress regarding the telephony metadata collection program. It is our understanding that both Intelligence Committees made this document available to all Members prior to the February 2010 reauthorization of section 215. That briefing paper clearly explained that the government and the FISC had interpreted Section 215 to authorize the collection of telephony metadata in bulk. An updated version of the briefing paper was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year.

Finally, we do not agree with the suggestion in your letter that the Department's March 9, 2011 public testimony on section 215 conveyed a misleading impression as to how this authority is used. Quoting a portion of that testimony, your letter states that it "left the committee with the impression that the Administration was using the business records provision sparingly and for specific materials. The recently released FISA order, however, could not have been drafted more broadly." In fact, key language in the testimony in question noted that orders issued pursuant to section 215 "have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately

briefed." We hope that the explanation above regarding the use of this authority to identify specific terrorism-related telephony metadata records helps to clarify the point.

The recent unauthorized disclosure of this and other classified intelligence activities has caused serious harm to our national security. Since the disclosure of the telephony metadata collection program, the Department of Justice and the Intelligence Community have worked to ensure that Congress and the American people understand how the program operates, its importance to our security, and the rigorous oversight that is applied. As part of this effort, senior officials from ODNI, NSA, DOJ and FBI provided a classified briefing for all House Members on June 11, 2013 and separate classified briefings to the House Democratic Caucus and the House Republican Conference on June 26, 2013.

The Department of Justice is committed to ensuring that our efforts to protect national security are conducted lawfully and respect the privacy and civil liberties of all Americans. We look forward to continuing to work with you and others in the Congress to ensure that we meet this objective.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance with this or any other matter.

Sincerely,

Peter J. Kadzik
Principal Deputy Assistant Attorney General

Mr. SENSENBRENNER. Part of that letter said that, in effect, that all of the phone calls, meaning the telephony metadata, had to be collected pursuant to the court order, and then it would be up to the security apparatus to make a determination of which needles in that large haystack were relevant to a foreign terrorist investigation.

Now doesn't that mean that instead of the court making a determination of relevance, it is the security apparatus that makes a determination of what is relevant and which of the less than 300 series of phone calls get picked out, according to your testimony? Mr. Cole, would you like to answer that?

Mr. COLE. Yes, Mr. Sensenbrenner, I am happy to address that. What the court does is it sets out a framework and a set of rules that we must follow to implement its orders.

Mr. SENSENBRENNER. But they don't determine which specific phone calls are relevant pursuant to the statute. You do that.

Mr. COLE. Well, we report to the court periodically on the implementation of this. We get it re-upped every 90 days when there are——

Mr. SENSENBRENNER. But you do that. The court does not.

Mr. COLE. We—the court does not——

Mr. SENSENBRENNER. Now if there was a criminal trial involved, it would be the court that would be determining a relevance standard pursuant to subpoena or for proffered evidence, wouldn't it?

Mr. COLE. Not necessarily, Mr. Sensenbrenner.

Mr. SENSENBRENNER. Okay. Well, then let me continue on this. You know, I have been the author of the PATRIOT Act and the PATRIOT Act reauthorization of 2006. Mr. Conyers was correct in saying why the relevance standard was put in, and that was an attempt to limit what the intelligence community could be able to get pursuant to Section 215.

It appears to me that according to this letter and according to the testimony of FBI Director Mueller, that relevant was an expansion of what could happen rather than a limitation when the law was amended, when relevant was not included in that statute. And doesn't that make a mockery of the legal standard because you are trying to have it both ways?

Mr. COLE. I don't think we are trying to have it both ways.

Mr. SENSENBRENNER. Well, you sure are because you are saying get—authorize, have the court authorize to get us the records of all the phone calls that are made to and from phones in the United States, including people who have nothing to do with any type of a terrorist investigation.

And then what you are saying is, is that we will decide what to pick out of that massive maybe a billion phone calls a day on what we are looking at, rather than saying this person is a target. Why don't you get an authorization only for that person's telephone records?

Mr. COLE. Again, going to the analogy of the criminal context, we would never in a grand jury situation or in an investigation that is a traditional criminal investigation even go to a court for the framework or the setting of rules or have sunsetting every 90 days of the authority or having compliance procedures——

Mr. SENSENBRENNER. But, Mr. Cole, with all due respect, the letter that I got from the department that you are the number-two person in says that you get the FISA court order because there are "reasonable grounds to believe that the data is relevant to an authorized investigation to protect against international terrorism," as Section 215 requires, even though most of the records in the dataset are not associated with terrorist activity.

So you gobble up all of those records, and then you turn around and say, well, we will pick out maybe 300 phone numbers out of the billions of records that you have every day, and you store for 5 years there, and all the rest of this stuff is sitting in a warehouse, and we found out from the IRS who knows who wants to have any kind of illegal access to it.

You are having it both ways. Let me tell you, as one who has fought PATRIOT Act fights usually against the people over on the other side of the aisle, Section 215 expires at the end of 2015, and unless you realize you have got a problem, that is not going to be renewed. There are not the votes in the House of Representatives to renew Section 215, and then you are going to lose the business record access provision of the PATRIOT Act entirely.

It has got to be changed, and you have to change how you operate Section 215. Otherwise, in the year and a half or 2½ years, you are not going to have it anymore.

And I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from New York, Mr. Nadler, for 5 minutes.

Mr. NADLER. Thank you.

The problem, obviously, Mr. Cole, with what we are hearing from this panel and what we have heard generally about the relevant standard is that everything in the world is relevant. And that if we removed that word from the statute, you wouldn't consider or the FISA court wouldn't consider that it would affect your ability to collect metadata in any way whatsoever, which is to say you are disregarding the statute entirely.

Now in public briefings, including to this Committee when we were considering reauthorization of Section 215, Administration officials have suggested that we view the authority of Section 215 as similar to a grand jury subpoena. And we specified in the statute that an order under Section 215 "may only require the production of a tangible thing if such thing can be obtained" through a grand jury subpoena.

Now can you give me, Mr. Cole, any examples where grand jury subpoenas were used to allow the bulk ongoing collection of telephone metadata?

Mr. COLE. It is difficult to go into specific examples of what grand jury subpoenas call for——

Mr. NADLER. Are there any such——

Mr. COLE [continuing]. Because those are subject to the rules of secrecy under Rule 6.

Mr. NADLER. Oh, come on. Are there any—are there any instances in the history of the United States that you know of where a grand jury subpoena said get every—get all information other than the content of a telephone call of all telephone calls in the United States or anything like that?

Mr. COLE. The admonition in the statute is that it is the types of records that are collected by grand jury subpoena, not that it is an identical process to the grand jury process because this is quite different from a grand jury process.

Mr. NADLER. All right. The type of data——

Mr. COLE. The FISA court involves——

Mr. NADLER. Excuse me. The type of data—the type of data is metadata unlimited to specific individuals.

Mr. COLE. The type of data is metadata and that——

Mr. NADLER. Unlimited to specific individuals because it is directed to everybody. Can you give—it is directed to every phone call in the United States. Can you give me any example where a grand jury subpoena has ever been used for anything remotely like that?

Mr. COLE. These are instances where we have gone to the court under the 215 requirements with the relevancy——

Mr. NADLER. You are not answering my question. Can you give me any example in the history of the United States where a subpoena, a grand jury subpoena was used for anything remotely resembling all metadata not to specific phones or to specific individuals?

Mr. COLE. Grand jury subpoenas have a different function than a 215 under the PATRIOT Act——

Mr. NADLER. I understand that. But the statute says——

Mr. COLE. It is hard to equate the two, Mr. Nadler.

Mr. NADLER. You are not answering my question. You are deliberately not answering. We know they have a different function. But the statute says that it may only require the production of a tangible thing if such a thing can be obtained through a grand jury subpoena.

Could you obtain through a grand jury procedure all metadata without being limited to specific named individuals or specific listed telephones?

Mr. COLE. I think it would depend on the circumstances, the limitations that the court would——

Mr. NADLER. Okay. Is there is any instance in history——

Mr. COLE [continuing]. The nature of the investigation, and then, yes, I think there are instances where a court in the right circumstances could authorize that.

Mr. NADLER. And could you give me any instance in history where that has ever been done?

Mr. COLE. I am not aware of one, sitting here right now.

Mr. NADLER. You are not aware of one. Could you supply us, please, with any instance because I believe this is totally unprecedented and is way beyond the statute. And you can't give me any instance because it doesn't exist.

So within a week or two, could you supply this Committee with that information?

Mr. COLE. Depending on the restrictions of Rule 6 of the Criminal Rules of Procedure, which prohibit disclosing grand jury information, we will take that record back for response—that question back for response.

Mr. NADLER. And can you give us an example where ongoing bulk collection has been allowed by virtue of grand jury subpoena

without a showing of the connection between those tangible things and a specific existing investigation?

Mr. COLE. Well, in this instance, we are showing it as a relationship to a specific investigation and specific phone number. We have to show reasonable——

Mr. NADLER. No, only for use of that information, not for collection of it.

Mr. COLE. Well——

Mr. NADLER. The statute is talking about collection. You are trying to confuse us by talking about use.

Mr. COLE. But the collection is only there and is only valuable if it is used, and the use is severely restricted——

Mr. NADLER. We are not talking about the use. The abuse of the statute, the abuse of civil liberties, the abuse of privacy is not only misuse, but miscollection. If you are collecting information about my telephone when you shouldn't be doing that, that is an abuse, even if you just simply file that and never use it.

Mr. COLE. We go to the court and describe to them exactly how the program will work, what the limitations are——

Mr. NADLER. Well, that—excuse me. That doesn't help me. The fact that the——

Mr. COLE. The court authorizes us to do this collection.

Mr. NADLER. Let me ask the question. The fact—the fact that a secret court, unaccountable to public knowledge of what it is doing, for all practical purposes unaccountable to the Supreme Court, may join you in misusing or abusing the statute is of no comfort whatsoever. So to tell me that you go to the FISA court is irrelevant if the FISA court is doing the same abuse of the statute.

So, again, can you give me some examples where ongoing bulk collection—I am not asking about use—has been allowed by virtue of grand jury subpoena without showing of a specific connection—without showing the connection between those tangible things and a specific existing investigation?

Mr. GOODLATTE. The time of the gentleman has expired. Mr. Cole will be allowed to answer the question.

Mr. COLE. We will take that similarly as a question for the record, and again, depending on the Rules of Criminal Procedure, we will see what we can get back to you, sir.

Mr. NADLER. And be aware, of course, that you could give it to us on a classified basis so that we could say our conclusions about that information.

Mr. GOODLATTE. The time of the gentleman has expired.

The gentleman from North Carolina, Mr. Coble, is recognized for 5 minutes.

Mr. COBLE. Thank you, Mr. Chairman.

Lady and gentlemen, good to have you all with us today.

Mr. Cole, let me start with you. Does the Fourth Amendment protection against unreasonable search and seizure apply to business records that could be obtained under 215 of the PATRIOT Act?

Mr. COLE. In particular, Mr. Coble, it does not apply to the metadata records. There is a case, *Smith v. Maryland*, where the Supreme Court ruled that these kinds of records, there is no rea-

sonable expectation of privacy. So there is no Fourth Amendment protection.

Mr. COBLE. Let me follow up with another question. So does a person then have a reasonable expectation of privacy in third-party business records?

Mr. COLE. People generally do not when they are in third-party hands because other people already have them. So the expectation of privacy has been severely undermined.

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

Mr. COLE. Yes, it does. There are a number of provisions in 215 that provide much greater protection than a grand jury process would. First, you have to go to a court. The court has to specifically review the program and the description of the relevance of these records, how they will be accessed, how they will be overseen, how there will be auditing, how there will be reporting on it, how there will be compliance with all of the rules of the court.

None of that takes place in the grand jury context.

Mr. COBLE. Mr. Cole, if the Fourth Amendment applies to foreign countries, do other American protections under the Bill of Rights apply, such as the Second Amendment under the due process clause?

Mr. COLE. Not necessarily, sir. The Fourth Amendment applies to U.S. persons who are outside of the United States, but it generally does not apply to non-U.S. persons who are outside of the United States.

Mr. COBLE. Mr. Cole, for the benefit of the uninformed, and sometimes I feel I am in that category, describe for the Committee the makeup of the FISA court, who sits on it, where it resides, and how it operates.

Mr. COLE. The FISA court is made up of judges, Article III judges, who have been nominated by the President. They cover any number of different Administrations. They have been confirmed by the United States Senate for a life appointment. They have their regular duties as District Court judges.

They are appointed by the Chief Justice of the United States to serve a term on the FISA court. There are 11 of them at any given time when you have a full complement. Each of them serves for a week at a time. They do not take care of their other court duties back in their home districts. They come and serve on the FISA court for that week, handling the applications.

There is a staff there as well that helps them and goes through it and is their clerks and some of their legal research assistants in this matter, and these last for, I believe, a term of 7 years that each judge can sit on the court.

Mr. COBLE. And I believe you, Mr. Cole, or one of the members of the panel may have indicated this. That to some extent, there is confusion as to the number of denials. There has been criticism leveled at the court, indicating very few denials. But I think you addressed that or one of you addressed that earlier in your comment. Do you want to add to that?

Mr. COLE. Yes, the level of denials is very similar to the same level of denials, which is small, for normal Title III in a criminal context—wiretap applications that are made to judges in regular courts. These are also done in chambers and with one party.

And the reason that the number is so low, first of all, is under the FISA, you have to have either the Attorney General or myself, or the Assistant Attorney General for the National Security Division, sign off on the application, very high-ranking officials in the department. So those applications are done very carefully in the first place.

Number two, the court, if they are not satisfied with an application that comes in, will tell us, and they will say you need more information. You need more restrictions. You need more requirements. So we will respond to that, and unless we satisfy them on all of their requirements, they will not sign the application. But more often than not, we can go back and find the additional information that they will need.

So there is something of an iterative process, but it is not unlike what goes on with a normal court every day in the Title III or the wiretap process.

Mr. COBLE. Thank you, Mr. Cole.

Mr. Chairman, I see my amber light. I would like to make one final statement. And this may not be the day for it, but Mr. Chairman, at some point, I would like to know the cost that has been expended in implementing this matter. If you would concur with that, I will pursue that at a later date.

Mr. GOODLATTE. I do concur with that. That is a very important piece of information to have, but I believe that is classified and would entail the subsequent hearing that I anticipate we will have in a classified setting where we can get answers to questions like that.

Mr. COBLE. I thank you, Mr. Chairman.

And good to have you all with us. I yield back, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Virginia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you.

Mr. Cole, did I understand you to say that you do not have an expectation of privacy on your phone records?

Mr. COLE. The Supreme Court ruled in *Smith v. Maryland* that you do not have a sufficient expectation of privacy in the phone records, as we have talked about it. The two——

Mr. SCOTT. Okay. That is fine.

Ms. Douglas, you indicated that you do not—you just get the numbers, not the names. Is there—if the numbers are relevant under whatever standard you are using, why are not the names equally relevant?

Ms. DOUGLAS. Well, the names are not collected in the metadata.

Mr. SCOTT. Well, where is the limitation? If you can get the numbers, why can't you get the names?

Ms. DOUGLAS. Well, we can through other legal process, and that is what the FBI will do. And so, if we receive a phone number——

Mr. SCOTT. No, I mean why don't you get it all at once? Where is the statutory limitation?

Mr. LITT. If I can answer the question here, I think that this indicates the fact that as the Deputy Attorney General said that this program is carefully set up in such a manner——

Mr. SCOTT. Where is the——

Mr. LITT [continuing]. As to minimize the invasion of privacy. One of the reasons——

Mr. SCOTT. Where is the statutory limitation?

Mr. LITT [continuing]. This program is found reasonable is the fact that the collection is very limited. The access is very limited.

Mr. SCOTT. Okay, okay.

Mr. LITT. And it is on that basis the court has approved the collection.

Mr. SCOTT. You have made up. That is because you have made up the program. I asked you a specific question where if this is available, where is the statutory limitation to what you can get? There is no statutory limitation. You are kind of making it up as you go along.

Mr. LITT. We are not making it up. We are seeking the approval of the court, and this collection——

Mr. SCOTT. Okay. What——

Mr. LITT [continuing]. Has been repeatedly approved by numerous judges of the FISA court, found to be in compliance with the statute.

Mr. SCOTT. Okay. Once you get the information, we know through the recent case on DNA, once you get DNA from somebody, you can use it in ways that you could not have obtained the information. But once you get it, you can run it through, no probable cause or anything, through the database.

My question is once you get this metadata, where is the limitation on what you can use it for?

Mr. LITT. It is in the court's order.

Mr. SCOTT. Where is the statutory limitation?

Mr. LITT. The court—the statutory limitation says that we can acquire the information as ordered by the court. The court sets limits on what we can do with it, and we adhere to those limits.

Mr. SCOTT. Well, is there a limit in criminal investigations or an exception for criminal investigations without a probable cause?

Mr. LITT. With respect to information obtained under Section——

Mr. SCOTT. Once you have got the metadata, can you run a criminal investigation without probable cause?

Mr. LITT. The metadata can only be used in pursuit of a terrorism investigation, and the only thing that is done with that is that telephone numbers are generated out of it for further investigation. It cannot be used for a criminal investigation unrelated to terrorism.

Mr. SCOTT. Wait a minute. You are talking about minimization?

Mr. LITT. The court's order provides that we can only use this data for purposes of a terrorism investigation.

Mr. SCOTT. Well, how does the court get to—why is the court required to place that limitation on it?

Mr. LITT. Because the court looks at the application that we are submitting and determines that with all of the restrictions that are imposed here, this is a reasonable method of collecting this infor-

mation and that it complies with both the statute and the Fourth Amendment.

Mr. SCOTT. Is there an exception under minimization for criminal investigations? Section (g) minimization procedures (2)(c) says that "notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or about to be committed, and that is to be retained or disseminated for law enforcement purposes" are exempted from the minimization requirements.

Mr. LITT. The procedures applicable to this kind of collection allow it only to be used on the terms specified by the court, and that is limited to generating the kind of information that you——

Mr. SCOTT. Well, is that——

Mr. LITT [continuing]. Talked about in pursuit of a terrorism investigation.

Mr. SCOTT. Okay. And so, the minimization exception for criminal investigations doesn't apply? If you trip over some criminal, some crimes——

Mr. LITT. We are not allowed to use this database for a criminal investigation unrelated to terrorism.

Mr. SCOTT. Well——

Mr. COLE. Mr. Scott, I think there may be some confusion——

Mr. SCOTT [continuing]. Then that is not what the code section says, but if that is what you want, maybe we need to change it. Does exclusionary rule apply? If you trip over some crimes and try to use it, does it—and including the principle of the poison tree, evidence of a poison tree, does that apply? Do those exclusions apply to stuff you may trip over that you have gotten through this?

Mr. LITT. We don't have the ability to trip over it in this. All this data is, is a series of telephone numbers and other identifiers. The only thing we can use this data for is to submit to the pool of data a telephone number or other identifier that we have reason to believe, based on articulable facts, is associated with terrorism. We can then say what numbers has that been in contact with?

Any other further investigation has to be done under some other authority.

Mr. SCOTT. Well, you have—Mr. Chairman, I apologize, but the limitation, the minimization exception for a criminal investigation, and when I asked the Attorney General Gonzales about what you could use this information for, he specifically indicated criminal—it is (g)(2)(C) under minimization requirements procedures.

He specifically said you could run a criminal investigation without the necessity, implying without the necessity of probable cause that you usually need to do to get information.

Thank you, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Alabama, Mr. Bachus, for 5 minutes.

Mr. BACHUS. Thank you.

Let me start by saying I am satisfied, at least from what limited knowledge I have, that the motivation behind this was legitimate and necessary for our national security to start this process, establishment of a court. And that from your testimony you have not, apparently not abused individual rights, and you have been an effective tool for terrorism.

But my concern is this could evolve into something that is quite different. The Star Chamber, I mean, in England started out as very good, very popular with the people. It allowed people to get justice that otherwise would not. But it evolved over time into a powerful weapon for political retribution by the king.

And my question is, in fact, I was reading the Supreme Court. It said it symbolized disregard of basic individual rights. They talk about actually the right against self-incrimination was a direct result of what happened in England when this court evolved into something quite different from what it was intended to do.

So my first question to all of you is how do we—how do we keep this from evolving into a weapon, an unchecked weapon by the Government to violate people's constitutional rights? And I am more concerned about Americans' rights, not terrorists' rights.

Mr. COLE. I think you raise a very excellent point, and I think the way this is designed, to make sure that all three branches of Government are involved, that this isn't just the king or the administration or an executive branch doing it. This is something that is done with permission of the court and supervision of the court, with rules laid down by the court to make sure it comports with the Constitution and the privacy rights of U.S. citizens.

It is done through statutes that are passed by this body, where we report back to this body and tell you what we have done with it and how it works and let you know what problems we have had and how we have fixed them. And it is also done with a lot of oversight within the executive branch, with Inspectors General and a number of different executive branch agencies that audit and oversee exactly how it is done and make sure it is done right.

I think that is how.

Mr. LITT. If I can just emphasize one point on that? This Committee has a very important role in ensuring that these authorities are not abused. We are required to report extensively on all activities under FISA to the Intelligence and Judiciary Committees of both houses, and we do that. We provide—we are required to provide copies of all significant opinions. We are required to provide reports about how these activities are carried out.

And we welcome your participation in that oversight to ensure that, in fact, we don't cross the bounds that the people want us to adhere to.

Mr. BACHUS. Anyone else? You know, when I learned about this, I was not aware of it at all, and I think the original response was that 14 Members of Congress knew something about this. Were those reports erroneous? Did——

Mr. LITT. I can't speak to what Members actually knew. I can tell you what we did to inform Members.

At the time when this legislation was first up for renewal in 2009-2010, we provided a classified letter to the Intelligence Committees that described this program in great detail.

Mr. BACHUS. How about the Judiciary Committee?

Mr. LITT. The letter was provided to the Intelligence Committee. The Intelligence Committee, my understanding is, sent an all-Member letter saying that this is available to all Members. This was our intention.

We also offered classified briefings to Members of this Committee, and I recall participating in one of those briefings. And in fact, the letters were also referenced in a statement on the floor by a Member of the Intelligence Committee, saying these letters are available, and I urge you all to come and read them. So we were not trying to hide this program.

Mr. BACHUS. Do you have any objection to the court opinions and periodic reports being made available to all Members of Congress?

Mr. LITT. I think we would have to take that back. I think the answer is probably no, but I think we would have to think about the implications of that.

Mr. BACHUS. Sure, and I think that is my response would be I want to think about it.

Mr. GOODLATTE. The time of the gentleman has expired.

Mr. BACHUS. Thank you.

Mr. GOODLATTE. The gentlewoman from California, Ms. Lofgren, is recognized for 5 minutes.

Ms. LOFGREN. Well, thank you, Mr. Chairman, and thanks to our witness.

I was thinking back to September 11th, one of the worst days I have ever spent in the Congress, and remembering that that weekend, after the attack, that members of the White House, the intelligence community, Members of this Committee and our staff, sat right at that table. We sat around that table and worked together to craft the PATRIOT Act.

And it is worth remembering that that original act was passed unanimously by the House Judiciary Committee, and it had the balance that we thought was important to protect the country, but also looking forward to protect the rights of Americans under the Constitution. And I share the concern expressed by Mr. Sensenbrenner that things have gone off in a different direction from that day.

Now I, as my colleague has indicated from Alabama, I don't question your motivation, which is to keep America safe. I mean, I know that that is what you are trying to do, and certainly we all want that.

But the concern is that the statute that we crafted so carefully may not be being adhered to as envisioned by us and as reported to us. And I just want to say this. I mean, yes, we have a system where there are checks and balances, but part of that is that the legislative branch needs to have understanding of what the executive branch and the judicial branch is doing, and we can't do that without information.

It has been discussed that we get these ample reports. And I just want to—I just recently reviewed the annual report on Section 215. Is it true, Mr. Cole, or isn't it true that the annual 215 report to the Committee is less than a single page and not more than 8 sentences?

Mr. COLE. I think that the 215 annual reports are quite a bit less than the 702 annual reports.

Ms. LOFGREN. I just ask the question. Is that about the size, is it your recollection?

Mr. COLE. I would have to go back and take a look to answer specifically.

Ms. LOFGREN. All right. Is it true that the report of the number of applications really gives the Committee information as to the amount of records and the number of entities impacted?

Mr. COLE. I am sorry?

Ms. LOFGREN. The number of applications, is there a direct correlation between the number of entities impacted by those applications or the number of records?

Mr. COLE. The number of entities impacted will depend on how many phone numbers have been called by the selector.

Ms. LOFGREN. Right. So you could report the number of applications, but it would have no relationship to the amount of records actually acquired?

Mr. COLE. It would not necessarily, no. But you can imagine it is small.

Ms. LOFGREN. Thank you very much.

I just—looking at this letter that was sent to Mr. Sensenbrenner, and I thank him for sending it out. And by the way, he and I have sent a letter to Attorney General Holder and to Director Clapper asking that U.S. companies be authorized to publish information regarding the Government request for user data under FISA.

I think it is terribly unfair that these companies that are being discussed around the world have no capacity legally to say what has been asked of them. So I know the letter was just sent. I would ask that you respond to that as promptly as possible just out of basic fairness to the companies involved.

But going back to the letter, it seems to me that if you take a look at page 2 of the letter, the second paragraph, it indicates that NSA has reported in the last calendar year fewer than 300 unique identifiers. This means that only a very small fraction of the records is ever reviewed by any person and is actually relevant to the records. Per se, that sentence indicates that getting all the data is clearly not relevant to a specific inquiry.

And then if you go on to the next page, and this really gets to my question and you have referred to it in the testimony as well, the consistency allegedly with the Constitution—now it is true that the Constitution in the Smith case indicated that there is no expectation, reasonable expectation of privacy with information held by third parties. Is it your position that that constitutional provision trumps a statute?

Can the Congress say the Constitution would allow you to capture every phone record, every photograph taken of an American at an ATM machine because that is in plain sight and that that constitutional provision would trump the ability of Congress to say, no, we are going to authorize less?

Mr. COLE. No. As long as whatever Congress does is consistent with or within the bounds of the constitutional provision——

Ms. LOFGREN. So Congress can do less?

Mr. COLE [continuing]. They can do that. Certainly.

Ms. LOFGREN. Can do less. I would just like to say that as to the FISA court, and I am sure that the judges take their obligation as seriously as you do. But the whole system of our justice system is set up in an adversarial way. And when you have only one party there, you don't have a counterparty making a case before the court.

The expectation that our system will work well, as it does in other environments, I think is misplaced. I share with Mr. Sensenbrenner the belief that this will not be able to be sustained. I look forward, Mr. Chairman, to our classified briefing, but I think that very clearly this program has gone off the tracks legally and needs to be reined in.

And I thank the Chairman for yielding to me.

Mr. GOODLATTE. The Chair thanks the gentlewoman and recognizes the gentleman from Virginia, Mr. Forbes, for 5 minutes.

Mr. FORBES. Thank you, Mr. Chairman.

And ladies and gentlemen, thank you for being here today.

I don't want to scream at you or yell at you, but you know we have got a lot of people across the country that would like to do that. And the reason this room is packed so much today and people were waiting in long lines is not just about this program. They kind of feel their country is shifting, and they feel, rightly or wrongly, that this Administration has adopted the philosophy that somehow the end justifies the means.

They feel like that more than any Administration in history this is an Administration that has used taxpayer resources to advocate their political agendas. They feel like more than any Administration in history, this is an Administration that has decided which laws they want to obey, which ones they want to ignore, and which ones they want to just rewrite.

They feel like more than any Nation in history, this is an Administration that has used enormous power of Government agents to oppress and harass U.S. citizens like they have seen with the IRS. And now they see this Administration using this unprecedented amount of data collection, first in their campaigns and then in Government, on amounts of data to use for the aforementioned goals.

And they don't know, every time they see a Benghazi, they don't know how many more boards they are going to pull up, and there is one that they don't know about or IRS programs that they pull up and they don't know another one that they might see and that there are other data programs that they don't know about.

And this is something that I just don't think we realize enough because over and over again, we hear Administration coming over here and saying this to us. They say, well, this isn't illegal, and you need to change the law.

And we need to emphasize part of this Committee is just because something is not illegal, it doesn't mean that it is not wrong. And when we look at something, you have got a difficulty because you can't even really come in here and explain what this program does. You can't tell us how many people are involved with it. You can't tell us the cost. You can't tell us what the court is saying.

But this is my question for you. There has to be an enormously large number of individuals administering this program. Can you tell us if any of those individuals have abused the power that they have within this program that has not been disclosed to the Congress or the American people, one? Because it would be hard for us to believe that there hasn't been some abuses.

Number two, what is your process for collecting that information to make sure those abuses don't take place, and how do you dis-

tribute that information? And three, has anybody ever been disciplined for abusing that information?

And any of you who have that information, I would love for you to offer it to us.

Mr. COLE. Let me if I can, Mr. Forbes, start by answering the questions that you have put. First of all, I think it is important to note that this program has been going on across a number of Administrations, and it is not unique by any means to this Administration. It has been for prior Administrations, too.

It is also done pursuant to court authorization and pursuant to statute, and so it is done not as some rogue matter, but as some matter that, in fact, has been authorized by law, authorized by the courts, and carefully scrutinized. And that gets to the main part of the question that you have asked, which is we know of no one—and I can let Mr. Inglis expand on that—who has ever intentionally or in any kind of wrongful way abused this.

There may have been technical problems that have happened here and there, but there has been nobody who has abused this in a way that would be worthy of or cause discipline. This program goes under careful audit. Everything that is done under it is documented and reviewed before the decision is made and reviewed again after these decisions are made to make sure that nobody has done the things that you are concerned about happening.

And those are valid concerns, and we take them into account by having these audit procedures and having the reporting that we do and the consultation both with the court and with Congress to make sure that those things don't happen. We have not, to my knowledge, disciplined anybody for this because our controls make sure this doesn't happen. But we do look for it and we look for it hard, and we haven't found it.

Mr. INGLIS. Sir, if I can just—I concur with Mr. Cole's remarks. Say across my time, I have been the Deputy Director now for 7 years, there have been no willful abuse of the 215 or the 702 program. In fact, the Senate Select Committee on Intelligence in the summer of 2012 said that in a formal report that in a 4-year review that they had detected no willful abuse of the 702 program.

I would say how would those be identified? In much the same way that Mr. Cole talked about. That there are a number of processes that review the formation of the selectors, the results generated by those selectors not just at NSA, but between NSA and the Department of Justice and the court, and there are any number of opportunities then to turn up a misappropriation of the resources dedicated to this program for some other purpose.

And would those persons who abused this program then be disciplined? Of course, they should be.

Mr. FORBES. And my time is expired. And I don't mean to cut you off, but I would love to have your responses for the record.

But when you guys tell me nobody has abused it, I thought Mr. Snowden abused it pretty badly. And I can't imagine if we had somebody like that doing it that we don't have at least that capacity. But I would love to have your responses for the record because I don't want to abuse other people's time.

And Mr. Chairman, I yield back my time.

Mr. GOODLATTE. Mr. Inglis, if you care to respond to the gentleman from Virginia's comment about Mr. Snowden, we would be happy to have it.

Mr. INGLIS. I would be happy to take that question for the record but would say here for the record that we do not have any evidence that Mr. Snowden abused the program as we have defined it today. He may have abused his trust in disclosing classified details of that program.

Mr. FORBES. But in all due respect—and I said I wasn't going to yell at you, and I am going to try not to. But that is exactly what the American people are really worried about, that somebody is getting their data and using it to disclose it in some other situation. And for the life of me, I don't understand how you guys parse that issue that is there.

So, Mr. Chairman, that is what is infuriating the American people. They are understanding that if you collect this amount of data, people can get access to it and use it in ways that can harm them, not just the United States of America. And that is what is concerning them, I think, in a lot of areas.

So, Mr. Chairman, I hope we can get a more elaborate response maybe for the record on that.

Mr. INGLIS. We would be happy to provide a response for the record, sir.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Let me thank you very much.

And I think it is important to make sure that as those of us who represent Americans, we appreciate what the intelligence community does. But the very idea that the Chairman and Ranking Member has held this hearing and that you are having any number of hearings, I think the issue is that we have to do something. We have to do more to be able to ensure the trust of the American people, and I raise these questions in the context of that.

One point that our Ranking Member made that if we cannot prove the necessity of this megadata collecting, then why are we necessarily doing it? And then we join with the Chairman that says it must show value, but we must also have the premise and the respect for the civil liberties of the American people.

So I pose the first question that deals with the idea that witnesses have testified in recent hearings that the phone record data were queried 300 times last year. How do you define a query, and how do you define the necessity of what I call trolling? And someone wanted to have me rephrase that. But the gathering of millions and millions of megadata gathering, how do you define query first, but then how do you justify that gathering?

Mr. INGLIS. Yes, ma'am. I will take that question. So, first, the court has approved procedures by which we can form a selector, and the reasonable, articulable suspicion standard was what we described earlier. And less than 300 times in 2012, we approved a selector for entering the database.

The court also approves what is called——

Ms. JACKSON LEE. So the query is based upon permission by the FISA court?

Mr. INGLIS. Yes, ma'am. The FISA court approves the rules, but as we have described in this hearing, the decisions about how to form those selectors are made at the National Security Agency and subject to auditing and review.

Ms. JACKSON LEE. So the query is made without a warrant. You go by criteria that has been set, and then you make a query and a preliminary oversight, if you will. Is that what you are saying?

Mr. INGLIS. That is correct, ma'am. And can I just then add that the court has also given permission to do not just first hop analysis, meaning what numbers are in contact with that selector, but to then from those numbers go out two or three hops. In many of the cases that Ms. Douglas referenced earlier, it was at the second hop. It was at that second connection that something of interest came that then caused the Federal Bureau of Investigation to apply their resources to essentially uncover or add additional information to terrorist activities.

Ms. JACKSON LEE. Once you do the query out of the 300, then what are the next step?

Mr. INGLIS. So that query, when it is returned, can be a first hop query or a second or a third hop query. That information is then reviewed by the National Security Agency analyst, and a report would be written and disseminated to the Federal Bureau of Investigation if we see something that would be of interest to them.

In many cases when a query is performed, nothing of consequence turns up. No connections that are untoward turn up. Therefore, no report would be made. But when——

Ms. JACKSON LEE. Let me ask Mr. Cole. Thank you very much.

Let me ask Mr. Cole when does the DOJ become engaged? The FBI, of course, is the investigatory arm. What is the DOJ's oversight role more specifically? And how do you utilize the FISA court?

And as you do that, I have introduced bipartisan legislation dealing with the whole issue of the FISA court. It specifically asks for the release and the reporting of nonclassified opinions, which I think would contribute more to the trust of the American people. Would the Justice Department consider that? As you answer the question.

Mr. COLE. Thank you, Ms. Jackson Lee.

Certainly, we will consider that and work with you in regard to that.

The Justice Department's involvement here is to first make sure that the provisions of the statute in making the application to the court meet the standards that have been set out under law. So we are in the process of the application and making sure through legal advice that this, in fact, meets the standards set out by the statute as passed by Congress.

We also engage with the court for any questions that the court may have as to how this will be done, what kind of oversight will be done, what kind of limitations will be imposed. So that we end up with what is a court-authorized system, as described by Mr. Inglis, where we go and make those and have NSA make that determination. We will——

Ms. JACKSON LEE. Mr. Cole——

Mr. COLE [continuing]. Audit as well the determinations on a random basis to make sure that they are in compliance with what

the court has ordered. And if they are not in compliance, we will then report that to the court and then oversee, with the court's supervision, fixing those compliance issues to make sure that they do comply.

Ms. JACKSON LEE. Let me interrupt you so I can just get this last question in to Mr. Inglis. Mr. Inglis—thank you very much.

Mr. Inglis, let me just put this question out. We have had a release of data and a suggestion that the release that has been given by an individual that is now traveling around the world has a dastardly impact on knowing the system of collection of data, in the person of Mr. Snowden.

Can you speak generally to the idea of the impact, and can you also express the reason for 70 percent of the intelligence budget being used for contractors? I offer to you 2434 that is asking for a study for that, a bill that I have introduced. But I would like to know those two questions quickly, please.

Mr. INGLIS. Yes, ma'am. On the first question, I would say that the impact associated with Mr. Snowden's disclosures can be very, very harmful. It is too soon to tell whether, in fact, adversaries will take great note of the things that he has disclosed. But those capabilities, sensitive capabilities give them a playbook as to how they would avoid, right, the time and attention of the U.S. foreign intelligence and, for that matter, domestic intelligence organizations. So we are very concerned about that.

Mr. Litt would like to take the second question on contractors.

Mr. LITT. Yes, on the question about contractors, it is important to differentiate between two kinds of contractors. When we—when Lockheed Martin or somebody builds a satellite for us, that is a contractor. And so, when you talk about 70 percent of the budget being contractors, and I don't know that number offhand, but I will assume it is accurate, that includes all the contracts for building of satellites, for rental of space, and so on and so forth.

There is another category of contractors, which we call core contractors, which are the people who work in the building side-by-side with us. We have been working very hard to reduce the number of core contractors. I think in the last 5 years, we have reduced it by 36 percent.

Obviously, as a result of what has happened recently, we are looking again at whether certain categories of employees should not be contractors but should be made Government employees.

Ms. JACKSON LEE. Mr. Litt, we have had this discussion before.

Mr. GOODLATTE. The time of the gentlewoman has expired.

Ms. JACKSON LEE. I think you need help, and I would like to work with you on the legislation.

Thank you, Mr. Chairman. I would like to work with Mr. Litt to get that done and get that more——

Mr. GOODLATTE. The time of the gentlewoman has expired.

Ms. JACKSON LEE. I yield back.

Mr. GOODLATTE. The gentleman from Iowa, Mr. King, is recognized for 5 minutes.

Mr. KING. Thank you, Mr. Chairman. I appreciate this hearing and the testimony of the witnesses.

And I would first turn to Mr. Litt. And if I remember in your opening statement, you made mention that there wasn't restriction

on foreign intelligence surveillance prior to 1978 and the FISA court. Am I correct on that?

Mr. LITT. Yes, there was no judicial involvement.

Mr. KING. And I would submit that every Nation that I know of does foreign surveillance, and I don't know of other Nations that have judicial interference with the national security activity of foreign surveillance. And are you aware of any?

Mr. LITT. I can't speak for every Nation, but I think, generally speaking, you are correct that other Nations do not have their courts involved in foreign intelligence activities.

Mr. KING. So we are relatively unique in that, and neither do I understand why we would be concerned about the privacy or I will say the manufactured constitutional rights of foreign persons in foreign countries communicating with other foreign persons in foreign countries. I don't know why we would worry about their privacy.

And I don't know why we would worry about their privacy if there is a nexus that might happen to be in the United States, provided it didn't interfere with the rights of a U.S. person. Would you agree with that?

Mr. LITT. Well, I think from the point of view of the Constitution, it is correct that as the Deputy Attorney General said, that foreigners generally aren't protected by the Constitution. It is, nonetheless, true that we don't go out indiscriminately even as to foreigners. We only collect intelligence that has a valid foreign intelligence purpose.

Mr. KING. Yes, I understand the decency of the American people, but are we safer when we have judges deciding what we can surveil in foreign countries when there are foreign persons?

Mr. LITT. I think that we have found that the operation of FISA so far has allowed us to collect the foreign intelligence that we need to collect to protect the Nation.

Mr. KING. And I am hearing that. Just another way of asking questions about this. The phone companies collect a lot of data, and it was mentioned that you like to keep that data for 5 years, the metadata. But some only keep it for a year and a half.

If an agreement could be reached with the phone companies to maintain that data for a 5-year period of time, the duration that you request, wouldn't that be a firewall that would be more reliable than having to have the facility to restore all that data. Mr. Inglis?

Mr. INGLIS. Yes, sir. A reasonable question, and I think that there are some challenges that could be overcome. The first is that those companies collect that data for their own business purposes, not necessarily for the Government's.

And so, to rely upon what they hold themselves, there would have to be some basis by which you could either compel them or have some confidence that over time——

Mr. KING. A contractual agreement perhaps?

Mr. INGLIS. Pardon, sir?

Mr. KING. A contractual agreement perhaps?

Mr. INGLIS. Contractual agreement, possibly some liability protection. I will leave the legal framing of that to those who do statute and policy.

Two, you would have to have some confidence that you could efficiently, quickly query that data.

Mr. KING. Sure.

Mr. INGLIS. And so, if you had multiple providers, upwards of more than two providers, you would then run pillar to post querying that data to——

Mr. KING. Could I ask you to take a careful look at that and come back to me with a—with really a serious, reasoned answer? You are giving me a good answer so far. I would just like you to dig in——

Mr. INGLIS. Yes, sir, we will. So it turns out that the Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence, and the executive branch have all asked us a question along those lines. We would be happy to provide those to you.

Mr. KING. Curious. Okay. Well, my clock is ticking down, but I will stick with you, Mr. Inglis.

Now I am just going to ask this question, and it is not really a hypothetical, but point it out this way. And I am going to go through the list. So you have to check on each one, and I will come back if I need to.

Do we have the ability to not necessarily listen in, but track every phone call in the United States? That is one question.

Second one, do we have the ability to track any email in the United States? Do we have the ability to track Web site activity, any Web site activity in the United States?

Do we have the ability to enter into active chat rooms and in real time monitor? Do we have the ability to track any electronic credit or debit transactions, including the ATM transaction mentioned by the gentlelady from California? Do we have the ability to locate cell phones that are active?

Do we have the ability to track GPS locators, whether they are on vehicles or other devices? And then I know my clock is running down, so I want to pour a little more in here.

It is reported by the Obama campaign that they profiled voters with open source data and used that data to target voters for turnout and voter suppression. The IRS has used their search engine to target the President's political enemies.

Now if we can go this far, if all of these things are happening, if the answer is relatively yes to this list that I have given, then I would charge that it would be likely impossible to drive from Bangor, Maine, to Los Angeles without leaving a data trail in this country. And all of these things can be justified by the Constitution, by statute, by case law.

Am I close? And how would you respond to that big question?

Mr. INGLIS. Yes, sir. If the predicate to each of those eight questions is "in the U.S." and if the further predicate is "can the NSA," the answer would be no to all of those questions. Is it technically feasible to do some of those things? Of course.

And some of those things are, in fact, done by marketing organizations, by the telecommunications writers who attempt to determine the flow and the allocation of resource bandwidth to their resources. But the National Security Agency, as a foreign intelligence

entity, lacks the authority and, frankly, lacks the collection to do the things that are on that list of eight questions.

Mr. KING. I would like to drill into that a little deeper if I had the time, but I thank you and I will yield back.

Mr. INGLIS. Sir, we would be happy to take a visit at NSA or come down and talk to you in whatever detail you would prefer.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Tennessee, Mr. Cohen, for 5 minutes.

Mr. COHEN. Thank you, Mr. Chair.

First, I would like to make a point. One of the previous questioners took the opportunity to attack the Administration and said this Administration has used the ends to justify the means in many areas.

I believe, Mr. Cole, you said that all these programs started under the Bush administration and have not differed from Republican and Democrat. Is that correct?

Mr. COLE. That is correct, sir.

Mr. COHEN. I appreciate your clearing it up. And then to this question that the President and this Administration on the IRS, I believe it has come out that they not only looked at Tea Party, but they looked at liberal groups and any group that they felt was more than 50 percent political to look at in IRS. And it is wrong to question this President on those issues once the facts have come out to show that it was not a partisan or issue-driven area.

And I find—take umbrage on behalf of the Administration at such questions and such allegations.

Now let me ask you this, sir. Mr. Snowden, what security status did he have? He could see anything there that he wanted to? Was he limited in what he had access to?

Mr. COLE. Let me put that over to Mr. Inglis.

Mr. COHEN. Sure.

Mr. INGLIS. Mr. Snowden had a top secret special compartmented intelligence clearance. That is standard for someone in the U.S. intelligence community given access to top secret information.

He, as a system administrator, had additional privileges that he could then set the permissions on various devices within the information systems, who could access things and how you could move data around.

Mr. COHEN. Generally, how many people—how many people generally are in the same level as he was to access this information?

Mr. INGLIS. Across the population—and again, in this forum, I will be general in my description. But across the population numbering in tens of thousands, and you would expect hundreds of people would have those sorts of extraordinary permission, system administrator permissions——

Mr. COHEN. So tens of thousands of people could have done what Snowden did?

Mr. INGLIS. No, sir. I would say that perhaps hundreds. And could I make a further distinction between his privileges in terms of what he could control?

Like any organization, NSA has a side of its information architecture that is intended to make information available to people so that they might discover capabilities, they might find each other,

they might pass email to each other. It is intended to be a free exchange of information.

But then there is a production side that is much more rigorously controlled, and there is a need-to-know rule, philosophy on that side. Now Mr. Snowden took ruthless advantage of the former and did not have access to the latter, except in some limited circumstances in the training that he undertook in the last few months of his——

Mr. COHEN. I asked in a letter, and you responded to me—I believe I got it last night—about the background on the security processing of Mr. Snowden. And I was concerned that a high school dropout, not that there can't be great high school dropouts, but it shows you can't meet certain criteria.

Because basically finishing high school is you are going to jump through the loops. That guy wouldn't jump through the loops, and he has shown at other places he wouldn't jump through the hoops and he wouldn't do that. To put him in that type of top security level, I think, is questionable.

But it was said that the Associate Directorate for Security and Counterintelligence begins the clearance process. Is any of the work of the Associate Directorate for Security and Counterintelligence contracted out, or is that all done by Government employees?

Mr. INGLIS. I think the determinations of whether to grant a clearance or not, that is an inherently governmental function. And so, that would be retained by Government employees. But in the investigation, the determination of the facts and circumstances associated with anyone's clearance determination, some of that would be contracted out.

And I could provide the details——

Mr. COHEN. Does it concern you at all? Should it be contracted out, or should that be strictly in-house?

Mr. INGLIS. There is an inherently governmental decision to be made in that, and that, therefore, should be withheld and retained inside the Government. The production of information in terms of conducting interviews, investigations, I think that some of that can be reasonably contracted out such that the synthesis and an examination of that is done by someone that has the higher trust.

Mr. COHEN. And how did Mr. Snowden take this data with him? He has got certain information in Moscow with him now. How did he do that?

Mr. INGLIS. Sir, I don't actually know precisely how he took the information with him, and it is a matter of investigation. I think in due course, we will know, and we would be happy to provide that to you.

Mr. COHEN. But he would have probably taken it on some type of a disk or some type of a little with him?

Mr. INGLIS. I just——

Mr. COHEN. From a secure facility, I presume——

Mr. INGLIS. I would just be speculating. I think that that is possible.

Mr. COHEN. Well, should there not be some changes in the procedures to make sure that people don't leave that secure facility with disks or anything else?

Mr. INGLIS. Mr. Cohen, I would say that we are examining all of that. There are some controls already in the system about who can download to secondary storage devices——

Mr. COHEN. All right. Let me ask Mr. Cole. You mentioned that the judges come from different Administrations, the FISA judges. Would it surprise you to know that 10 of the 11 judges all came—were appointed by Republican Presidents?

Mr. COLE. These are—it wouldn't surprise me. It wouldn't surprise me either way. These are selections that are made by the Chief Justice.

Mr. COHEN. By the Chief Justice, who is a Republican appointee. And he has picked—10 of the 11 judges he has picked were appointed by Republican Presidents. Yet if you go back over history, back to Jimmy Carter, it is about the same number of years. There is a difference of 4 of Democratic and Republican Presidents. But he chose Republicans.

Do you think there should be some change to make sure that there is possibly an ideological balance on that FISA court?

Mr. GOWDY [presiding]. You can answer the question. The gentleman's time has expired, but you can answer the question.

Mr. COLE. I think those are issues that we can discuss, that we try to take partisan politics out of the judicial aspect of it, and it operates, I think, best when it is insulated from that.

Mr. COHEN. I thank the panel, and I thank the gentleman from the Palmetto State.

Mr. GOWDY. Thank the gentleman from the Volunteer State.

The Chair would now recognize the gentleman from Texas, Judge Poe.

Mr. POE. Thank the Chair.

Thank you for being here.

My background is, as the Chairman just mentioned, a judge. I spent 22 years at the criminal courthouse in Houston trying everything from stealing to killing. So I don't like criminals at all.

But I have looked at the Constitution and read it, and I am going to just read you one thing, one phrase that all of you know probably by memory. It is the Fourth Amendment, "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated. No warrants shall issue, except upon probable cause, supported by oath or affirmation, and particularly describing the place to be seized and searched and the persons or things to be seized."

And as we all know, generally speaking, historically, warrants are brought to judges by law enforcement and the judge signs or doesn't sign the warrant, issuing the paper to go out and seize that person in that specific place.

Now I have read that numerous times, and I don't see in here anywhere as an exception for national security. Do any of you see a national security exemption to the Fourth Amendment?

Mr. LITT. There is not a national security exemption, but several courts have held that there is—that the warrant requirement of the Fourth Amendment does not extend to the conduct of foreign intelligence. That is not to say that the reasonableness requirement doesn't apply.

Mr. POE. Okay.

Mr. LITT. But the warrant requirement——

Mr. POE. I just have a little bit of time. I understand your answer. We are not talking now about foreign intelligence. Let us set the foreign issue and terrorists overseas where they are running wild, set that aside.

Let us talk about searches and seizures in the United States of American citizens. Question, is there a national security exception to the Fourth Amendment when it comes to American citizens in the United States? Do you see that in the Fourth Amendment, any of you?

Mr. LITT. Again, there is not a national security exception. There is a case of the Supreme Court called *United States v. United States District Court*. It is possible to have foreign intelligence collection against Americans, and I offer you the situation of an American who is a spy for Russia. We can be collecting valid foreign intelligence there, even though that person is an American.

It happens that the Congress, in the FISA, has established warrant requirements for electronic surveillance and so on.

Mr. POE. I understand that. But the Fourth Amendment doesn't give that example.

Mr. LITT. With due respect, there are cases that say——

Mr. POE. Okay.

Mr. LITT [continuing]. There is an exception——

Mr. POE. We are going to argue until the sun goes down. The Fourth Amendment doesn't mention national security exception when it comes to the Fourth Amendment. That has been expanded throughout the years because of FISA, because of court rulings, but it is not in the Fourth Amendment.

And I think that we should remember that the Fourth Amendment was written because of what was going on with King George III, how he was going into people's homes in the United States—the Colonies in those days—and seizing things with his Redcoats without a warrant. That is the basis of it.

And I hope we don't get to a point in this country in the name of national security that we infringe and bruise the Fourth Amendment. I don't know about the four of you——

Mr. NADLER. Would the gentleman yield?

Mr. POE. I won't. Sorry. I don't know about the four of you, but I have been in the former Soviet Union when it was—we can't use this word anymore—Communistic. And I was there, and the actions of the citizens were constantly under surveillance by government.

And anything that was done, the government would say we are doing this for national security reasons because of those bad, old Americans overseas. We go into your homes. We bruise the concept of rights all in the name of national security.

That concerns me, and I hope, as we move forward as a Congress, we rein in the concept that it is okay to bruise the spirit of the Constitution in the name of national security.

Question, people who have had their—the law NSA violated. I think Snowden, I don't like him at all, but we would have never known what happened if he hadn't have told us. Do they have a recourse against the Government for improperly seizure of their records? Is there a recourse?

Mr. GOWDY. You may answer the judge's question. His time is expired, but you may answer the judge's question.

Mr. COLE. It depends on the nature of that seizure, depending on where they came from. For example, if it comes from a third party, it is not necessarily their records. But the phone company can certainly challenge the subpoenas. And if it was to be used against them in a court, they would be in a position to be able to challenge that use.

Mr. POE. I thank the Chairman. I have other questions I would like to submit for the record for the four panelists.

Mr. GOWDY. And I am confident that one of your colleagues will yield you time, Your Honor, since you have made it known that you want it. And if they won't, I will give you mine.

The Chair will now recognize the gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Cole, to follow up on some of the principles that you were just talking about, are you familiar with the case of *State v. Maryland* back in 1979, U.S. Supreme Court?

Mr. COLE. *Smith v. Maryland*?

Mr. JOHNSON. Yes.

Mr. COLE. Yes, I am, sir.

Mr. JOHNSON. Having to do with telephone records. Is that correct?

Mr. COLE. That is correct.

Mr. JOHNSON. And the question was whether or not there was a Fourth Amendment privacy interest in telephone records held by the telephone company?

Mr. COLE. That is correct. That was the issue.

Mr. JOHNSON. And how did the court rule on that issue?

Mr. COLE. The court ruled that there was no reasonable expectation of privacy in those records because they really belong to the telephone company. They didn't belong to the individual who they related to.

Mr. JOHNSON. Now is that case applicable to the case or to the issue of collection of metadata?

Mr. COLE. Yes, sir, it is.

Mr. JOHNSON. All right. And so, it was the collection of metadata, domestic-to-domestic phone calls metadata—not content, but metadata. Domestic-to-domestic, domestic-to-foreign, foreign-to-domestic. Is that correct?

Mr. COLE. That is correct. That is the metadata that we are talking about here.

Mr. JOHNSON. That is the program that Edward Snowden revealed. Is that correct?

Mr. COLE. That is correct.

Mr. JOHNSON. And he also revealed a program called the PRISM program. Is that correct?

Mr. COLE. That is correct as well.

Mr. JOHNSON. The PRISM program was a program that enabled the collection of Internet metadata, not content. Is that correct?

Mr. COLE. No, that is not correct.

Mr. JOHNSON. That is not correct. Okay. Explain to me what the PRISM program——

Mr. COLE. PRISM, and I can defer to some of my colleagues if I get any of this wrong. PRISM is under the 702 provision, which allows collection of content, but it is only content of non-U.S. persons who are reasonably believed to be outside of the United States.

Mr. JOHNSON. Okay. So that is the PRISM program which collects data, including content, from foreign communications, and then there is a minimalization process of eliminating domestic-to-foreign or foreign-to-domestic communications that were not relevant to national security. Is that correct?

Mr. COLE. That is generally correct, or some serious impending death or something like that, if there is an emergency. But generally, that is correct.

Mr. JOHNSON. Now that program, certainly we don't want our adversaries to know of what we are doing to watch them and to surveil them, foreign intelligence collection. We certainly don't want that to be exposed to the public?

Mr. COLE. No, sir. We do not.

Mr. JOHNSON. We need that to be kind of secret. But with respect to the data collection of domestic-to-domestic metadata, why is it necessary that the American people not know of that program? Why is it that that program has to be confidential, classified, secret?

Mr. COLE. I wasn't there at the time that it was classified, but I can give a little bit of speculation. The more people know about the way we go about trying to identify terrorist networks, the more they will avoid the kinds of ways that we use to do that. They may start to avoid communicating through phones.

Mr. JOHNSON. If they can't communicate through phones or can't communicate over the Internet, what will they do? Take a can on one end and put a string through it, and a can on the other end? Would they communicate like that?

Mr. COLE. It may be more difficult for them to communicate, but they may find other ways or other mechanisms or other providers to do it through.

Mr. JOHNSON. Well, it is always going to be a cat and mouse game in that regard.

Mr. COLE. That is correct.

Mr. JOHNSON. The American people, in my opinion, should know of the activities that affect them, the collection of telephone metadata is not personal information. However, the Government collecting this information and creating a database with which it can then use to investigate information that is acquired from foreign sources related to national security or terrorist act, the American people may conclude that they want their Government to collect that data.

But if they don't know that the Government is collecting the data and then they find out after it is leaked by someone who thinks that it is illegal, they find out in that way and then they start to lose confidence in their Government. Is that the situation that we find ourselves in today, anyone?

Mr. GOWDY. The gentleman's time has expired. You may answer the question.

Mr. JOHNSON. And by the way, I am a former judge, too. [Laughter.]

Mr. GOWDY. Your Honor, had I known that, I would have addressed you appropriately. Please accept my apologies, Your Honor.

Mr. JOHNSON. Thank you. Thank you, Mr. Chairman.

Mr. COLE. I think that is always the kind of issue that we wrestle with, which is the issue of trying to balance the need to protect the secrecy of some of these programs so that they will be effective with the need to be as transparent as we can about it because that is the kind of society we live in, where people participate in the decisions of government.

So those are always difficult balances to find, and that is the one we are trying to find and we find ourselves in right now.

Mr. JOHNSON. Thank you.

Mr. GOWDY. Thank you, Judge Johnson.

The Chair would now recognize the gentleman from Idaho, Mr. Labrador.

Mr. LABRADOR. Thank you, Mr. Chairman.

You know, I think more important than balancing those needs is to balance our liberties with our security, and I think that is what we are all concerned about today. We are looking at a system that is allowing the Government to collect everybody's metadata.

And just recently, I had the opportunity to travel through a series of countries, and I won't mention which country it is, but I was told before I went to that country that it was a police state. And I had heard that term my entire life. I had never really understood what it meant.

I had heard about the USSR and other Nations that were constantly surveilling their citizens and the people who visited that country, and I had never experienced what I experienced when I was there. Where I actually felt, literally, like I was being observed in very place that I went.

And the place was very secure. The place was very safe. There was very little crime. There were very few things happening. But it was because people had given up their liberty in exchange for security.

And I think that is what this Committee and I think what most Americans are concerned about, that we are going to give up our liberties in exchange for security. So I just have a few questions.

Mr. Litt, you said in your introductory statement that this was not a rubber stamp, that the judges were not a rubber stamp. But I had a hard time following your argument because your argument seems to be that because the judges are actually reading the material, it is not a rubber stamp. That seems to be a nonsensical argument to me.

I can either rubber stamp something by reading the material or not reading the material. That doesn't seem to be a determination of whether somebody is rubber stamping something. It seems to me that the difference—I was a criminal defense attorney. Never a judge, just a criminal defense attorney.

Mr. LITT. There is still time, sir.

Mr. LABRADOR. But no thank you. And it seems to me that there is always a check and balance on the power of the Government. Even when you go get a warrant when something happens, you

still have an adversary on the other side who can contest it in court, who can contest it in hearings, who can contest all those things. But that is not happening in the FISA court.

How can we address that?

Mr. LITT. So I have a couple of things to say, if I would? On your first point about the FISC being a rubber stamp, it is not just that they read the opinions. I mean, the idea of a rubber stamp is that they don't think about it. They just say you are giving me this, approved. And my point is that is not what happens.

They not only read it. They ask questions. They think about it. They push back. They do a careful study and analysis. So it wasn't—I didn't mean to suggest that it is only because they read the——

Mr. LABRADOR. Okay. All right.

Mr. LITT. On your second point, if I can just get philosophical for a second, this goes to one of the other points that I made in my opening remarks, and that is that what we have here is not—is the oversight of intelligence activities. It is not a litigation. It is not a criminal trial. It is not a civil trial.

This is a situation——

Mr. LABRADOR. And I understand that, but let me stop you there. And again, like Judge Poe did just a minute ago, I am not so worried about Section 702. I am not so worried about foreign intelligence. I am worried about you are gathering my information. It is my personal data that right now the United States has, and I am concerned about that.

I am concerned about you having the data, the metadata of every single American, and I think there should be some mechanism for us to be able to counter whatever the—and I have all respect for judges. I served as a lawyer for 15 years. They were usually right, and I was usually wrong. At least I would tell them that.

And I have a great respect for the legal system, for the judiciary system. But I am concerned when you don't have somebody on the other side, advocating for the rights of citizens of the United States, and it is something that we need to discuss here in this Committee and we need to figure out.

Now let us go to *Smith v. Maryland*. Mr. Cole, you mentioned *Smith v. Maryland*. It is totally not an analogous case, I believe, to what we are talking about here. What in the FISA statute or in the PATRIOT Act allows you to collect the data of every single American? That is what I am not understanding.

Because even if you follow *Smith v. Maryland*, you are talking about one individual who was suspected of committing a crime, and now you are telling me, and we have just recently learned, that we are collecting the metadata of every single American. And that concerns me.

Mr. COLE. I think there are two different issues that are involved here. *Smith v. Maryland* only goes to the issue of whether the Fourth Amendment applies to this kind of data, not whether the Fourth Amendment prohibits or allows the kind of collection under 215. That is a separate issue, and that is governed by the provisions of the statute of Section 215, which requires that in order for a court to approve the collection method that is being put forth, it

must have demonstrated to it that the data is relevant to the investigation of the specified terrorist groups.

The relevance is found in the combination of the two orders. The limitations first, where the court says you can't just roam through this any time you want, for any purpose you want, any day you want, any time you want. That cannot be done. You must find reasonable, articulable suspicion that the number you want to query is related to one of these terrorist groups.

Mr. LABRADOR. And I understand that. I believe that this argument, before my time has expired, but I think that determination has to occur before you collect the data, not after you collect the data. And I think that is what is wrong with what you guys are doing at this time.

But I appreciate your service. I appreciate you being here today.

Mr. GOWDY. I thank the gentleman from Idaho.

The Chair will now recognize the gentlelady from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair.

I was listening to the steps that you outlined for actually doing a query for the metabase, the metadata. And you were describing it as a way of showing what kind of constraints you use on this information.

So, Mr. Inglis, I would like to ask this. It sounds to me like, first, you have determined that the phone numbers of all the American people is relevant. Then in order to actually query the database, you have to establish reasonable, articulable suspicion. And in order to do that, you have said that 22 people at NSA can approve the query.

I wonder why is it that these 22 people have this power? They appear to be acting like court judges, and why would they be performing the job that the FISA courts were set up to do?

In other words, shouldn't the agency go to a FISA court to seek to retrieve data from a third party's database when they actually have need of specified information, and who are these 22 people?

Mr. INGLIS. So the court, in its order, has prescribed that particular procedure, has prescribed that those people, that number of people would have that authority, and that those people would follow court-ordered procedure and that they be trained to a standard, again approved by the court. And so, that is how we came to that particular implementation.

Defer to Mr. Cole for any of the legal analysis under that.

Mr. COLE. I think the only issue that I would take with how you describe it is by saying you first have to define or find that all of those records are relevant. This is a combination of two different court orders that come together, and they have to be read together as you look at this.

So it is not just one or the other. It is a whole program that is put together and presented to the court with the limitations and the oversight and the restrictions on how it can be accessed. Only with all of those considered as a whole does the court then make the relevancy determination.

Ms. CHU. Well, then let me continue on with the description that you gave with regard to how you proceed along these lines, which is that after they approve it, then it appears that after the fact you

have an audit, and then you file papers with the court on this audit. And then the Department of Justice reviews it.

Mr. COLE. It is not exactly in that order, and again, Mr. Inglis can correct me if I am wrong. There is the documented reasonable, articulable suspicion that takes place ahead of time. That is then reviewed again by supervisors ahead of time to make sure that it is being done properly and the standards are being applied properly.

The query is then made. On a periodic basis, the Department of Justice and the Office of the Director of National Intelligence, the Inspector General for NSA all sample and look at these things to make sure that, in fact, it is being applied properly and that it is being done properly and that there aren't any misapplications of it.

And there are periodic reports that go to the court of any compliance problems. We have to talk about every 90 days getting renewed authority. And when there are any issues that come up and any problems that are discovered, they are reported to the Congress and to the Intelligence and the Judiciary Committees as well.

So there are a lot of different checks and balances and audits that go on, both before the query is made, as well as after the query is made. And if there are problems found with the query, then that is all fixed, and whatever is collected is remediated.

Ms. CHU. Well, my concern with regard to the second half is that it is retroactive, and it seems that more of the protection should be on the first half of these steps that you are talking about. And are those documents with regard to your DOJ reviews of the queries, are those available to this Committee?

Mr. COLE. I would imagine that those would probably be classified documents. I would have to go back and check, but that is—it certainly would look at the facts that we have and how we get them and what the nature of them is. So my guess would be that those would be classified.

Ms. CHU. Are they—well, you said they were reviewed by Congress, but where?

Mr. COLE. I think that the review takes place. There are reports that are made. When leadership of the Committee or other aspects of the Committee want briefings in classified settings, those are arranged as well.

Ms. CHU. Okay. Well, let me ask also about the issue of court documents. I understand that secrecy is essential when conducting any intelligence investigations. But we have to ensure that these efforts are working within the legal framework of the Constitution.

We learned earlier this week that a FISA court agreed to declassify documents from a 2008 case in which Yahoo! raised concerns about NSA's data collecting program, and other requests have been filed by companies that are in similar situations. What is the harm in releasing this type of information? Shouldn't the American public be informed about how this type of information is collected and used, and why couldn't you redact the information that is of security concern?

Mr. GOWDY. You may answer the question. The gentlelady's time has expired, but you may answer her question.

Mr. LITT. I think we all agree that that is something that should be done. It is difficult to do because, frequently, the classified infor-

mation is fully intertwined with the legal analysis. But we recognize that it is our obligation to make as much of this available to the public as we can, and we are working as hard as we can to accomplish that.

Ms. CHU. Thank you.

Mr. GOWDY. Thank the gentlelady from California.

The Chair will now recognize the gentleman from Texas, Mr. Farenthold.

Mr. FARENTHOLD. Thank you, Mr. Chairman.

I don't know where to start here. I have got so many questions. I guess I will start with Mr. Cole.

Do you see any limitation under the Fourth Amendment or the PATRIOT Act on the Government's power to gather information in mass on people?

Mr. COLE. Yes, sir. I see very many limitations from both the Fourth Amendment and from the PATRIOT Act and from the FISA Act. There are many, many limitations that are put in and many, many checks and balances, both through the United States Congress and the courts.

Mr. FARENTHOLD. All right. So let us go over a couple of those. I assume you would have to go to the FISA court, and those are one of the checks and balances. Could you go to the FISA court and argue that you had a right to obtain, say, either an individual's or every American's tax return. Could you argue that with a straight face?

Mr. COLE. Well, I think they——

Mr. FARENTHOLD. I have got a long list of them. Yes or no.

Mr. COLE. Any individual's tax return, there are separate laws that cover the acquisition of tax returns.

Mr. FARENTHOLD. All right. So you can get tax returns. Could you get at somebody's permanent record from school?

Mr. COLE. If it was relevant to the investigation, you could go to the FISA court and ask for that——

Mr. FARENTHOLD. Could you get somebody's hotel records?

Mr. COLE. If it was relevant to the investigation.

Mr. FARENTHOLD. Could you get records of everybody who stayed in a particular hotel at any time?

Mr. COLE. If you can demonstrate to the court that it is relevant to the investigation.

Mr. FARENTHOLD. Okay. Could you—you could get my Visa/Mastercard records?

Mr. COLE. If I can demonstrate to the court that it is relevant——

Mr. FARENTHOLD. All right. Could you demonstrate, could you argue with a straight face you could demonstrate the court to create a database of everybody's Visa and Mastercard, every financial transactions that happened in the country because Visa and Mastercard only keep those for a couple of years?

Mr. COLE. Mr. Farenthold, that is all dependent on exactly what I am investigating and what the relevance of information would be and how it would be used and how it would be limited. All of those factors have to go into it. It is not a simple yes or no, black or white issue. It is a very complicated issue.

Mr. FARENTHOLD. Could you get Google searches?

Mr. COLE. I am sorry, sir?

Mr. FARENTHOLD. Could you get all the searches I made on a search engine?

Mr. COLE. Again, it would depend. I would have to make a showing to the court that that kind of information was relevant to the investigation.

Mr. FARENTHOLD. Could you get all Google searches and then come back and say we are going to search them later when we have got that information?

Mr. COLE. It would depend on the way that I would be able to search them. And again, under 215 of these—of this statute that we are talking about, it is only if I can show that it is related to specific terrorist organizations. It is not for anything under the sun.

Mr. FARENTHOLD. Can you get the GPS data from my phone, too, probably?

Mr. COLE. I am sorry?

Mr. FARENTHOLD. You can probably make a good argument for getting the GPS data out of my phones or the mappings off where I use on my phones, too?

Mr. COLE. Again, there is great limitations on how I can do that and only if it is relevant to an investigation of those specific terrorist organizations.

Mr. FARENTHOLD. All right. But how is having every phone call that I make to my wife, to my daughter relevant to any terror investigation?

Mr. COLE. I don't know that every call you make to your wife or your daughter——

Mr. FARENTHOLD. But you have got them.

Mr. COLE. I don't know that they would be relevant, and we would probably not seek to query them because we wouldn't have the information that we would need to make that query.

Mr. FARENTHOLD. But somebody like Mr. Snowden might be able to query them without your knowledge?

Mr. COLE. I don't believe that is true, but Mr. Inglis could answer that. I don't think he would have access to that or be able to do it.

Mr. FARENTHOLD. Okay.

Mr. INGLIS. We don't believe that he could query those without our knowledge, and therefore, those would be caught.

Mr. FARENTHOLD. All right. That is slightly reassuring.

The Fourth Amendment specifically was designed, as Judge Poe pointed out, to prohibit general warrants. How could collecting every piece of phone data be perceived as anything but a general warrant?

Mr. COLE. Because the phone data, according to the Supreme Court, is not something within which citizens have a reasonable expectation of privacy. It belongs to the phone company.

Mr. FARENTHOLD. So do I have a reasonable expectation of privacy in any information that I share with any company, my Google searches, the email I send? Do I have a reasonable expectation of privacy in anything, but maybe a letter I hand deliver to my wife in a skiff?

Mr. COLE. Those are all dependent on the facts and circumstances of the documents we are talking about. In the case of metadata, the Supreme Court specifically ruled that there was not coverage by the Fourth Amendment because of no reasonable expectation of privacy.

Mr. FARENTHOLD. I just want to point out how concerned I am about this data being so easily available, and just with a stroke of a pen, Congress and the President could change the search criteria as to what is searched or change the definition of a terrorist or search—the fact that this data exists in the hands of the Government. We saw what the IRS has done with tax returns, targeting people for political belief.

Let me ask you one other quick question. Why do these orders not violate the First Amendment? We have talked a lot about the Fourth Amendment, but why doesn't it violate the First Amendment, my right to freedom of association and my freedom of speech, having the Government know who I am talking to and when?

Mr. COLE. Again, these are issues that are looked at by the court in determining whether any constitutional rights are involved. We don't know who it is that has a specific phone number that is being called under this.

Mr. FARENTHOLD. And you can't look that up on one page on the Internet?

I yield back.

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

The Chair will now recognize the gentleman from Florida, Mr. Deutch.

Mr. DEUTCH. Thank you, Mr. Chairman.

Mr. Chairman, like many Americans, I was shocked by the revelations that the NSA has been secretly collecting phone records, Internet data on millions of Americans, thanks to a lawfully issued warrant approved by the Foreign Intelligence Surveillance Court, often called the FISA court. Many Members of Congress, myself included, were left completely in the dark about the extent of the NSA's data mining program, and I worry about the balance between legitimate national security needs and the constitutionally protected rights of all Americans.

The Government is stockpiling sensitive personal data on a grand scale. Intelligence officers, contractors, and personnel only need a rubber stamp warrant from the FISA court to then learn virtually everything there is to know about an American citizen.

The American people have a right to know about this program and at the very least know that such a program is operating within our system of checks and balances. And I believe Congress has a constitutional obligation to protect individual privacy rights, and I believe it is time to reexamine the PATRIOT Act, insert greater accountability into the FISA court, and ensure that our laws cannot be interpreted behind the backs of the American public.

With this hearing, this Committee has begun this important work of oversight and repair, and I thank the Chairman and the Ranking Member for calling this hearing. I thank the witnesses as well for participating.

Mr. Cole, I want to ask you about the October 2011 letter sent by then-Assistant Attorney General Ronald Weich to Senators

Wyden and Udall regarding Section 215. The disturbing information that Senators Wyden and Udall learned, however, was classified and was, thus, kept from the American public and even most Members of Congress.

Now Mr. Weich seemed to imply in his response to Senators Wyden and Udall that because Congress, or at least a select number of Members of Congress anyway, received intelligence briefings in accordance with the PATRIOT Act that there is no cause for alarm that the Government was using some sort of secret law, secret law to expand its surveillance activities.

Now the PATRIOT Act was passed in response to the horrific attacks on 9/11, designed to bolster national security by expanding the investigative techniques used by the Government and law enforcement officials to hunt down suspected terrorists, something that we all agree is important. But Section 215 had a standard of relevance, and there had to be concrete information linking a person to a terrorist organization before the NSA could secure that person's information.

Instead, what we have learned is that the FISA court has essentially rewritten Section 215 to say that any and all person's records may be considered relevant, therefore allowing the NSA to indiscriminately collect sensitive data on all Americans. The fact is in 2012, the Government made 1,789 requests to conduct electronic surveillance. The court approved 1,788, and the Government withdrew the other.

Now as a Member of Congress who was not privy to those intelligence briefings, I had to accept Mr. Weich's assurance that there is no secret law. But in the aftermath of these recent leaks, however, it seems that there may be secret laws. Laws not passed by Congress. Laws not publicly interpreted by the Supreme Court, but rather secret laws born out of a classified interpretation of the PATRIOT Act by the FISA court.

The New York Times recently reported that the FISA court has quietly become almost a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues. I would point out with only the arguments of the Federal Government alone to be considered.

Now even a former FISA judge has come forward with concerns that the body has become a de facto administrative agency, which makes and approves rules for others to follow. Now that it has become public that FISA courts have broadly, perhaps even unconstitutionally, redefined the relevance standard in Section 215, is it still the department's position that the Government isn't essentially operating with a secret playbook?

Mr. COLE. Mr. Deutch, I don't think we are operating with a secret playbook. There is, again, as we have discussed in many instances in our hearing today, the tension that exists between maintaining the integrity and the secrecy of some of the national security investigative tools that we use and making sure that people know about it.

We have, in the course of the reauthorization of the PATRIOT Act, on several occasions done classified briefings, made individual——

Mr. DEUTCH. Mr. Cole, I am sorry to cut you off, but I only have a second left. Let me just broaden the question then for a second

because I am speaking about these decisions that the FISA courts make as the supreme arbiter of this law.

And stepping back for a moment at a more basic level, does the panel understand why the American people may find this revelation shocking, that secret court rulings could expand the powers of the Federal Government beyond perhaps what was originally authorized by law and that an entire chapter in our laws is being written outside of the three branches of Government altogether?

Mr. COLE. I think, again, this is an area where we are looking to see what kinds of opinions from the FISA court we can make public. These are things that we are trying to do and trying to go through.

All significant opinions and all significant pleadings that have been filed with the FISA court are made available to the Committees, to the Intelligence Committee and Judiciary Committee, so they can see them. We are not trying to keep them secret. We are just trying to maintain the classified nature of some of these.

But these are issues that we are trying to grapple with and trying to determine what we can let out so that we can have this broader discussion.

Mr. GOWDY. I thank the gentleman from Florida.

The Chair would now recognize the gentleman from North Carolina, the former United States attorney, Mr. Holding.

Mr. HOLDING. Thank you, Mr. Chairman.

In a different professional capacity, I successfully used FISA warrants to investigate, disrupt, and prosecute terrorists and terrorist acts, and I can attest that not only are they effective, but there are very high burdens and hurdles to use FISA warrants. And they are significant.

But I want to step for the few moments that I have outside of the prosecution of terrorism and investigation of terrorism and just talk about the use of telephone records in everyday, garden-variety criminal cases, whether they are public corruption cases, fraud cases, drug cases. And Mr. Cole, I will direct my questions to you.

If you could step through for us how the Department of Justice prosecutors and investigative agencies obtain telephone records just in garden-variety cases and how they are ultimately used?

Mr. COLE. There are two different ways we do it, pursuant to the law. Historical telephone records that exist for prior calls we can get with grand jury subpoenas in a normal criminal case. Those can be issued by a prosecutor, delivered to the telephone provider, and ask for a range of data.

Mr. HOLDING. So no judicial involvement, just a grand jury involved?

Mr. COLE. There is no judicial involvement, just the grand jury involvement, and the prosecutor defines the scope and the nature and the numbers that are involved.

Mr. HOLDING. So the prosecutor could request telephone records going back as long as they want to, the only limitation being does the telephone company still have those records?

Mr. COLE. There would be one additional limitation. The telephone company could challenge the subpoena as being overly burdensome and irrelevant to any reasonable investigation, and the

court could take that up, which would be in a sealed proceeding because it is a grand jury proceeding. So it wouldn't be public.

Mr. HOLDING. And what would the standard be that the judge would use to evaluate the motion to quash?

Mr. COLE. Generally, relevance to the investigation.

Mr. HOLDING. So the Fourth Amendment doesn't come into play there?

Mr. COLE. Not for telephone records. It does not.

Mr. HOLDING. And this is available to prosecutors, Federal prosecutors across the country?

Mr. COLE. Yes, it is.

Mr. HOLDING. And the only showing that they have to make to the grand jury is what, that it is relevant?

Mr. COLE. That it is relevant.

Mr. HOLDING. And once you have gotten the telephone records and it shows let us say hits between the person, the subject that you are investigating and a relevant other person in the investigation, then what do you do to start listening to those telephone calls?

Mr. COLE. Well, if we wanted to listen to any telephone calls, and that would obviously be just telephone calls that would start happening into the future, we would have to go to the court and seek authorization under Title III of the U.S. Code to get a wiretap. And we would have to show probable cause to believe that, in fact, the person talking on the phone was involved in criminal activity and that through that phone they were discussing criminal activity. And we would obtain evidence of that criminal activity by listening to the calls.

Mr. HOLDING. Would you hazard to make a guess of how many wiretaps are in use on a daily basis?

Mr. COLE. I couldn't hazard a guess, but there are a fair number of them.

Mr. HOLDING. Probably hundreds perhaps?

Mr. COLE. Probably.

Mr. HOLDING. As far as my friend Mr. Scott was talking about, if you find evidence of some other criminal conduct during an investigation, let us say during a Title III wiretap, you are investigating one crime, you hear a conversation that suggests that another crime is being committed, are there any limitations on use?

Mr. COLE. Generally not, other than the restrictions on how you can use wiretap information. There are restrictions on that and the secrecy that is involved in those and the protection of innocent calls. But generally, you can use that information if it relates to other criminal conduct, according to the rules of procedure in the law.

Mr. HOLDING. So in my take-away, having heard you describe in detail how the 215 program works and the 702 program works, the restrictions and the limitations on use from those two programs is much more restrictive and limited than what prosecutors and law enforcement are using on a daily basis throughout the United States investigating garden-variety crimes being committed by U.S. citizens?

Mr. COLE. In the main, there are some differences here and there. For example, the burden to get a wiretap may be a higher

burden than for 702 coverage, but it is a different burden if we wanted to do a FISA for somebody in the United States. That would be, again, a probable cause standard, but probable cause that they are involved in foreign intelligence.

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

Mr. GOWDY. I thank the gentleman from North Carolina.

The Chair will now recognize the gentlelady from Washington, Ms. DelBene.

Ms. DELBENE. Thank you, Mr. Chair, and thank all of you for being here today.

Last month, when Director Mueller appeared before this Committee, I stated that I agree with those who believe that greater transparency about the requests that governmental entities are making to Internet companies and providers will help inform the discussion that we are having on balancing national security with privacy rights and civil liberties.

And one of the questions that I asked the Director was how the FBI and the Department of Justice will respond to the request by Google that it be permitted to provide reports of the number of FISA national security requests it receives, as well as their scope.

And at the time, Director Mueller noted that this was being looked at. And so, I was wondering, Mr. Cole, if you are able to share with us what the response is to this request?

Mr. COLE. Unfortunately, this is a matter that is currently before the court. It is in litigation. So I can't say too much about it, other than to reiterate what Director Mueller said, which is this is a matter that we are, in fact, looking at and take seriously.

Ms. DELBENE. Now we do have some data that is out there already because in March of this year, Google worked with—I believe Google worked with the DOJ and the FBI to disclose in broad strokes the number of national security letters that Google receives. Correct?

Mr. COLE. That is correct.

Ms. DELBENE. And so, we do have some information. Do we know whether that information that was released has had any impact on national security?

Mr. COLE. Generally, it is hard to tell unless you have a substantial period of time afterwards as to whether or not it has an impact. So we haven't had enough time yet.

Ms. DELBENE. Okay, thank you.

The public also now knows that the telephone metadata collection is under Section 215, the business records provision of FISA, and that allows for the collection of tangible things. But we have also seen reports of a now-defunct program collecting email metadata.

With regard to the email metadata program that is no longer being operated, can you confirm that the authority used to collect that data was also Section 215?

Mr. COLE. It was not. It was the pen register trap and trace authority under FISA, which is slightly different. But it amounts to the same kind of thing. It does not involve any content. It is, again, only to and from.

It doesn't involve, I believe, information about identity. It is just email addresses. So it is very similar, but not under the same provision.

Ms. DELBENE. And could you have used Section 215 to collect that information?

Mr. COLE. Hard to tell. I would have to take a look at that.

Ms. DELBENE. Because I think it is important for us to know whether or not there is any limitations on the types of information within Section 215 that prevent you from collecting whether it is email metadata or GPS and geolocation information, et cetera. How broad is that authority?

Mr. COLE. Again, it is only as broad as what the courts can find under 215 that is relevant. But there are different authorities in FISA. So we would have to look to see how those all work together.

Ms. DELBENE. Mr. Litt, were you going to——

Mr. LITT. No, I was just going to say that it is important to remember that the 215 authority allows you to acquire existing records and documents, and it is limited to that.

Ms. DELBENE. Although you could argue that geolocation information may also be existing, and would you consider that to be metadata as well?

Mr. LITT. I think that the Director of the National Security Agency has stated that we are not collecting that under Section 215 and that we will come to the Congress and consult with the Congress before any decision was made to do so.

Ms. DELBENE. But you understand it is important for us to know what the breadth and limitations are, as we look at policy. And clearly, there is some confusion here right now. So we need to understand how it is being used and what information might be being collected so we can make sure intent is delivered appropriately.

So I agree with the President's view that we need to set up a national conversation on balancing privacy and security. But in order to have that conversation, have a productive conversation, we need information that is going to help fuel that conversation, information like the breadth of Section 215, et cetera. And so, I hope we can continue that and have—and get access to more information so that we can have a productive discussion going forward.

And thank you for your time. I yield back.

Mr. GOWDY. Thank the gentlelady from Washington.

The Chair would now recognize the gentleman from Texas, Judge Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman.

In answer to some of the other questions, you have provided an adequate defense. The trouble is we have seen the abuses of Government. We have seen the gathering of data. And I can tell you from having been here not when the PATRIOT Act was passed originally, but when it was extended back in my first term in Congress, it got down to where there were only two Republicans demanding any type of safeguard, I thought. And there were two of us that wanted sunsets.

I was the one that argued for 25 minutes in our 30-minute prehearing meeting demanding sunsets, and then my friend Dan Lungren had the amendments. And we got at least two sunsets on 206 and 215. And the argument I made for 25 minutes that turned my

colleagues, Republicans, around in our meeting was I have seen how there can be violations of due process if everyone is not very diligent, and we need the safeguards in order to have proper oversight.

And what we have seen and what has been disclosed of the monitoring scares me. We have had hearings in this room. People like Jerry Nadler have argued about dangers of Government having too much information. And from my experience as a judge and chief justice with State judges and Federal judges and having practiced before a very conservative Federal judge named Bill Steger and a very liberal judge named William Wayne Justice, I couldn't imagine anybody granting the kind of orders we have now seen granted. Just a blanket summary, go get all of these phone records.

And I understand the assurances, no, we don't have names with them. But isn't it true that you can go on public or private data, any individual, and secure the names for different numbers? Isn't that true?

Mr. COLE. There are ways to secure the names for any number of numbers, maybe not every single one.

Mr. GOHMERT. And I recall back in 2002, as a chief justice at a conference, getting into a debate with a CIA lawyer who was arguing, look, banks have all your financial records. Why shouldn't the Government?

And I was pointing out as a conservative it is because banks can't show up at your house, put you in handcuffs, throw you to the ground, and drag you off to jail, which has been done by the Government. So there is an important distinction.

And then we find out that though many of us opposed it, the Consumer Financial Protection Bureau has been gathering information on everybody's financial records. But they say the same thing that most of you are saying, look, we are not putting the names with it. But isn't it true that the Federal—that even the NSA can get access to the information gathered by the Consumer Financial Protection Bureau?

Mr. INGLIS. Sir, I imagine that could be true, but I would say that we can't pull the telephone numbers from this database under any circumstances other than that prescribed by the court.

Mr. GOHMERT. But you are entitled to go—I mean, we have had this debate in here. You are entitled to go on the Internet or go to private sources that any private citizen could and gather that information without violating any constitutional rights. Isn't that correct?

Mr. INGLIS. Certainly. But if the premise is we would do that to match names, identification, personal information against the telephone numbers, we don't have access to the telephone numbers unless we follow the prescribed rules of the court, pursuant to a terrorism investigation.

Mr. GOHMERT. But if you can gather the information that a private individual could and couple that with information that only the Federal Government we are now learning is gathering, then it really constitutes a grave threat to privacy. By the way, the Consumer Financial Protection Bureau said this, their Director said this in testimony before Congress.

The bureau has also issued regulations that limit the circumstance in which it may disseminate internally, share with other agencies, or disclose the public confidential information, share with other agencies. So they know they can share with other agencies if another agency or they feel it is helpful.

This begins to be a little scary, and the justification we get seems to be, well, but look, there are a handful of cases where we have avoided terrorism by really gathering all this private information. And it makes me think how many times could King George III have argued that, look, by putting officers in every one of your homes that we were uncomfortable with, we ended up being able to avoid a couple of problems of violence.

We don't want people in our homes, and that includes the Federal Government watching through a big eye through our computers.

And I appreciate you being here today. Thank you.

Mr. GOWDY. Thank the gentleman from Texas.

The Chair would now recognize the gentleman from New York, Mr. Jeffries.

Mr. JEFFRIES. Thank you.

Mr. Cole, am I correct that it is your position and the position of everyone on the panel that the telephone records of potentially hundreds of millions of Americans in the form of metadata, as has been discussed today, is relevant to a national security investigation?

Mr. COLE. They are relevant when they are only queried under the limitations that are described by the court, where you have to have reasonable, articulable suspicion that the phone numbert is connected to some terrorist matter and investigation.

Mr. JEFFRIES. So, fundamentally, it is your position that they are relevant because the court, the FISA court has articulated a set of criteria by which further inquiry can be undertaken. Is that correct?

Mr. COLE. They are. And they are relevant because you have to have the—it is the old adage of if you are looking for the needle in the haystack, you have to have the entire haystack to look through. But we are not allowed to look through that haystack willy-nilly.

Mr. JEFFRIES. Right. Now in terms of looking through that haystack of these phone records that are acquired based on reasonable, articulable suspicion, am I correct that it is 22 NSA individuals who are authorized to make the determination of reasonable, articulable suspicion? Is that right?

Mr. COLE. I will give that to Mr. Inglis to give you the numbers.

Mr. INGLIS. That is correct, sir.

Mr. JEFFRIES. Okay. So these individuals don't have to go back to the court in order to determine whether they can move forward with a more invasive inspection of the phone records of the Americans contained in the database that you have acquired. Is that correct?

Mr. INGLIS. They use the rules of the court to make the limited query that the court——

Mr. JEFFRIES. Right. They are using the rules of the court, but they are making the determination, not the court, as to the invasiveness of the further inspection. Am I correct?

Mr. INGLIS. On a case-by-case basis, they determine the selector.

Mr. JEFFRIES. Okay. Now, Mr. Litt, you have indicated that in your view, the FISA court is not a rubber stamp. Correct? That was your testimony?

Mr. LITT. That is correct.

Mr. JEFFRIES. And I think in response to the distinguished gentleman from Idaho, you said, well, it is not a rubber stamp because they read. They ask questions. They pushback. There is careful study and analysis. Is that an accurate characterization of your testimony?

Mr. LITT. Reasonably accurate. Yes, sir.

Mr. JEFFRIES. Okay. Now we just had the baseball all-star game yesterday, and of course, we know nothing is as American as baseball and apple pie. And if you think back on the history of baseball, I just took a quick look. I am a baseball fan myself.

Now Stan "the man" Musial, great hitter from St. Louis, his batting average lifetime, he was close to being in the top 25, .331, Stan "the man" Musial.

Babe Ruth, 10th all time. His lifetime batting average was .342. Ted Williams, the great lefty from the Boston Red Sox, his lifetime batting average was .344. Ty Cobb, the Georgia peach—I may disagree with some of his views on social justice issues, but he was a great hitter. The number-one hitter all time——

Mr. LITT. .363?

Mr. JEFFRIES [continuing]. Based on average, .366. [Laughter.]

Mr. JEFFRIES. Pretty impressive, though, but I am still going to continue to ask you questions about this dynamic.

Now I took a look. So these are the greatest hitters of all time. I took a look at what your batting average is as it relates to the FISA court, and I am a little troubled at what we were able to determine.

So am I correct that in terms of the total applications submitted since 1979, there were 33,949 applications submitted. Is that accurate?

Mr. LITT. I don't know the number. I wouldn't disagree with your number. I just don't know it off the top of my head.

Mr. JEFFRIES. Okay. And of that total number of applications, 490 it appears were modified. Is that correct? You have no reason to disagree with that number. Is that right?

Mr. LITT. Again, I don't know the answer.

Mr. JEFFRIES. Okay. So——

Mr. LITT. But if I can just add one——

Mr. JEFFRIES. Well, let me just make an observation.

Mr. LITT. Okay.

Mr. JEFFRIES. And I have got limited time here. One-point-four percent of the total number of applications made were modified. But what is even more troubling, since 1979, 11 applications were denied. Is that correct, 11?

Mr. LITT. Again, I will take your word for that.

Mr. JEFFRIES. Okay. So your success rate, your batting average, was 99 percent of the time that you have applied to acquire infor-

mation that could possibly include communication from one American to another American, yet you have taken the position that the FISA court is an independent check to protect the civil liberties and constitutional rights of Americans. Is that correct?

Mr. LITT. So I guess the answer is that we are not exactly talking about baseball here. We have a—if you imagine a situation where the kind of interaction we have with the FISA court is the FISA court throws a pitch, and we don't hit it. And the court says we want the pitch a little bit higher. Can you throw the pitch a little bit higher? And it is still not right. So make it a little more inside.

That is the interaction we have with the FISA court. They come back to us and tell us what we need to do to submit an application that will get approved.

Mr. JEFFRIES. Right. Those modifications, and I know my time has run out, only took place 1.4 percent of the times, and that is why I think we are all concerned, or many of us are concerned that there is not an appropriate check on behalf of the Americans whose records could be subjected to an invasive search.

I thank you all for your service, yield back the balance of my time.

Mr. LITT. May I say one thing briefly, Mr. Chairman?

Mr. GOWDY. Sure.

Mr. LITT. The number for modification there I think does not reflect the full number of times in which the court asks questions and comes back to us. My understanding is that that is simply—that comes at the very end of the process, but there is a substantial give and take before we get to that point. So that is not a full reflection.

Mr. GOWDY. The Chair thanks the gentleman from New York and now recognizes the gentleman from Utah, Mr. Chaffetz.

Mr. CHAFFETZ. I thank the Chairman.

And I thank the four of you for your service. I know how much you care for your country, and we do as well, and appreciate the dialogue. It is what differentiates the United States of America from most others.

So, Mr. Cole, is geolocation information metadata, or is it content?

Mr. COLE. That is an area of the law that is, I think, evolving in light of the Jones case, and it is one that I think the courts are now grappling with. It is not clearly as——

Mr. CHAFFETZ. The courts—the courts did rule in the Jones case 9-0. They were pretty clear. Justice Alito was also fairly clear that Congress needed to grapple with this as well. Has the Department of Justice issued any guidance on Jones?

Mr. COLE. We are in the process of looking through that. Jones was based mostly on a trespass——

Mr. CHAFFETZ. I know what it was.

Mr. COLE [continuing]. Opposed to a search and seizure.

Mr. CHAFFETZ. Have you issued any guidance on Jones?

Mr. COLE. We are in the process of looking through that to do it.

Mr. CHAFFETZ. That is not an accurate answer. My understanding is there are at least two documents that the Department

of Justice has issued to the Federal Bureau of Investigations, for instance. It was uncovered through a FOIA request. Almost every page of this was redacted.

So you have, indeed, actually issued guidance on Jones. Correct?

Mr. COLE. I will stand to be corrected. If you have those, yes.

Mr. CHAFFETZ. Will the Department of Justice provide to this body, to this Committee, the guidance on Jones?

Mr. COLE. That is something we will have to look into. There are lots of law enforcement——

Mr. CHAFFETZ. No, no, no. Wait a second. I know there are law enforcement issues. I know there are other things. Why would you not provide to the United States Congress, the Committee on the Judiciary, why would you not provide a copy of that guidance for this Committee?

Mr. COLE. If it discloses law enforcement sensitive information and techniques of how we go about fighting crime and finding criminals, then we may not feel free to disclose it.

Mr. CHAFFETZ. And to the Chairman of this Committee, I think this is one of the great concerns. So let me ask you again, is geolocation metadata, or is it content?

Mr. COLE. It is not content, as that would be called. It doesn't give you the content of anybody's calls. All it gives you is information about where they are.

Mr. CHAFFETZ. So you are saying, in other words, that geolocation you would classify as metadata?

Mr. COLE. I am not sure that it is one or the other. I think there are times where there are things that are in between, and this may be one of those. It is certainly not content. It probably tends more toward metadata. But again, this is an evolving area of the law.

Mr. CHAFFETZ. How is it evolving? I mean, we haven't—this is what scares me about what you are doing and how you are doing it. If you knew exactly where I was standing, you are telling me that that is not content?

Mr. COLE. That is not the content of your conversation, no. And other people may see you——

Mr. CHAFFETZ. So the content——

Mr. COLE. If you are standing out in public, any number of other people may see you there.

Mr. CHAFFETZ. So, but if I was standing on private property?

Mr. COLE. This is part of what Jones talks about is the trespass issue.

Mr. CHAFFETZ. And they ruled 9-0 that it was an overstep and an overreach. So are you collecting that data?

Mr. COLE. We are not collecting that data.

Mr. CHAFFETZ. Let me ask the NSA. Is the NSA collecting this data?

Mr. INGLIS. We are not collecting that data under this program. We believe that the authority could be granted by the courts to collect that attribute. We have not done that, and as Mr. Cole and Litt indicated earlier, the Director of NSA has given an affirmation to the Congress that before such time as we would reconsider that decision, we would come back to the Congress.

Mr. CHAFFETZ. How—going back to you, Mr. Cole. What other bits of information fall in this gap between metadata and content?

What is this third category that you are talking about? What is the right word for it?

Mr. COLE. I am not sure. It is just a third category, Mr. Chaffetz. I think there is metadata that was described by the court in *Smith v. Maryland*, which is the telephone records that we have been talking about today that were covered by the 215 program that we have been discussing today.

There is content, which is the actual—the conversations themselves that people have, and there are any number of things that may fall in between those, and it is not just a third category. It is probably a continuum.

Mr. CHAFFETZ. What else would be in that continuum?

Mr. COLE. I am sorry, sir?

Mr. CHAFFETZ. What else would be in that continuum?

Mr. COLE. It is hard for me to just hypothesize about all the many different things that could be out there and where they would fall in that continuum.

Mr. CHAFFETZ. There is a report out today about license plates and that information that is being collected by thousands of camera readers and stored about specific location. Does that fall within this category?

Mr. COLE. In which category?

Mr. CHAFFETZ. License plate readers.

Mr. COLE. The whole issue comes down to the reasonable expectation of privacy, and this is what the court bases its rulings on.

Mr. CHAFFETZ. Do you believe that I have a reasonable expectation of privacy about my specific whereabouts?

Mr. COLE. It depends on where you are and how many other people see you as——

Mr. CHAFFETZ. Do I have a reasonable expectation of privacy on private property?

Mr. COLE. In general, I think the courts are saying that there is a trespass theory that gives you a reasonable expectation of privacy, depending on whose property it is, whether it is your own or somebody else's, how many other people are there. These are all the types of issues that would go into that.

Mr. CHAFFETZ. My time is expired. But, Mr. Chairman, this is something we have to much more thoroughly understand. There is guidance out there, and I think this Committee should be able to see it.

Yield back.

Mr. GOODLATTE [presiding]. We are working our way in that direction, and there will be another hearing. You will be able to ask even more questions in a classified manner about questions you couldn't get answered here.

So we thank the gentleman, and the Chair now recognizes the gentleman from South Carolina, Mr. Gowdy, and thanks him for presiding for a period of time as well.

Mr. GOWDY. Thank you, Mr. Chairman.

I was listening to my colleagues and our witnesses discuss these issues, and for whatever reason, Mr. Chairman, my mind went to a guy by the name of Joseph Hartzler. I don't know whether he is still with the department or the U.S. attorney's office or not. He

was the lead prosecutor in a case called *United States v. Timothy McVeigh*.

And I thought to a presentation that Mr. Hartzler gave many years ago and the role that business records played in his ability to successfully prosecute that horrific act of domestic terrorism. And Mr. Chairman, I thought to myself, all right, we asked you, Mr. Hartzler, to prosecute the crime after it took place. What if we challenged you with the responsibility to prevent the next act of terrorism? What tools would you need to be able to prevent crime, as opposed to prosecute it in its aftermath?

And while this is at some level a debate between privacy and public safety, to me, it is also a debate between the difference between prosecuting something after it happens and then preventing it from happening in the first place. Mr. Hartzler used hotel records. He used business records where McVeigh went and purchased certain materials. He used—that was a very tedious, difficult case to prosecute, and the role of the business records played in it.

So this is what I would like to ask. I don't want to ask specific questions about the sections. I want to go to where the people of my district are who are not trained attorneys for the most part, trained law enforcement officials.

Mr. Litt, you would agree that the Constitution kind of sets the minimum standard by which Government must conduct itself——

Mr. LITT. Yes, sir.

Mr. GOWDY [continuing]. Is the minimum standard?

Mr. LITT. Yes, sir. And Congress has the power to set higher standards.

Mr. GOWDY. Exactly. So, in *Roper v. Simmons*, if the Supreme Court says you cannot put someone to death who was under the age of 18 at the time that they committed the offense, that does not keep Congress from saying we are going to raise it to 21?

Mr. LITT. That is correct.

Mr. GOWDY. Right. So who does get to decide whether or not our fellow citizens have a reasonable expectation of privacy?

Mr. LITT. It depends upon the purpose for which you are deciding it. For purpose of interpreting the provisions of the Fourth Amendment, as the Fourth Amendment, the Supreme Court is the ultimate arbiter. For purposes of determining what is the appropriate behavior, how do you want to regulate the actions of Government, that is Congress' role——

Mr. GOWDY. Well, I want to stop you. You say the Supreme Court is the ultimate arbiter. Are they the exclusive arbiter? Can the people weigh in on what they think they have a reasonable expectation of privacy in?

Mr. LITT. Absolutely. But——

Mr. GOWDY. Well, the Supreme Court doesn't have the benefit of public input.

Mr. LITT. Generally speaking, the public manages to get its voice heard in case in——

Mr. GOWDY. Well, I would hope they would listen to it. I mean, their job is not to weigh and balance—to Jason's point, if you are on private property but there is a helicopter above versus if you are

on private property and there are four other people at the picnic with you, I mean, you have no expectation of privacy in your face.

I don't think anyone would argue you have an expectation of privacy in your face. But that does not mean that our fellow citizens want Government to collect facial imagery data.

Mr. LITT. You know, I think that is exactly the right way to frame it, which is to say that the Fourth Amendment, as interpreted by the court, sets the minimum constitutional standard, but that the Congress, based on input from the people and whatever sources, can determine, no, this is how we want to regulate the behavior of our Government. And that set of regulations that we need to adhere to.

Mr. GOWDY. And technology can impact that. Agree technology can impact that?

Mr. LITT. I am sorry?

Mr. GOWDY. Technology? Technology can impact someone's reasonable expectation of privacy?

Mr. LITT. Oh, absolutely.

Mr. GOWDY. Culture?

Mr. LITT. Yes. All of those factors come into play.

Mr. GOWDY. I mean, there are already currently business records that an AUSA cannot access with a subpoena. Unless the world has changed, you can't get medical records with a subpoena.

Mr. LITT. Right. There are statutory restrictions on what you can get.

Mr. GOWDY. You can't get IRS tax returns with a subpoena.

Mr. LITT. That is right. You have got to go through a more elaborate process.

Mr. GOWDY. Both of those are business records, right?

Mr. LITT. That is correct.

Mr. GOWDY. So the notion that Miller stands for the proposition that all business records you have no expectation of privacy because there was a third party involved, we just came up with two examples where that is not the case.

Mr. LITT. Well, again, that was a case interpreting what the Fourth Amendment meant. The other examples you have given are cases where, as you said, Congress has gone beyond the minimum requirement——

Mr. GOWDY. But there was also a statute in play in Miller. There was a banking statute in play in Miller. You have read it more recently than I have. But——

Mr. LITT. No, I——

Mr. GOWDY. My point—my time is up. My point is this. All of us are asked back home by people who are not as well trained in the law as you all are, and there is this growing skepticism about the conduct of Government. And to the extent that the people can weigh in on what they have an expectation of privacy in, you can expect to see that scale balance back toward privacy and away from public safety unless we do a better job of regaining their trust and explaining why these programs are necessary.

Mr. LITT. So I couldn't agree with you more. I think that is absolutely right. I think as Deputy Director Inglis said before, in the intelligence community, we try very hard to keep in mind both the

protection of national security and the privacy and constitutional rights of Americans.

We think we have struck that balance in the right place, but if the people and the Congress determine that we struck that balance in the wrong place, that is a discussion that we need to have.

Mr. GOWDY. Thank you, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentleman.

And on that note, we thank this panel for giving a lot of answers. I think there are some that could not be answered here today, and therefore, you might anticipate that we will have a subsequent hearing in a classified setting and ask additional questions.

Whether it is of you four or something else, I don't know, but I want to thank each one of you for helping us to engage in a very thorough examination of the issues related to these two sections of the law and excuse you now.

Thank you again.

[Pause.]

Mr. GOODLATTE. Folks, if we could ask everyone to clear the hearing room, we are going to start with our second panel. No, just clear the area around the witness table.

And we would now invite our second panel to take their seats. And once you have taken your seats, we will invite you to stand back up again and be sworn.

So we will welcome our second panel and ask that each of you rise and be sworn in.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you very much.

Let the record reflect that all the witnesses responded in the affirmative, and we will now introduce our witnesses.

Our first witness is Mr. Stewart Baker, a partner at Steptoe & Johnson law firm here in Washington, D.C. And we would ask that the door in the back be closed so we can have a little more——

Mr. Stewart Baker is a partner at Steptoe & Johnson here in Washington, D.C. Mr. Baker also serves as a distinguished visiting fellow at the Center for Strategic and International Studies. Previously, he served as the First Assistant Secretary for Policy at the U.S. Department of Homeland Security.

He also served as general counsel of the NSA, where he led NSA and interagency efforts to reform commercial encryption and computer security law and policy. Mr. Baker has been a visiting fellow at the Hoover Institution and a fellow of the University Center for National Security Law.

Mr. Baker received his bachelor's degree from Brown University and his J.D. from the UCLA School of Law, where he was chief articles editor of the UCLA Law Review. And we are very fortunate to have him and his expertise with us today.

Our second witness is Mr. Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union and also serves as Director of the group's Center for Democracy. Mr. Jaffer previously directed the ACLU's National Security Project. Prior to joining the ACLU, Mr. Jaffer clerked for Amalya Kearse, the U.S. Circuit Court of Appeals for the Second Circuit, and the Right Honorable Beverley McLachlin, Chief Justice of Canada.

Mr. Jaffer earned degrees from Williams College, Cambridge University, and Harvard Law School, and we welcome his expertise and experience as well.

Our third witness today is Mr. Steven G. Bradbury, an attorney at Dechert, LLP, here in Washington, D.C. Formerly, Mr. Bradbury headed the Office of Legal Counsel in the U.S. Department of Justice during the Administration of George W. Bush, handling legal issues relating to the FISA court and the authorities of the National Security Agency. He served as a law clerk for Justice Clarence Thomas on the Supreme Court of the United States and for Judge James L. Buckley of the United States Court of Appeals for the D.C. Circuit.

Mr. Bradbury is an alumnus of Stanford University and graduated magna cum laude from Michigan Law School. We thank him for serving as a witness today and look forward to his insight into this complex topic.

Our final witness on the first panel is Ms. Kate Martin, Director of the Center for National Security Studies since 1992. She was formerly a lecturer at Georgetown University Law School and has also worked in the position of general counsel to the National Security Archive. She is currently a member of Constitution Project's bipartisan Liberty and Security Committee.

Previously, Ms. Martin was a partner with the Washington, D.C., law firm of Nussbaum, Owen & Webster. She graduated from the University of Virginia Law School, where she was a member of the Law Review and from Pomona College with B.A. in philosophy. We welcome her dedication and expertise in this area.

Thank you all for joining us, and we will begin with Mr. Baker. Each witness should summarize his or her testimony in 5 minutes or less. Your entire statement will be made a part of the record. And to help you stay within that time, there is a timing light on your table.

When the light switches from green to yellow, you will have 1 minute to conclude your testimony. When the light turns red, it signals that the witness's 5 minutes have expired.

Mr. Baker, welcome.

TESTIMONY OF STEWART A. BAKER, STEPTOE & JOHNSON, LLP

Mr. BAKER. Thank you, Mr. Chairman.

Mr. GOODLATTE. You may want to pull the microphone close and turn it on.

Mr. BAKER. Thank you, Mr. Chairman and Ranking Member Conyers. Yes, thank you very much.

It is a pleasure to be here, and I will say that this is not as unprecedented a climate as it may seem. I thought I would take advantage of the fact that it is my birthday to talk a little about the history of FISA. Here is a quote from the Cato Institute.

"If constitutional report cards were handed out to Presidents, the President would receive an F, an appalling grade for any President, let alone a former professor of constitutional law."

About the same time that they were saying that, the FISA court judge, chief judge, felt obliged to say, "We are not a rubber stamp. I carefully review every one of these applications."

This was the second term of Bill Clinton when many of these criticisms were very prominent. And quite frankly, I think they contributed to the FISA court at the time adopting, it turns out without legal justification, a set of restrictions on the conduct of intelligence that built a wall between law enforcement and intelligence that contributed directly to the FBI not being able to find the hijackers when they knew they were in the country but were not allowed to look for them because they were on the wrong side of the wall.

I say that because this climate and the search for ever greater protections for civil liberties does have a cost, and we don't know where that cost will be paid. That is why it seems to me that we need to be as careful as we can to ask the question what sorts of protections are there already. And I will confess, I was very surprised and a little troubled when I saw that initial metadata order.

Only when I came to realize that the order allowed the collection, but not the actual searching of that data, and that the searches were so carefully circumscribed that only 300 were made in a particular year, did I realize that when you look at the two sets of orders together, that there are actually extraordinary limitations on the ability of anyone at NSA to look at metadata of any individual. I contrast that to the fact that there are hundreds of thousands of subpoenas issued every year for metadata by State and local law enforcement with far fewer guarantees of protection for that data.

And then, finally, and I will close with this, the other cost that we are likely to pay here is that we are not the only audience for the debates that we are going through. It may feel like a family fight, but the neighbors are listening.

And indeed, Europe has already made it clear that they intend to punish everybody who participated in these programs if they possibly can. They intend to try to restrict our intelligence gathering by going after the companies that only did their duty in responding to orders that were lawful under U.S. law.

This is a fixed feature now of European public policy and diplomacy. It ignores the fact that, by and large, the U.S. record on protecting civil liberties and even this kind of data is much better. According to the Max Planck Institute, you are 100 times more likely to be surveilled by your own government if you live in the Netherlands or you live in Italy. You are 30 to 50 times more likely to be surveilled if you are a French or a German national than in the United States.

Only in the United States and Japan are there limitations on simply volunteering information to Government if you happen to have this metadata. As long as you have a good reason, by and large, you can give it over, and certainly law enforcement would appear to be a good reason.

And on this question of assembling a database of metadata, the Europeans don't do that because they passed a law telling every one of their carriers, you assemble the database. You maintain it. And if law enforcement comes calling or if you want to volunteer the information, you will have it.

We have never done that. We have never had a data retention law in the United States for civil liberties reasons, and that is one

of the reasons why we have ended up trying to collect this data and then imposing a set of limitations on when it is searched.

I will reserve and answer any questions you may have at the end of the discussion.

[The prepared statement of Mr. Baker follows:]

Oversight Hearing on the Administration's use of FISA Authorities

Committee on the Judiciary

United States House of Representatives

July 17, 2013

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP

Mr. Chairman, Ranking Member Conyers, members of the Committee, it is an honor to testify before you on such a vitally important topic. The testimony that I give today will reflect my decades of experience in the areas of intelligence, law, and national security. I have practiced national security law as general counsel to the National Security Agency, as general counsel to the Robb-Silberman commission that assessed U.S. intelligence capabilities and failures on weapons of mass destruction, as assistant secretary for policy at the Department of Homeland Security, and in the private practice of law.

To be blunt, one of the reasons I'm here is that I fear we may repeat some of the mistakes we made as a country in the years before September 11, 2001. In those years, a Democratic President serving his second term seemed to inspire deepening suspicion of government and a rebirth of enthusiasm for civil liberties not just on the left but also on the right. The Cato Institute criticized the Clinton Administration's support of warrantless national security searches and expanded government wiretap authority as "dereliction of duty," saying,"[i]f constitutional report cards were handed out to presidents, Bill Clinton would certainly receive an F–an appalling grade for any president–let alone a former professor of constitutional law."[1] The criticism rubbed off on the FISA court, whose chief judge felt obliged to give public interviews and speeches defending against the claim that the court was rubber-stamping the Clinton administration's intercept requests.[2]

This is where I should insert a joke about the movie "Groundhog Day." But I don't feel like joking, because I know how this movie ends. Faced with civil liberties criticism all across the ideological spectrum, the FISA court imposed aggressive new civil liberties restrictions on government's use of FISA information. As part of its "minimization procedures" for FISA taps, the court required a "wall" between law enforcement and intelligence. And by early 2001, it was enforcing that wall with unprecedented fervor. That was when the court's chief judge harshly disciplined an FBI supervisor for not

[1] Timothy Lynch, *Dereliction Of Duty: The Constitutional Record of President Clinton*, Cato Policy Analysis No. 271 (March 31, 1997), http://www.cato.org/pubs/pas/pa-271.html.

[2] Hon. Royce C. Lamberth, Presiding Judge of the Foreign Intelligence Surveillance Court, Address Before the American Bar Ass'n Standing Comm. on Law and Nat'l Sec. (April 4, 1997), in 19 AMERICAN BAR ASS'N NAT'L SEC. LAW REPORT 2, May 1997, at 1-2.

strictly observing the wall and demanded an investigation that seemed to put the well-regarded agent at risk of a perjury prosecution. A chorus of civil liberties critics and a determined FISA court was sending the FBI a single clear message: the wall must be observed at all costs.

And so, when a law enforcement task force of the FBI found out in August of 2001 that al Qaeda had sent two dangerous operatives to the United States, it did ... nothing. It was told to stand down; it could not go looking for the two al Qaeda operatives because it was on the wrong side of the wall. I believe that FBI task force would have found the hijackers – who weren't hiding – and that the attacks could have been stopped if not for a combination of bad judgment by the FISA court (whose minimization rules were later thrown out on appeal) and a climate in which national security concerns were discounted by civil liberties advocates on both sides of the aisle.

I realize that this story is not widely told, perhaps because it's not an especially welcome story, not in the mainstream media and not on the Internet. But it is true; the parts of my book that describe it are well-grounded in recently declassified government reports.[3]

More importantly, I lived it. And I never want to live through that particular Groundhog Day again. That's why I'm here.

I am afraid that hyped and distorted press reports orchestrated by Edward Snowden and his allies may cause us – or other nations – to construct new restraints on our intelligence gathering, restraints that will leave us vulnerable to another security disaster.

Intelligence Gathering Under Law

The problem we are discussing today has roots in a uniquely American and fairly recent experiment – writing detailed legal rules to govern the conduct of foreign intelligence. This is new, even for a country that puts great faith in law.

The Americans who fought World War II had a different view; they thought that intelligence couldn't be conducted under any but the most general legal constraints. This may have been a reaction to a failure of law in the run-up to World War II, when U.S. codebreakers were forbidden to intercept Japan's coded radio communications because section 605 of the Federal Communications Act made such intercepts illegal. Finally, in 1939, Gen. George C. Marshall told Navy intelligence officers to ignore the law.[4] The military successes that followed made the officers look like heroes, not felons.

That view held for nearly forty years, but it broke down in the wake of Watergate, when Congress took a close look at the intelligence community, found abuses, and in 1978

---

[3] STEWART BAKER, SKATING ON STILTS 66-69 (2010).

[4] DAVID KAHN, THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET 12 (2d ed. 1996).

adopted the first detailed legal regulation of intelligence gathering in history – the Foreign Intelligence Surveillance Act. No other nation has ever tried to regulate intelligence so publicly and so precisely in law.

Forty years later, though, we're still finding problems with this experiment. One of them is that law changes slowly while technology changes quickly. That usually means Congress has to change the law frequently to keep up. But in the context of intelligence, it's often hard to explain *why* the law needs to be changed, let alone to write meaningful limits on collection without telling our intelligence targets a lot about our collection techniques. A freewheeling and prolonged debate -- and does Congress have any other kind? – will give them enough time and knowledge to move their communications away from technologies we've mastered and into technologies that thwart us. The result won't be intelligence under law; it will be law without intelligence.

Much of what we've read in the newspapers lately about the NSA and FISA is the product of this tension. Our intelligence capabilities – and our intelligence gaps – are mostly new since 1978, forcing the government, including Congress, to find ways to update the law without revealing how we gather intelligence.

Section 215 and the Collection-First Model

That provides a useful frame for the most surprising disclosure made by Edward Snowden – that NSA collects telephone metadata (*e.g.*, the called number, calling number, duration of call, etc., but not the call content) for all calls into, out of, or within the United States. Out of context – and Snowden worked hard to make sure it *was* taken out of context – this is a troubling disclosure. How can all of that data possibly be "relevant to an authorized investigation" as the law requires?

But context is everything here. It turns out that collecting the data isn't the same as actually looking at it. Robert Litt, General Counsel of the Director for National Intelligence, has made clear that there are court-ordered rules designed to make sure that government officials only look at relevant records: "The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations. And the only purpose for which we can make that query is to identify contacts."[5] And in fact these rules have been interpreted so strictly that last year the agency only actually looked at records for 300 subscribers.[6]

Still, the government is "seizing" millions of records without a warrant or probable cause, even if it's not searching them. "How can that be constitutional?" you might ask.

---

[5] Robert Litt, General Counsel, Office of the Director of National Intelligence, Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction (June 26, 2013) (transcript available at http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction).

[6] *Id.*

Very easily, as it happens. The Supreme Court has held that such records are not protected by the Fourth Amendment, since they've already been given to a third party.[7]

And even if the Fourth Amendment applied, at bottom it requires only that seizures be reasonable. The Court has recognized more than half a dozen instances where searches and seizures are reasonable even in the absence of probable cause and a warrant.[8] They range from drug screening to border searches. There can hardly be doubt that the need to protect national security fits within this doctrine as well, particularly when waiting to conduct a traditional search won't work. Call data doesn't last. If the government doesn't preserve the data now, the government may not be able to search it later, when the need arises.

In short, there's less difference between this "collection first" program and the usual law enforcement data search than first meets the eye. In the standard law enforcement search, the government establishes the relevance of its inquiry and is then allowed to collect and search the data. In the new collection-first model, the government collects the data and then must establish the relevance of each inquiry before it's allowed to conduct a search.

I know it's fashionable to say, "But what if I don't trust the government to follow the rules? Isn't it dangerous to let it collect all that data?" The answer is that the risk of rule-breaking is pretty much the same whether the collection comes first or second. Either way, you have to count on the government to tell the truth to the court, and you have to count on the court to apply the rules. If you don't trust them to do that, then neither model offers much protection against abuses.

But if in fact abuses were common, we'd know it by now. Today, law enforcement agencies collect several hundred thousand telephone billing records a year using nothing

---

[7] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (affirming the Court's previous holdings that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed") (citing *U.S. v. Miller*, 425 U.S. 435, 442 (1976)).

[8] *See, e.g., O'Connor v. Ortega*, 480 U.S. 709, 720 (1987) (plurality opinion) (concluding that, in limited circumstances, a search unsupported by either warrant or probable cause can be constitutional when "special needs" other than the normal need for law enforcement provide sufficient justification); *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (holding Wisconsin Supreme Court's interpretation of regulation requiring "reasonable grounds" for warrantless search of probationer's residence satisfies the Fourth Amendment reasonableness requirement); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652–653 (1995); *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (asserting that when historical analysis of common law at the time of the Fourth Amendment proves inconclusive as to what protections were envisioned, the Court must "evaluate the search or seizure under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests"); *Packwood v. Senate Select Committee on Ethics*, 510 U.S. 1319, 1321 (1994) (observing the uncontested application of a Fourth Amendment legal standard that "balanced applicant's privacy interests against the importance of the governmental interests. The court concluded that the latter outweighed the former"); *U.S. v. Cantley*, 130 F.3d 1371, 1375 (10th Cir., 1997) (noting that the Supreme Court "has recognized exceptions to the warrant requirement for certain "special needs" of law enforcement, including a state's parole system").

but a subpoena.[9] That means you're roughly a thousand times more likely to have your telephone calling patterns reviewed by a law enforcement agency than by NSA. (And the chance that law enforcement will look at your records is itself low, around 0.25% in the case of one carrier[10]). So it appears that law enforcement has been gaining access to our call metadata for as long as billing records have existed – nearly a century. If this were the road to Orwell's 1984, surely we'd be there by now, and without any help from NSA's 300 searches.

Section 702 and "PRISM"

This brings us to PRISM and the second of the Snowden stories to be released. Without the surprise of the phone metadata order, the PRISM slide show released by Snowden would have been much less newsworthy. Indeed, the parts of the PRISM story that were true aren't actually new and the parts that were new aren't actually true.

Let's start with what's true. Despite the noise around PRISM, the slides tell us very little that the law itself doesn't tell us. Section 702 says that the government may target non-U.S. persons "reasonably believed to be located outside the United States to acquire foreign intelligence information." It covers activities with a connection to the United States and is therefore subject to greater oversight than foreign intelligence gathered outside the United States. Although the Attorney General and the Director of National Intelligence can authorize collection annually, the collection and use of the data is covered by strict targeting and minimization procedures that are subject to judicial review and aimed at protecting U.S. persons as well as other persons located inside the United States.

That's what the law itself says, and the Snowden slides simply add voyeuristic details about the collection. Everyone already knew that the government had the power to do this because, unlike many countries, we codify these things in law. It should come as no surprise then that the government has been using its power to protect all of us.

There was one surprise in those stories though. That's the part that was new but not true. When the story originally broke, reporters at the *Guardian* and the *Washington Post* made it look as if the NSA had direct, unfettered access to private service providers' networks and that they were downloading materials at will. To be fair, the slides were

---

[9] In 2012, Rep. Markey sent letters to a large number of cell phone companies, asking among other things how many law enforcement requests for subscriber records the companies received over the past five years. The three largest carriers alone reported receiving more than a million law enforcement subpoenas a year. *Letters to mobile carriers regarding use of cell phone tracking by law enforcement*, CONGRESSMAN ED MARKEY, http://markey.house.gov/content/letters-mobile-carriers-reagrding-use-cell-phone-tracking-law-enforcement (last visited July 15, 2013).

[10] Letter from Timothy P. McKone, Exec. Vice President, AT&T, to Congressman Ed Markey 3 (May 29, 2012), http://markey.house.gov/sites/markey.house.gov/files/documents/AT%26T%20Response%20to%20Rep.%20Markey.pdf.

confusing on this point, talking about getting data "directly from the servers" of private companies. But that phrase is at best ambiguous; it could easily mean that NSA serves a lawful order on the companies and the companies search for and provide the data from their servers. In fact, everyone with knowledge, from the DNI to the companies in question, has confirmed that interpretation while denying that NSA has unfettered access to directly search the private servers. In short, it now looks as though the *Washington Post* and the *Guardian* hyped this aspect of their story to spur a public debate about NSA surveillance.

Actually, they didn't just want to spur debate; they tried to control it – by withholding information from the public. If you're an American concerned about government collection of data, slides that talk about large-scale collection direct from private databases are bound to raise concern, especially after release of the phone metadata order. But many of those concerns can be answered by reading the very detailed and strict minimization and targeting guidelines adopted by Justice and the DNI and approved by the FISA court for this program. The whole point of those guidelines is to make sure that NSA's collection protects the privacy of Americans while still allowing foreign intelligence collection to go forward.

In short, in both section 215 and section 702, the government has found a reasonable way to square intelligence-gathering necessities with changing technology. Now that they've been exposed to the light of day, these programs are not at all hard to justify. But we cannot go on exposing every collection technique to the light of day just to satisfy everyone that the programs are appropriate. The exposure itself will diminish their effectiveness. Even a fair debate in the open will cause great harm.

And this was never meant to be a fair debate. Snowden and his allies in the press had copies of the minimization and targeting guidelines; they surely knew that the guidelines made the programs look far more responsible. So they suppressed them, waiting a full two weeks – while the controversy grew and took the shape they preferred – before releasing the documents. Since no self-respecting reporter withholds relevant information from the public, it's only fair to conclude that this was an act of advocacy, not journalism. Perhaps the reporters lost their bearings; perhaps the timing was controlled by advocates. Either way, the public was manipulated, not informed.

What Next?

Setting aside the half-truths and the hype, what does the current surveillance flap tell us about the fundamental question we've faced since 1978 – how to gather intelligence under law? I think the current flap exposes two serious difficulties in using law to regulate intelligence gathering.

1. Regulating Technology – What Works and What Doesn't

First, since American intelligence has always been at its best in using new technologies, intelligence law will always be falling out of date, and the more specific its requirements the sooner it will be outmoded.

Second, we aren't good at regulating government uses of technology. That's especially a risk in the context of intelligence, where the government often pushes the technological envelope. The privacy advocates who tend to dominate the early debates about government and technology suffer from a sort of ideological technophobia, at least as far as government is concerned. Even groups that claim to embrace the future want government to cling to the past. And the laws they help pass reflect that failing.

To take an old example, in the 1970s, well before the personal computer and the Internet, privacy campaigners persuaded the country that the FBI's newspaper clipping files about U.S. citizens were a threat to privacy. Sure, the information was public, they acknowledged, but gathering it all in one file was viewed as sinister. And maybe it was; it certainly gave J. Edgar Hoover access to embarrassing information that had been long forgotten everywhere else. So in the wake of Watergate, the attorney general banned the practice in the absence of some investigative predicate.

The ban wasn't reconsidered for twenty-five years. And so, in 2001, when search engines had made it possible for anyone to assemble a clips file about anyone in seconds, the one institution in the country that could not print out the results of its Internet searches about Americans was the FBI. This was bad for our security, and it didn't protect anyone's privacy either.

Now we're hearing calls to regulate how the government uses big data in security and law enforcement investigations. This is about as likely to protect our privacy as reinstating the ban on clips files. We can pass laws turning the federal government into an Amish village, but big data is here to stay, and it will be used by everyone else. Every year, data gets cheaper to collect and cheaper to analyze. You can be sure that corporate America is taking advantage of this remorseless trend. The same is true of the cyberspies in China's Peoples' Liberation Army.

If we're going to protect privacy, we won't succeed by standing in front of big data shouting "Stop!" Instead, we need to find privacy tools – even big data privacy tools – that take advantage of technological advances. The best way to do that, in my view, was sketched a decade ago by the Markle Foundation Task Force on National Security, which called on the government to use new technologies to better monitor government employees who have access to sensitive information.[11] We need systems that audit for

[11] The Task Force's first report called for the federal government to adopt

> robust permissioning structures and audit trails that will help enforce appropriate guidelines. These critical elements could employ a wide variety of authentication, certification, verification, and encryption technologies. Role-based permissions can be implemented and verified through the use of certificates, for example, while encryption can be used to protect communications and data transfers. … Auditing tools that track how, when, and by whom information is accessed or

data misuse, that flag questionable searches, and that require employees to explain why they are seeking unusual data access. That's far more likely to provide effective protection against misuse of private data than trying to keep cheap data out of government hands. The federal government has in fact made progress in this area; that's one reason that the minimization and targeting rules could be as detailed as they are. But it clearly needs to do better. A proper system for auditing access to restricted data would not just improve privacy enforcement, it likely would have flagged both Bradley Manning and Edward Snowden for their unusual network browsing habits.

2. The Rest of the World Has a Ringside Seat – And It Wants a Vote, Too

There's a second reason why the American experiment in creating a detailed set of legal restraints on intelligence gathering is facing unexpected difficulties. The purpose of those restraints is to protect Americans from the intelligence collection techniques we use on foreign governments and nationals. At every turn, the laws and regulations reassure Americans that they will not be targeted by their own intelligence services. This makes plenty of sense from a policy and civil liberties point of view. Intelligence gathering isn't pretty, and it isn't patty cake. On occasion, the survival of the country may depend on good intelligence. Wars are won and lives are lost when intelligence succeeds or fails. Nations do whatever they can to collect information that might affect their future so dramatically. After a long era of national naïveté, when we thought that gentlemen didn't read other gentlemen's mail and when intercepting even diplomatic radio signals was illegal, the United States found itself thrust by World War II and the Cold War into the intelligence business, and now we play by the same rules as the rest of the world.

The purpose of much intelligence law and regulation is to make sure we do not apply those rules to our own citizens. On the whole, I'm confident that we have gone about as far in pursuit of that goal as we can without seriously compromising our ability to conduct foreign intelligence. And we've spelled those assurances out in unprecedented detail. All of that should – and largely has – left the majority of Americans satisfied that intelligence under law is working reasonably well.

The problem is that Americans aren't the only people who read our laws or follow our debates. So does the rest of the world. And it doesn't take much comfort from legal assurances that the privacy interests of *Americans* are well protected from our intelligence agencies' reach. So, while the debate over U.S. intelligence gathering is already beginning to recede in this country, the storm is still gathering abroad. Many other countries have complained about the idea that NSA may be spying on their citizens. Politicians in France, Brazil, Germany, the Netherlands, the United Kingdom, Belgium, and Romania, among others, have expressed shock and called for investigations into

---

used ensure accountability for network users. These two safeguards—permissioning and auditing—will free participants to take initiatives within the parameters of our country's legal, cultural, and societal norms.

MARKLE FOUNDATION TASK FORCE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE 17 (October 2002), http://www.markle.org/sites/default/files/nstf_full.pdf.

PRISM. On July 4, the European Parliament passed a resolution calling for a range of possible actions, such as delaying trade talks and suspending law enforcement and intelligence agreements with the United States over allegations that the United States gathered intelligence on European diplomats. [12]

Some of this is just hypocrisy. Shortly after President Hollande demanded that the U.S. "immediately stop" its intercepts[13] and the French Interior Minister used his position as guest of honor at a July 4th celebration to chide the United States for its intercepts, *Le Monde* disclosed what both French officials well knew -- that France has its own program for large-scale interception of international telecommunications traffic.[14]

But some of reaction is grounded in ignorance. Thanks to our open debates and detailed legislative limits on intelligence gathering, Europeans know far more about U.S. intelligence programs than about their own. The same is true around the world.

As a result, it's easy for European politicians to persuade their publics that the United States is uniquely intrusive in the way it conducts law enforcement and intelligence gathering from electronic communications providers. In fact, the reverse is true.

Practically every comparative study of law enforcement and security practice shows that the United States imposes more restriction on its agencies and protects its citizens' privacy rights from government surveillance more carefully than Europe.

I've included below two figures that illustrate this phenomenon. One is from a study done by the Max Planck Institute, estimating the number of surveillance orders per 100,000 people in several countries. While the statistics in each are not exactly comparable, the chart published in that study shows an unmistakable overall trend. The number of U.S. orders is circled, because it's practically invisible next to most European nations; indeed, an Italian or Dutch citizen is more than a hundred times more likely to be wiretapped by his government than an American.[15]

---

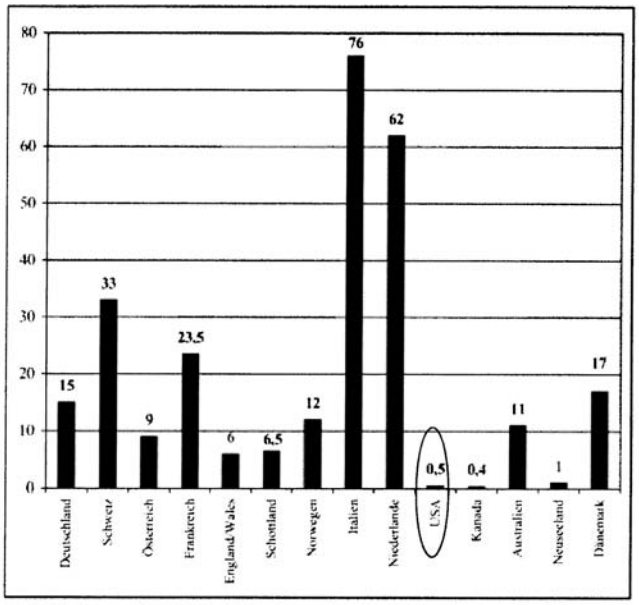
[12] European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)) at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN [hereinafter *European Parliament Resolution*].

[13] Sébastian Seibt, *France's 'hypocritical' spying claims 'hide real scandal'*, FRANCE24 (July 3, 2013), http://www.france24.com/en/20130702-france-usa-spying-snowden-hollande-nsa-prism-hypocritical.

[14] Jacques Follorou and Franck Johannès, *In English: Revelations on the French Big Brother*, LE MONDE (July 4, 2013, 5:24 PM), http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html.

[15] Hans-Jörg Albrecht, et al., *Legal Reality and Efficiency of the Surveillance of Telecommunications*, MAX PLANCK INSTITUTE 104 (2003), http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_%20abschlussbericht.pdf.

Which countries do the most surveillance per capita?



Similarly, the PRISM program is widely believed to show a uniquely American enthusiasm for collecting data from service providers. In fact, it owes that reputation in part to detailed statutory provisions that are meant to protect privacy but that also spell out how the program works.

European regimes, by and large, offer far less protection against arbitrary collection of personal data – and expose their programs to far less public scrutiny. One recent study showed that, out of a dozen advanced democracies, only two – the United States and Japan – impose serious limits on what electronic data private companies can give to the government without legal process. In most other countries, and particularly in Europe,

little or no process is required before a provider hands over information about subscribers.[16]

Which countries allow providers simply to volunteer information to government investigators instead of requiring lawful process?

	Can the government use legal orders to force cloud providers to disclose customer information – as in PRISM?	Can the government skip the legal orders and just get the cloud provider to disclose customer information voluntarily?
Australia	**Yes**	**Yes**
Canada	**Yes**	**Yes***
Denmark	**Yes**	**Yes***
France	**Yes**	**Yes****
Germany	**Yes**	**Yes****
Ireland	**Yes**	**Yes***
Japan	**Yes**	**No**
Spain	**Yes**	**Yes***
UK	**Yes**	**Yes***
USA	**Yes**	**No**

*Voluntary disclosure of personal data requires valid reason
**Some restrictions on voluntary disclosure of personal data without a valid reason and of some telecommunications data

[16] Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS (July 18, 2012).

At most, European providers must have a good reason for sharing personal data, but assisting law enforcement investigations is highly likely to satisfy this requirement. In the United States, such sharing is prohibited in the absence of legal process.

Despite the evidence, however, it is an article of faith in Europe that the United States lags Europe in respect for citizens' rights when collecting data for security and law enforcement purposes. Again, this is the unfortunate result of our commitment to regulating our intelligence services in a more open fashion than other countries.

The U. S. government has learned to live with Europe's misplaced zeal for moral tutelage where data collection is concerned. Our government can ride out this storm as it has ridden out others. But the antagonism spawned by Snowden's disclosures could have more serious consequences for our information technology companies.

Many countries around the world have launched investigations designed to punish American companies for complying with American law. Some of the politicians and data protection agencies pressing for sanctions are simply ignorant of their own nation's aggressive use of surveillance, others are jumping at any opportunity to harm U.S. security interests. But the fact remains that the price of obeying U.S. law could be very high for our information technology sector.

Foreign officials are seizing on the disclosures to fuel a new kind of information protectionism. During a French parliament hearing, France's Minister for the Digital Economy declared that, if the report about PRISM "turns out to be true, it makes [it] relatively relevant to locate datacenters and servers in [French] national territory in order to better ensure data security."[17] Germany's Interior Minister was even more explicit, saying, "Whoever fears their communication is being intercepted in any way should use services that don't go through American servers."[18] And Neelie Kroes, Vice President of the European Commission, said, "If European cloud customers cannot trust the United States government or their assurances, then maybe they won't trust US cloud providers either. That is my guess. And if I am right then there are multi-billion euro consequences for American companies."[19]

Hurting U.S. information technology firms this way is a kind of three-fer for European officials. It boosts the local IT industry, it assures more data for Europe's own surveillance systems, and it hurts U.S. intelligence.

---

[17] Valéry Marchive *France hopes to turn PRISM worries into cloud opportunities*, ZDNET (June 21, 2013, 9:02 GMT), http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/.

[18] *German minister: Drop US sites if you fear spying*, ASSOCIATED PRESS (July 3, 2013), http://m.apnews.com/ap/db_307122/contentdetail.htm?contentguid=OmnMPwXK.

[19] Neelie Kroes, Vice President, European Commission, Statement after the meeting of European Cloud Partnership Board, Tallinn, Estonia (July 4, 2013) (transcript available at http://europa.eu/rapid/press-release_MEMO-13-654_en.htm).

The European Parliament has been particularly aggressive in condemning the program as a violation of European human rights. [20] Its resolution pulls out all the stops, threatening sanctions if the United States does not modify its intelligence programs to provide privacy protections for European nationals. The resolution raises the prospect of suspending two anti-terror agreements with the United States on passenger and financial data, it "demands" U.S. security clearances for European officials so they can review all the documents about PRISM, and it threatens US-EU trade talks as well as the Safe Harbor that allows companies to move data freely across the Atlantic.

This may be the most egregious double standard to come out of Europe yet. Unlike our section 215 program, the EU doesn't have a big metadata database. But that's because Europe doesn't need one. Instead, the European Parliament passed a measure forcing all of its information technology providers to create their own metadata databases so that law enforcement and security agencies could conveniently search up to two years' worth of logs. These databases are full of data about American citizens, and under EU law any database held anywhere in Europe is open to search (and quite likely to "voluntary" disclosure) at the request of any government agency anywhere between Bulgaria and Portugal.

I have seen this movie before, too. During my tenure at Homeland Security, European officials tried to keep the United States from easily accessing travel reservation data to screen for terrorists hoping to blow up planes bound for the United States. In order to bring the United States to the table, European officials threatened to impose sanctions not on the government but on air carriers who cooperated with the data program. [21] Similarly, to limit U.S. access to terror finance information, European data protection authorities threatened the interbank transfer company, SWIFT, with criminal prosecution and fines for giving the U.S. access to transfer data. [22] In the end, the threat of sanctions forced SWIFT to keep a large volume of its data in Europe and to deny U.S. authorities access to it.

Now, whenever Europe has a beef with U.S. use of data in counterterrorism programs, it threatens not the U.S. government but U.S. companies. The European Parliament is simply returning to that same playbook. There is every reason to believe that European governments, and probably some imitators in Latin America and elsewhere, will hold U.S. information technology companies hostage in order to show their unhappiness at the PRISM disclosures.

3. What Congress Should Do About It

As a result, 2013 is going to be a bad year for companies that complied with U.S. law. We need to recognize that our government put them in this position. Not just the

---

[20] *European Parliament Resolution*, *supra* note 12.

[21] BAKER, *supra* note 3, at 114-15.

[22] *Id.* at 145-51.

executive branch that served those orders, but Congress too, which has debated and written intelligence laws as though the rest of the world wasn't listening.

The U.S. government, all of it, has left U.S. companies seriously at risk for doing nothing more than their duty under U.S. law. And the U.S. government, all of it, has a responsibility to protect U.S. companies from the resulting foreign government attacks.

The executive branch has a responsibility to interpose itself between the companies and foreign governments. The flap over Snowden's disclosures is a dispute between governments, and it must be kept in those channels. Diplomatic, intelligence, and law enforcement partners in every other country should hear the same message: "If you want to talk about U.S. intelligence programs, you can talk to us – but not to U.S. companies and individuals; they are prohibited by law from discussing those programs."

Congress too needs to speak up on this question. European politicians feel free to demand security clearances and a vote on U.S. data programs in part because they think Congress and the American public share their views. It's time to make clear to other countries that we do not welcome foreign regulation of U.S. security arrangements.

There are many ways to convey that message. Congress could – should – adopt its own resolution rejecting the European Parliament's.

Congress could prohibit U.S. agencies from providing intelligence and law enforcement assistance or information to nations that have harassed or threatened U.S. companies for assisting their government – unless the agency head decides that providing a particular piece of information will also protect U.S. security.

It could require similar review procedures to make sure that Mutual Legal Assistance Treaties do not provide assistance to nations that try to punish U.S. companies for obeying U.S. law.

And it could match the European Parliament's willingness to reopen the travel data and terror finance pacts with its own, prescribing in law that if the agreements are reopened they must be amended to include an anti-hypocrisy clause ("no privacy obligations may be imposed on U.S. agencies that have not already been imposed on European agencies") as well as an anti-hostage-taking clause ("concerns about government conduct will be raised between governments and not by threatening private actors with inconsistent legal obligations").

And, just to show that this particular road runs in both directions, perhaps Congress could mandate an investigation into how much data about individual Americans is being retained by European companies, how often it is accessed by European governments, and whether access meets our constitutional and legal standards.

Conclusion

Thirty-five years of trying to write detailed laws for intelligence gathering have revealed just how hard that exercise is – and why so few nations have tried to do it. Two lessons are particularly salient as a result of the latest flap over Edward Snowden's revelations.

First, as technologies and security problems change, it is not easy for the law to keep up – at least not without the kind of debate and legislative specification that puts sources and methods at risk. The solution of the past decade has been to erect many safeguards for civil liberties, but behind a veil of classification. The end result has been discouraging. Not because civil liberties have been eroded in secret; in my view, all three branches of government have bent over backwards to protect the privacy of Americans while still conducting intelligence on the frontier of technology. Rather, it's clear that large parts of the body politic are reluctant to trust classified protections. That has allowed irresponsible advocates to distort the debate over our intelligence programs.

Second, we are not alone when we write these laws. Every other country – and practically every terror group – is listening and sifting our debate for clues about what it means for them. The very things that we are proudest of – our ability to conduct intelligence while protecting the rights of Americans – is no comfort to the rest of the world. Instead, it looks to many in the rest of the world like a provocation. They feel entitled to demand for their citizens the protections we have given to Americans. In pursuit of that goal, we can expect them also to attack the technology companies that are at the heart of our competitive and our intelligence advantage. If nothing else, we need to make sure that other governments do not punish those companies for the contribution they make to our security.

Mr. GOODLATTE. Thank you, Mr. Baker.
Mr. Jaffer, welcome.

TESTIMONY OF JAMEEL JAFFER,
AMERICAN CIVIL LIBERTIES UNION (ACLU)

Mr. JAFFER. Thank you. Mr. Chairman, Mr. Ranking Member, Members of the Committee, on behalf of the ACLU, thanks for the invitation to testify today.

Over the last 6 weeks, it has become clear that the NSA is engaged in far-reaching, intrusive, and unconstitutional surveillance of Americans' communications. Under Section 215, the NSA is tracking every single phone call made by a resident of the United States—who they called, when they called them, for how long they spoke. Until recently, it was tracking ordinary Americans' Internet activity as well.

Under Section 702 and on the pretext of monitoring people outside the United States, the NSA is using Section 702 of FISA to build massive databases of Americans' domestic and international communications, not just so-called metadata, but content as well. Those programs have been made possible by huge advances in the technology of surveillance, but in many respects, they resemble the generalized warrants, the generalized surveillance programs that led to the adoption of the Fourth Amendment more than 200 years ago.

The FISA court orders resemble general warrants, albeit general warrants for the digital age. That the NSA is engaged in this kind of unconstitutional surveillance is the result of defects in the statute itself and in the current oversight system.

FISA affords the Government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and the scope of the Government surveillance activities, and structural features of the Foreign Intelligence Surveillance Court have prevented that court from serving as an effective guardian of constitutional rights.

To say that the NSA's activities present a grave danger to American democracy is not an overstatement. Thirty-six years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on Government surveillance "threaten to undermine our democratic society and fundamentally alter its nature."

That warning should have even more resonance today than it did in 1976 because in recent decades, the NSA's resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more power and more intrusive.

Because the problem that Congress confronts today has many roots, there is no single solution to it. But there are a number of things that Congress should do right away.

It should amend Section 215 and 702 to expressly prohibit suspicionless or dragnet monitoring or tracking of Americans' communications. It should require the executive to release basic infor-

mation about the Government's use of foreign intelligence surveillance authorities, including those relating to pen registers and national security letters.

The executive should be required to disclose for each year how many times each of those provisions was used, how many individuals' privacy was implicated by the Government's use of each provision. And with respect to any dragnet, generalized, or bulk surveillance program, it should be required to disclose the types of information that were collected.

Are they collecting medical records? Are they collecting educational records? Are they collecting firearms records? That should be disclosed to the American public.

Congress should also require the publication of FISA court opinions that evaluate the meaning, scope, or constitutionality of the foreign intelligence laws. The ACLU recently filed a motion before the FISA court, arguing that the publication of those opinions is required by the First Amendment, but Congress need not wait for the FISA court to act. Congress has the authority and the obligation to ensure that Americans are not governed by a system of secret law.

Finally, Congress, and this Committee in particular, should hold additional hearings to consider further amendments to FISA, including amendments to make FISA court proceedings more transparent. Congress should not be indifferent to the Government's accumulation of vast quantities of sensitive information about Americans' lives. This Committee in particular has a crucial role to play in ensuring that the Government's efforts to protect the country don't compromise the freedoms that make the country worth protecting.

Thank you.

[The prepared statement of Mr. Jaffer follows:]

Testimony of

Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy
Director, Washington Legislative Office
American Civil Liberties Union

Before
The House Committee on the Judiciary

Oversight Hearing on
The Administration's Use of FISA Authorities

July 17, 2013

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting the ACLU to testify before the Committee.

Over the last six weeks it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans' telephone calls and electronic communications. That the NSA is engaged in this surveillance is the result of many factors. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government's surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly used procedural doctrines to place the NSA's activities beyond the reach of the Constitution.

To say that the NSA's activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance "threaten[ed] to undermine our democratic society and fundamentally alter its nature." This warning should have even more resonance today, because in recent decades the NSA's resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately. It should amend relevant provisions of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications. It should require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should ensure that the public has access to basic information, including statistical information, about the government's use of new surveillance authorities. It should also hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

I. Metadata surveillance under Section 215 of the Patriot Act

On June 5, 2013, *The Guardian* disclosed a previously secret FISC order that compels a Verizon subsidiary, Verizon Business Network Services (VBNS), to supply the government with records relating to every phone call placed on its network between April 25, 2013 and July 19, 2013.[1] The order directs VBNS to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating its customers' calls, including those "wholly within the United States."[2] As many have noted, the order is breathtaking in its scope. It is as if the government had seized every American's address book—with annotations detailing which contacts she spoke to, when she spoke with them, for how long, and (possibly) from which locations.

News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans' call details extends beyond customers of VBNS, encompassing subscribers of the country's three largest phone companies: Verizon, AT&T, and Sprint.[3]

---

[1] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, June 5, 2013, http://bit.ly/13jsdlb.

[2] Secondary Order, *In Re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), *available at* http://bit.ly/11FY393.

[3] *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement with Verizon, AT&T and Sprint, the country's three largest phone companies means, that every time the majority of

Members of the congressional intelligence committees have confirmed that the order issued to VBNS is part of a broader program under which the government has been collecting the telephone records of essentially all Americans for at least seven years.[4]

a. The metadata program is not authorized by statute

The metadata program has been implemented under Section 215 of the Patriot Act—sometimes referred to as FISA's "business records" provision—but this provision does not permit the government to track all Americans' phone calls, let alone over a period of seven years.

As originally enacted in 1998, FISA's business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international terrorism investigations by making an application to the FISC. *See* 50 U.S.C. §§ 1861-62 (2000 ed.). Only four types of records could be sought under the statute: records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862 (2000 ed.). Moreover, the FISC could issue an order only if the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power." *Id.*

The business records power was considerably expanded by the Patriot Act.[5] Section 215 of that Act, now codified in 50 U.S.C. § 1861, permitted the FBI to make an application to the FISC for an order requiring

---

Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total."); Siobhan Gorman & Jennifer Valentino-DeVries, *Government Is Tracking Verizon Customers' Records*, Wall St. J., June 6, 2013, http://on.wsj.com/13mLm7c.

In the days following *The Guardian*'s disclosure of the Verizon order, officials revealed other details about the government's surveillance under Section 215. *See* James R. Clapper, DNI Statement on Recent Unauthorized Disclosures of Classified Information, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13jwuFc. The DNI stated, for example, that "the [FISC] only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization."

[4] Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006,'* Guardian, June 6, 2013, http://bit.ly/13rfxdu; *id.* (Senator Saxby Chambliss: "This has been going on for seven years.").

[5] For ease of reference, this testimony uses "business records provision" to refer to the current version of the law as well as to earlier versions, even though the current

> the production of *any tangible things* (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . .

50 U.S.C. § 1861(a)(1) (emphasis added).

No longer limited to four discrete categories of business records, the new law authorized the FBI to seek the production of "any tangible things." *Id.* It also authorized the FBI to obtain orders without demonstrating reason to believe that the target was a foreign power or agent of a foreign power. Instead, it permitted the government to obtain orders where tangible things were "sought for" an authorized investigation. P.L. 107-56, § 215. This language was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b). Under the current version of the business records provision, the FBI must provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant*" to a foreign intelligence, international terrorism, or espionage investigation. 50 U.S.C. § 1861(b)(2)(A) (emphasis added).[6]

While the Patriot Act considerably expanded the government's surveillance authority, Section 215 does not authorize the metadata program. First, whatever "relevance" might allow, it does not permit the government to cast a seven-year dragnet over the records of every phone call made or received by any American. Indeed, to say that Section 215 authorizes this surveillance is to deprive the word "relevance" of any meaning. The government's theory appears to be that some of the information swept up in the dragnet might become relevant to "an authorized investigation" at some point in the future. The statute, however, does not permit the government to collect information on this basis. *Cf.* Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, Guardian, June 9, 2013, http://bit.ly/18iDA3x ("[B]ased on the scope of the released order, both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended."). The statute requires the government to show a connection between the records it seeks and some specific, existing investigation.

Indeed, the changes that Congress made to the statute in 2006 were meant to ensure that the government did not exploit ambiguity in the statute's language to justify

---

version of the law allows the FBI to compel the production of much more than business records, as discussed below.

[6] Records are presumptively relevant if they pertain to (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This relaxed standard is a significant departure from the original threshold, which, as noted above, required an individualized inquiry.

the collection of sensitive information not actually connected to some authorized investigation. As Senator Jon Kyl put it in 2006, "We all know the term 'relevance.' It is a term that every court uses. The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation."[7]

As Congress recognized in 2006, relevance is a familiar standard in our legal system. It has never been afforded the limitless scope that the executive branch is affording it now. Indeed, in the past, courts have carefully policed the outer perimeter of "relevance" to ensure that demands for information are not unbounded fishing expeditions. *See, e.g.*, *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) ("What is more troubling is the matter of relevance. The [grand jury] subpoena requires production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.").[8] The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of "relevance."[9]

b. The metadata program is unconstitutional

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans' phone records, it clearly is.

The Supreme Court's recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual's location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual's movements over an extended period allows the government to generate a "precise, comprehensive record" that reflects "a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* (Sotomayor, J., concurring).

---

[7] Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, Wall St. J., July 8, 2013, http://on.wsj.com/13x8QKU.

[8] *See also Hale v. Henkel*, 201 U.S. 43, 76-77 (1906).

[9] The metadata program also violates Section 215 because the statute does not authorize the prospective acquisition of business records. The text of the statute contemplates "release" of "tangible things" that can be "fairly identified," and "allow[s] a reasonable time" for providers to "assemble[]" those things. 50 U.S.C. § 1861(c)(1)-(2). These terms suggest that Section 215 reaches only business records already in existence.

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles she reads, whom she corresponds with, and whom *those* people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in *Jones*. In fact, the surveillance held unconstitutional in *Jones* was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in *Jones* was meant to further a specific criminal investigation into a specific crime, and the government collected information about one person's location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Some have defended the metadata program by reference to the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in *Smith,* however, was very primitive—it tracked the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country.

Another argument that has been offered in defense of the metadata program is that, though the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the *collection* of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans' private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans' private papers and communications in the first place.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. *See, e.g.*, *United States v. U.S. District Court*, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to "exacting scrutiny" where they substantially burden First Amendment rights. *See, e.g.*, *Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government's legitimate goals. *See, e.g.*, Press Release, *Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks*, June

7, 2013, http://1.usa.gov/19Q1Ng1 ("As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.").

c. Congress should amend Section 215 to prohibit suspicionless, dragnet collection of "tangible things"

As explained above, the metadata program is neither authorized by statute nor constitutional. As the government and FISC have apparently found to the contrary, however, the best way for Congress to protect Americans' privacy is to narrow the statute's scope. The ACLU urges Congress to amend Section 215 to provide that the government may compel the production of records under the provision only where there is a close connection between the records sought and a foreign power or agent of a foreign power. Several bipartisan bills now in the House and Senate should be considered by this Committee and Congress at large. The LIBERT-E Act, H.R. 2399, 113th Cong. (2013), sponsored by Ranking Member Conyers, Rep. Justin Amash, and forty others, would tighten the relevance requirement, mandating that the government supply "specific and articulable facts showing that there are reasonable grounds to believe that the tangible things sought are relevant and material," and that the records sought "pertain only to an individual that is the subject of such investigation." A bill sponsored by Senators Udall and Wyden would similarly tighten the required connection between the government's demand for records and a foreign power or agent of a foreign power. Congress could also consider simply restoring some of the language that was deleted by the Patriot Act—in particular, the language that required the government to show "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power."

II. Electronic surveillance under Section 702 of FISA

The metadata program is only one part of the NSA's domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans' electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008.[10] Under this program, labeled "PRISM" in NSA documents, the government collects emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.[11] The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it

[10] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, http://wapo.st/1888aNr.

[11] While news reports have generally described PRISM as an NSA "program," the publicly available documents leave open the possibility that PRISM is instead the name of the NSA database in which content collected from these providers is stored.

involves surveillance of foreigners outside the United States. [12] This is misleading. The PRISM program involves the collection of Americans' communications, both international and domestic, and for reasons explained below, the program is unconstitutional.

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.[13] While leaving FISA in place for purely domestic communications, the FISA Amendments Act revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications. Under the FISA Amendments Act, the Attorney General and Director of National Intelligence ("DNI") can "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881a(a). The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," *id.* § 1881a(b)(1), but an acquisition authorized under the FISA Amendments Act may nonetheless sweep up the international communications of U.S. citizens and residents.

Before authorizing surveillance under Section 702—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a "mass acquisition order"). *Id.* § 1881a(a), (c)(2). A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year.

To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court "a written certification and any supporting affidavit" attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "targeting procedures" reasonably designed to ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States,"

---

[12] James R. Clapper, DNI Statement on Activities Authorized Under Section 702 of FISA, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13JJdBE; *see also* James R. Clapper, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), http://1.usa.gov/10YY4tp.

[13] A description of electronic surveillance prior to the passage of the FISA Amendments Act, including the warrantless wiretapping program authorized by President Bush beginning in 2001, is available in Mr. Jaffer's earlier testimony to the Committee. *See* The FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security, H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (written testimony of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union Foundation), *available at* http://bit.ly/14Q61Bs.

and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id.* § 1881a(g)(2)(A)(i).

The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "minimization procedures" that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information." *Id.* § 1881a(g)(2)(A)(iii)–(vii).

Importantly, Section 702 does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. *Id.* § 1881a(g)(4).

Nor does Section 702 place meaningful limits on the government's retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt "minimization procedures," *id.* § 1881a, that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons," *id.* §§ 1801(h)(1), 1821(4)(A). The Act does not, however, prescribe specific minimization procedures. Moreover, the FISA Amendments Act specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is "foreign intelligence information." *Id.* § 1881a(e) (referring to *id.* §§ 1801(h)(1), 1821(4)(A)). The phrase "foreign intelligence information" is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs. *Id.* § 1801(e).

As the FISA Court has itself acknowledged, its role in authorizing and supervising surveillance under the FISA Amendments Act is "narrowly circumscribed."[14] The judiciary's traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FISA Amendments Act is to issue advisory opinions blessing in advance broad parameters and targeting procedures, under

[14] *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), *available at* http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf.

which the government is then free to conduct surveillance for up to one year. Under Section 702, the FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not closely supervise the implementation of the government's targeting or minimization procedures. In short, the role that the FISA Court plays under the FISA Amendments Act bears no resemblance to the role that it has traditionally played under FISA.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.[15] The statute's defects include:

- Section 702 allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

[15] The ACLU raised many of these defects in a constitutional challenge to the FISA Amendments Act filed just hours after the Act was signed into law in 2008. The case, *Amnesty v. Clapper*, was filed on behalf of a broad coalition of attorneys and human rights, labor, legal and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and email communications with individuals located outside the United States. In a 5-4 ruling handed down on February 26, 2013, the Supreme Court held that the ACLU's plaintiffs did not have standing to challenge the constitutionality of the Act because they could not show, at the outset, that their communications had been monitored by the government. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). The Court did not reach the merits of plaintiffs' constitutional challenge.

- Section 702 allows the government to conduct intrusive surveillance without meaningful judicial oversight.

Under Section 702, the government is authorized to conduct intrusive surveillance without meaningful judicial oversight. The FISA Court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is initiating any particular surveillance program. The FISA Court's role is limited to reviewing the government's "targeting" and "minimization" procedures. And even with respect to the procedures, the FISA court's role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time.

- Section 702 places no meaningful limits on the government's retention and dissemination of information relating to U.S. citizens and residents.

As a result of the FISA Amendments Act, thousands or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is "targeted" at people abroad. Yet the law fails to place any meaningful limitations on the government's retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt "minimization" procedures—procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." However, these minimization procedures must accommodate the government's need "to obtain, produce, and disseminate foreign intelligence information." In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is "foreign intelligence information." Because "foreign intelligence information" is defined broadly (as discussed below), this is an exception that swallows the rule.

- Section 702 does not limit government surveillance to communications relating to terrorism.

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather "foreign intelligence information." There are multiple problems with this. First, under the new law the "foreign intelligence" requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase "foreign intelligence information" has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the "foreign affairs of the United States." Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

b. The NSA's "targeting" and "minimization" procedures do not mitigate the statute's constitutional deficiencies.

Since the FISA Amendments Act was enacted in 2008, the government's principal defense of the law has been that "targeting" and "minimization" procedures supply sufficient protection for Americans' privacy. Because the procedures were secret, the government's assertion was impossible to evaluate. Now that the procedures have been published, however,[16] it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

- The NSA's procedures permit it to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.

While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

- The NSA's procedures allow the surveillance of Americans by failing to ensure that the its surveillance targets are in fact foreigners outside the United States.

The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA's procedures fail to ensure that its surveillance targets are *in fact* foreigners outside the United States. This is because the procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

---

[16] *See* Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, *Guardian*, June 20, 2013, http://bit.ly/105qb9B.

- The NSA's procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.

One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The NSA's procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

- The NSA's procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, Section 702 permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the FISA Amendments Act made clear that this was one of its principal purposes, and unsurprisingly, the procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

- The NSA's procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic.[17] The Act

[17] Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in "significant and systemic" overcollection of such domestic

should require the NSA to purge these communications from its databases, but it does not. The procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly.

- The NSA's procedures allow the government to collect and retain communications protected by the attorney-client privilege.

The procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

c. Congress should amend Section 702 to prohibit suspicionless, dragnet collection of Americans' communications.

For the reasons discussed above, the ACLU believes that the FISA Amendments Act is unconstitutional on its face. There are many ways, however, that Congress could provide meaningful protection for privacy while preserving the statute's broad outline. One bill introduced by Senator Wyden during the reauthorization debate last fall would have prohibited the government from searching through information collected under the FISA Amendments Act for the communications of specific, known U.S. persons. Bills submitted during the debate leading up to the passage of the FISA Amendments Act in 2008 would have banned dragnet collection in the first instance or required the government to return to the FISC before searching communications obtained through the FISA Amendments Act for information about U.S. persons. Congress should examine these proposals again and make amendments to the Act that would provide greater protection for individual privacy and mitigate the chilling effect on rights protected by the First Amendment.

III. Excessive secrecy surrounds the government's use of FISA authorities.

Amendments to FISA since 2001 have substantially expanded the government's surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of Congress and the public

---

communications. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, April 15, 2009, http://nyti.ms/16AIq5O.

have learned more about domestic surveillance in last two months than in the last several decades combined. While the Judiciary and Intelligence Committees have received some information in classified format, only members of the Senate Select Committee on Intelligence, party leadership, and a handful of Judiciary Committee members have staff with clearance high enough to access the information and advise their principals. Although the Inspectors General and others file regular reports with the Committees of jurisdiction, these reports do not include even basic information such how many Americans' communications are swept up in these programs, or how and when Americans' information is accessed and used.

Nor does the public have access to the FISC decisions that assess the meaning, scope, and constitutionality of the surveillance laws. Aggregate statistics alone would not allow the public to understand the reach of the government's surveillance powers; as we have seen with Section 215, one application may encompass millions of individual records. Public access to the FISA Court's substantive legal reasoning is essential. Without it, some of the government's most far-reaching policies will lack democratic legitimacy. Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.[18] Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA's sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such opinions, some close to one hundred pages long.[19] Executive officials testified before Congress several years ago that declassification review was already underway,[20] and President Obama directed the DNI to revisit that process in the last few weeks. If the administration refuses to release these opinions, Congress should consider legislation compelling their release. Possible vehicles include the LIBERT-E Act, cited above, or the Ending Secret Law Act, H.R. 2475, 113th Cong. (2013), a bipartisan bill sponsored by Rep. Adam Schiff, Todd Rokita, and sixteen other members of the House.

Congress should also require the release of information about the type and volume of information that is obtained under dragnet surveillance programs. The leaked Verizon order confirms that the government is using Section 215 to collect telephony metadata about every phone call made by VBNS subscribers in the United States. That the

---

[18] *See, e.g.*, Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, http://wapo.st/170VVSu.

[19] *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, http://nyti.ms/12beiA3.

[20] Prehearing Questions for Lisa O. Monaco Upon Her Nomination to be the Assistant Attorney General for National Security, Sen. Select Comm. on Intelligence, 112th Cong., at 12-13, *available at* http://bit.ly/10V5Ion.

government is using Section 215 for this purpose raises the question of what other "tangible things" the government may be collecting through similar dragnets. For reasons discussed above, the ACLU believes that these dragnets are unauthorized by the statute as well as unconstitutional. Whatever their legality, however, the public has a right to know, at least in general terms, what kinds of information the government is collecting about innocent Americans, and on what scale.

IV. Summary of recommendations

As discussed above, the ACLU urges Congress to:

- Amend Section 215 of the Patriot Act and Section 702 of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications.
- Require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws.
- Require the publication of information about the type and volume of information that the government obtains under dragnet surveillance programs.
- Hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

Thank you for this opportunity to present the ACLU's views.

Mr. GOODLATTE. Thank you, Mr. Jaffer.
Mr. Bradbury, welcome.

TESTIMONY OF STEVEN G. BRADBURY, DECHERT, LLP

Mr. BRADBURY. Thank you, Mr. Chairman, Ranking Member Conyers, and distinguished Members of the Committee.

I believe both of the recently disclosed NSA programs are critical to our national security, and I have every confidence that each is authorized by statute, consistent with the Constitution, and appropriately protective of privacy and civil liberties.

The first program involves the acquisition of telephone metadata under a Section 215 business records order. This metadata consists only of tables of numbers indicating which phone numbers called which numbers and the time and duration of the calls. It doesn't reveal any other subscriber information, and it doesn't enable the Government to listen to anyone's phone calls. There is no monitoring or tracking of phone calls.

The Constitution does not require a warrant supported by probable cause to acquire this metadata. Courts have held that there isn't a reasonable expectation of privacy in the phone numbers that are dialed. And the production of business records like these doesn't involve a Fourth Amendment search.

This acquisition is authorized under the terms of Section 215 because the use of the metadata is relevant to counterterrorism investigations. Acquiring a comprehensive database enables better analysis of the telephone links and calling patterns of terrorist suspects, which is often the only way to discover new phone numbers being used by terrorists.

To connect the dots effectively requires the broadest set of telephone metadata. The same relevance standard applies in other contexts, such as administrative subpoenas and grand jury subpoenas, which, unlike Section 215, typically do not require court approval.

While the metadata order is extraordinary in the amount of data acquired, it is also extraordinarily narrow and focused because of the strict limitations placed on accessing the data. There is no data mining or trolling through the database looking for suspicious patterns.

By court order, the data can only be accessed when the Government has reasonable suspicion that a particular phone number is associated with a foreign terrorist organization. And then that number is tested against the database to discover its connections. If it appears to be a U.S. number, the necessary suspicion can't be based solely on First Amendment protected activity.

Because of this limited focus, only a tiny fraction of the total data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the Government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers.

Any data records older than 5 years are continually deleted from the system. The order must be reviewed and reapproved every 90 days. And my understanding is that since 2006, 14 different Federal judges have approved this metadata order.

Let me now turn to the surveillance program that targets foreign communications. This program is authorized under Section 702 of

FISA, and if we just track through the provisions of Section 702, we can see the outline of this program. With court approval, Section 702 authorizes a program of foreign-focused surveillance for periods of 1 year at a time.

This authority may only be used if the surveillance does not, one, intentionally target any person of any nationality known to be located in the United States; two, target a person outside the U.S. if the purpose is to reverse target any particular person believed to be in the U.S.; three, intentionally target a U.S. person anywhere in the world; and four, intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S.

Section 702 mandates court approval of the targeting protocols and of minimization procedures to ensure that any information about U.S. persons that may be captured in this surveillance will not be retained or disseminated, except as necessary for foreign intelligence purposes. From everything that has been disclosed about this program, including the so-called PRISM Internet collection, I don't think there is any reason to doubt that this foreign-targeted surveillance is just what Section 702 was designed to authorize.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Bradbury follows:]

TESTIMONY OF STEVEN G. BRADBURY

Before the
HOUSE COMMITTEE ON THE JUDICIARY

Oversight Hearing into
The Administration's Use of FISA Authorities

July 17, 2013

Thank you, Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the Committee.

I appreciate the opportunity to appear before the Committee today to address the statutory authorities and constitutional principles governing the two National Security Agency programs that have been the subject of recent disclosures. These are:

> First, the acquisition of telephone call-detail records that involves only telephone metadata, not the content of any phone calls or the names or addresses of any phone subscribers; and
>
> Second, the surveillance, including the so-called "PRISM" Internet collection, that is targeted at the communications of foreign persons reasonably believed to be located outside the United States.

I believe it is most useful to discuss the legal basis for each of these two programs separately, since they are authorized under two different provisions of the Foreign Intelligence Surveillance Act, or FISA, though of course the programs can and should work together as part of the overall counterterrorism efforts of the United States.

Section 215 Order for Acquisition of Telephone Metadata

Let me focus first on the telephone metadata program. As the Government has stated, this program is supported by a business records order issued under the provision of FISA added by section 215 of the USA PATRIOT Act. *See* 50 U.S.C. § 1861. This section 215 order must be reviewed and reapproved by the federal

judges who sit on the FISA court every 90 days. I understand that 14 different federal judges have approved this order since 2006.

The metadata acquired consists of the transactional information that phone companies retain in their systems for a period of time in the ordinary course of business for billing purposes and that appears on typical phone bills. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls. ***This order does not give the government access to any information about the content of calls or any other subscriber information, and it doesn't enable the government to listen to anyone's phone calls.***

Access to the data is limited under the terms of the court order. Contrary to some news reports, there's no data mining or random sifting of the data permitted. The database may only be accessed through queries of individual phone numbers and only when the government has reasonable suspicion that the number is associated with a foreign terrorist organization. If it appears to be a U.S. number, the suspicion cannot be based solely on activities protected by the First Amendment, such as statements of opinion, books or magazines read, Web sites visited, or places of worship frequented. Any query of the database requires approval from a small circle of designated NSA officers.

A query will simply return a list of any numbers the suspicious number has called and any numbers that have called it and when those calls occurred. Nothing more.

The database includes metadata going back five years, to enable an analysis of historical connections. Any records older than five years are continually purged from the system and deleted.

In analyzing links to suspicious numbers, any connections that are found to numbers inside the United States will of course be of most interest, because the analysis may suggest the presence of a terrorist cell in the U.S. Based in part on that information, the FBI may seek a separate FISA order for surveillance of a U.S. number, but that surveillance would have to be supported by individualized probable cause.

The NSA has confirmed that in all of 2012, there were fewer than 300 queries of the database, and only a tiny fraction of the data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers generated from the queries.

In addition to court approval, the 215 order is also subject to oversight by the executive branch and Congress. FISA mandates periodic audits by inspectors general and reporting to the Intelligence and Judiciary Committees of Congress. When section 215 was reauthorized in 2011, I understand the leaders of Congress and members of these Committees were briefed on this program, and all members of Congress were offered the opportunity for a similar briefing.

Legal Basis and Constitutional Standards

Now let me address the statutory and constitutional standards applicable to the acquisition of this telephone metadata.

Section 215 permits the acquisition of business records that are "relevant to an authorized investigation." Here, the telephone metadata is "relevant" to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers described above, and this type of analysis is a critical building block in these investigations. In order to "connect the dots," we need the broadest set of telephone metadata we can assemble, and that's what this program enables.

The legal standard of relevance in section 215 is the same standard used in other contexts. It does not require a separate showing that every individual record in the database is "relevant" to the investigation; the standard is satisfied if the use of the database as a whole is relevant. As I've indicated, the acquisition of this data and the creation and use of this database are not only relevant to ongoing counterterrorism investigations; they're necessary to those investigations, because they offer the only means to conduct the critical analysis that provides links to new phone numbers used by agents of foreign terrorist organizations.

In terms of the background constitutional principles, it's important to remember that the Fourth Amendment itself would not require a search warrant or other individualized court order for such data acquisition. A government request for a company's business records is not a "search" within the meaning of the Fourth Amendment. Government agencies have authority under many federal statutes to issue administrative subpoenas without court approval for documents that are "relevant" to an authorized inquiry. In addition, grand juries have broad authority to subpoena records potentially relevant to whether a crime has occurred, and grand jury subpoenas also don't require court approval. In the modern world of electronic storage and data compilation, reliance on the same "relevance" standard in these other contexts can also result in extremely expansive requests for business records.

In addition, the Fourth Amendment does not require a warrant when the government seeks purely transactional information, or metadata, as distinct from the content of communications. This information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore said there's no reasonable expectation that it's private. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-05 (9th Cir. 2008).

I would stress, however, that section 215 is more restrictive than the Constitution demands, because it requires the approval of a federal judge. In this way, Congress in the PATRIOT Act adopted a requirement for judicial review and approval of FISA business records orders that is more protective of privacy and civil liberties interests than the Constitution would otherwise demand. And while the 215 order for metadata is extraordinary in terms of the amount of data acquired, it's also extraordinarily narrow and focused in terms of the strict limitations placed on accessing the data at the back end.

Section 702 Order Targeting Foreign Communications

Let me now turn to the other NSA program at issue: The surveillance program targeting the Internet and other communications of foreign persons reasonably believed to be outside the United States. This program, which includes the so-called "PRISM" collection, is supported by a FISA court order issued under section 702 of FISA, the provision for "programmatic" foreign-targeting authority

that was added by the FISA Amendments Act of 2008. *See* 50 U.S.C. § 1881a. Similar authority was initially provided on a temporary basis in the Protect America Act of 2007.

The best way to understand this foreign-targeting program is to review the provisions of section 702, which lays out the governing framework approved by Congress.

Section 702 provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year at a time, targeted surveillance of the communications of non-U.S. persons who are reasonably believed to be located outside the United States to acquire foreign intelligence information, provided the FISA court approves the targeting procedures under which the surveillance occurs and the minimization procedures that govern use of the acquired information.

Under section 702, the surveillance may not (1) intentionally target any person, of any nationality, known to be located in the United States, (2) target a person outside the U.S. if the purpose is to reverse target any particular person believed to be in the U.S., (3) intentionally target a U.S. person anywhere in the world, and (4) intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S.

Section 702 requires the Attorney General to adopt, and the FISA court to approve, targeting procedures reasonably designed to ensure compliance with these limitations, as well as detailed minimization procedures designed to ensure that any information about U.S. persons captured through this surveillance will not be retained or disseminated except as necessary for foreign intelligence reporting purposes.

Any foreign intelligence surveillance that is targeted at a particular U.S. person or any person believed to be in the United States requires a traditional individualized FISA order supported by probable cause.

Like the business records provision of FISA, section 702 goes beyond the baseline protections of the Fourth Amendment. Federal courts have consistently held that the Constitution permits the executive branch to conduct intelligence

surveillance within the United States without court involvement, provided the surveillance is focused on foreign threats. *See, e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980). By establishing a detailed procedure for court approval and congressional oversight, section 702 therefore provides a system of foreign intelligence surveillance that is more restrictive than the Constitution would otherwise require.

The PRISM Internet collection is precisely the type of court-approved foreign-targeted intelligence surveillance that Congress intended to authorize when it enacted and reauthorized section 702 by overwhelming majorities. This program is subject to extensive reviews and periodic reports to Congress by inspectors general, in addition to the oversight of the FISA judges. Moreover, I understand that in advance of the reauthorization of section 702 in 2012, the leaders and full membership of the Intelligence Committees of both Houses of Congress were briefed on the classified details of this program and all members of Congress were offered the opportunity for such a briefing.

* * *

For these reasons, I think these two programs are entirely lawful and are conducted in a manner that appropriately respects the privacy and civil liberties of Americans and the principles enshrined in the Constitution. Thank you, Mr. Chairman.

Mr. GOODLATTE. Thank you, Mr. Bradbury.
Ms. Martin, welcome.

TESTIMONY OF KATE MARTIN,
CENTER FOR NATIONAL SECURITY STUDIES

Ms. MARTIN. Thank you, Mr. Chairman and Ranking Member Conyers and other distinguished Members of this Committee, for inviting me to testify today.

I want to, first of all, thank the Committee for having asked some questions of the Government witnesses that I hoped the Committee would ask and congratulate you upon obtaining answers, at least in part, to some of those questions.

I want to raise two overarching concerns today about these programs and note, first of all, that I think it does not make sense for the Committee to consider the 215 program and the 702 program separately and, instead, that they need to be looked upon as part of an overall set of foreign surveillance authorities that work together to allow the Government to collect and keep massive amounts of information about Americans and to do so in secret.

And that that is the real nut of the problem. We have an incredibly complex set of laws governing those authorities and setting up safeguards, as this Committee is well aware, and we need to understand how those work together, where the holes are, and where the potential changes are.

So I would urge the Committee, in going forward, to expand your oversight and your questions to look at not just 215 and 702, but all the FISA Authorities and not just as exercised by the National Security Agency, but equally significantly regarding how the information is shared between the NSA, the FBI, the DHS, and perhaps the White House or the NCTC as well. Those are equally critical questions for both civil liberties and for evaluating the effectiveness and the necessity of the programs.

I agree with Mr. Jaffer and many of the Members here today that there is a lot to be concerned about, that we are seeing the unprecedented massive collection of information on Americans, the creation of secret data banks which are available for Government analysis, queries, and data mining by ever increasingly sophisticated computerized tools, and the dissemination of both raw information and the results of such analysis or data mining throughout the executive branch.

I think that the question is whether or not these new activities by the Government have the potential to fundamentally change the relationship between citizens and the state. I think that was the concern that many Members of this Committee were raising today.

In connection with the question of what is the harm here, I very much appreciate that the Administration and the NSA have been very detailed about the internal safeguards that they have created to ensure that no rogue employee or contractor can access the personal information of an individual American and misuse it.

I do not believe, however, that that is the primary worry of the American people about these programs. I think, rather, the primary worry and the primary concern when FISA was first drafted was that the Government would succumb to the temptation to use

information that it has about individual Americans to chill political dissent, to challenge its political opponents, et cetera.

I think this is one of those instances where when you discuss it in advance you can never believe that this would actually happen, but that when you look at history, it has happened too many times already in my own lifetime.

Just a couple of specific comments about information which I believe would be crucial for this Committee's consideration. First on questions about what kinds of authorities does the Government have under Section 215, one of the Members asked about the collection of Internet metadata. I would urge you to find out specifically whether or not under the Government's current understanding of its legal authorities under 215, it could make an application for the collection of all Internet metadata on communications within the United States; whether or not it could make an application under 215 for bulk collection of geolocation data; or for bulk collection of financial records or credit card records.

I think it is also important to know when the Government makes one of these 300 queries to the 215 database, does that query require the database to do a chain-linked—a chained analysis? Not simply what numbers have been in contact with the first number, but to then do a chain-linked analysis?

I know my time is up, and if I might just make one last comment? On the overall question of this is foreign intelligence, and traditionally it is done in secret; it is always done by government. There is a high cost when it is discussed in public.

It is foreign intelligence when it is directed against foreigners and other governments overseas. We are talking about massive authorities for massive collections on Americans. And that may be foreign intelligence. It is also at the core of the concerns of the constitutional framers. I think that what we have seen about the cost of secrecy here is that——

Mr. GOODLATTE. Sorry.

Ms. MARTIN. That is okay.

[The prepared statement of Ms. Martin follows:]

Testimony of
Kate Martin, Director
Center for National Security Studies

Before the
Committee on the Judiciary
United States House of Representatives

"Oversight of the Administration's use of FISA Authorities"
Wednesday, July 17, 2013

Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the House Judiciary Committee, thank you for inviting me to testify today. I am the Director of the Center for National Security Studies a think tank and civil liberties organization, which for almost 40 years has worked to ensure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights and that respect for our constitutional system of government will accomplish that. In our work on matters ranging from national security surveillance to intelligence oversight, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

I appreciate the Committee's long history of work since 9/11 on the amendments to the Foreign Intelligence Surveillance Act (FISA) contained in the Patriot Act and the many amendments since then, including the 2008 Foreign Intelligence Amendments Act, and its serious consideration of the civil liberties concerns expressed by my organization and our colleagues.

I want to raise two overarching concerns for this Committee's consideration during the current debate, which I hope will inform your consideration of necessary oversight measures as well as specific changes to the statutory language. First, we are concerned that the unprecedented massive collection of information on Americans, the creation of secret databanks which are available for government analysis, queries, and data-mining by ever increasingly sophisticated computerized tools, and the dissemination of both raw information and the results of such analysis or data-mining throughout the executive branch pose unprecedented threats to First and Fourth Amendment liberties. Second, the secrecy that surrounds this government surveillance – not of foreign governments or other foreign targets – but of Americans – poses a significant and perhaps unprecedented challenge to our system of constitutional checks and balances.

It has long been recognized as Senator Sam Ervin, the author of the Privacy Act put it in 1974:

> *"[D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.*
>
> *Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words."*

Senator Sam Ervin, June 11, 1974, reprinted in Committee On Government Operations, United States Senate And The Committee On Government Operations, House Of Representatives, Legislative History Of The Privacy Act Of 1974, S.3418, at 157 (Public Law 93-579)(Sept. 1976).

A key purpose of the Fourth Amendment was to prevent general searches by the government. This was accomplished in part through the Amendment's requirement of particularity -- that the target of a search or seizure, the place to be searched, the things to be seized all had to be specifically identified in a warrant issued by a judge. We now face the situation where the government has the capacity to collect massive amounts of information on millions of Americans, to store that information indefinitely, and to analyze that information to discover enormous amounts of revealing information about individual Americans' private lives and political activities. As others have demonstrated, the underlying rationales for the old distinctions between content and meta-data, or the notion that Fourth Amendment protections have no applicability to information about an individual held by third parties, no longer hold in the new world of massive electronic data about individuals held by Internet service providers, telecommunications companies and others.

At the same time, there has been a fundamental shift in the way that the government collects information on Americans. The two sections of FISA that have been the focus of the leaks, 50 U.S.C. § 1861, 1881a , "sections 215 and 702", are apparently used by the government to obtain information about thousands of communications of Americans, but without even any suspicion about the individual Americans whose communications are being collected. To the contrary, these authorities are apparently being used for en masse bulk collection on thousands or

millions of individuals without any individualized showing of suspicion about any party to the communication, whether American or foreigner. While it is true that the NSA has had such bulk collection capabilities for many years, those capabilities were aimed overseas and their purpose was to collect information about foreign governments and foreign terrorist organizations. That collection did include "incidentally acquired" information on Americans' communications, but that was not the purpose of the collection, and there were strict rules about the NSA disseminating that information to other government agencies for their use. Nor, as far as we know, was the government creating massive databases on Americans' communications as an integral part of its "foreign intelligence" activities.

Questions about these FISA authorities:

As others have detailed, there are serious questions whether these bulk collection programs are within the intended statutory authorizations, e.g., the domestic telephony meta-data program under sec. 215. There are serious constitutional concerns about the breadth of and lack of individualized suspicion or particularity in these programs. And there are serious questions whether the secrecy built into the programs is constitutional and whether it is consistent with effective oversight or a working system of checks and balances.

In examining these authorities and programs, it is important to review not only whether private information about Americans held in government databases is adequately protected from rogue employees or contractors stealing or misusing the information. While safeguards are needed against that kind of privacy abuse, the more important danger is that there are inadequate safeguards against government violations of the law or against deliberate misuse of the information to target the government's political opponents, chill dissent or unconstitutionally profile minority communities. As the original Framers recognized, all governments may succumb to the temptations of power. In my lifetime Senator McCarthy smeared civil servants, the FBI tried to blackmail Dr. Martin Luther King in order to weaken the civil rights movement, President Nixon created an enemies list of his political opponents, and the Justice Department wrote a secret legal opinion that the President could break the law in secret if he deemed it necessary for national security.

Since the leaks about these two particular programs, the Executive Branch has vigorously defended their usefulness in detecting and stopping terrorist plots and that is certainly relevant to the Congress' and public consideration. These claims merit careful analysis, especially in light of former NSA Director Michael Hayden's explanation that it is very difficult to determine which information was key in stopping any particular attack.[1] And in doing that analysis, there are at least two key questions to be considered: are there less intrusive ways to obtain this

[1] "...you know – we're asking for evidence that A caused B. And right now, if we're really good at our art, you'll never be able to do that. It'll all be a blend of different pieces of glass that you now get to create a mosaic from." Remarks of General Michael Hayden, "Is Big Brother Watching You?" American Enterprise Institute, June 19, 2013, http://www.aei.org/events/2013/06/19/is-big-brother-watching-you/.

information and more importantly, are there other equally or more effective counter-terrorism measures available. We have already begun to see alarmist statements unsupported by any analysis to the effect that without these programs, we face another 9/11. Such statements interfere with, rather than serve a careful and deliberate consideration of the issues.

The dangers of secrecy:

In addition to the fundamental change in the scope of and authority for government surveillance of Americans, the attendant secrecy has made it almost impossible to have the kind of informed public debate and democratic decision-making fundamental to the notion of self-government. It is not debatable that secrecy increases the danger that government will overreach. At the same time, there is no question that foreign intelligence activities depend to some degree on secrecy. A democracy must continually work to figure out ways to provide for the national defense while respecting civil liberties and preserving constitutional government. The increase in technological surveillance capabilities, global connectedness and the reliance on electronic communications has made doing this more complex.

The expansion of secret government surveillance and secret legal authorities especially in the last 12 years requires us to ask whether we are witnessing the serious erosion of our constitutional system of checks and balances and the rise of a system of secret law decreed by courts, carried out in secret, enabling the creation of massive secret government databases on Americans' personal and political lives. As you know, the system of checks and balances relies upon the existence of a Congress which engages in a public debate informed by the relevant information from the Executive; courts which hear two sides argue a question and know their opinions are subject to appeal and public critique; and an Executive branch who will be called to account for ignoring the law. All of this in turn depends upon an engaged press and informed public.

First step: necessary public disclosures:

The President has declared that he welcomes this debate and the Administration has already declassified some important information. This hearing and this Committee's involvement in the debate is a crucial step in restoring the needed transparency. The fact that the NSA is involved and that these programs (or at least the 702 program) may include legitimate foreign intelligence activities that do not affect Americans should not be used as a reason to bypass the jurisdiction of this Committee or the Senate Judiciary Committee. As this Committee has recognized ever since the introduction of the Patriot Act, surveillance authorities concerning information on Americans is at the core of this Committee's responsibilities; and congressional and executive branch procedures and rules for considering such legal authorities and conducting oversight should recognize the Judiciary Committees as full partners with the Intelligence Committees in these activities. As long ago as 1990, the Justice Department expressed concern

about the involvement of the Judiciary Committees.[2] This concern is not only misplaced, but inappropriate and we urge you to call upon the Executive Branch to treat the Committee as a full partner going forward and to insist that the rules of the House implement that understanding.

We urge the Committee first to insist on disclosure of sufficient information to enable the public to understand the existing legal authorities for national security surveillance of Americans and the scope of such surveillance. Such disclosures are necessary for an informed public debate, which in turn can inform Congress' consideration of these issues. We appreciate the legislation offered by the Ranking Member and others to accomplish this. However, we do not believe that legislation should be required in order to obtain the necessary disclosures from the Executive Branch and urge the Committee to make clear to the Executive Branch that you expect the necessary information to be disclosed as soon as possible and without waiting for enactment of legislation.

That information should include a full explanation of the FISA court's interpretations of existing law and the Executive's legal arguments made to the court, whether or not the court accepted them. If redaction of the court opinions and government pleadings is too time-consuming or difficult, the Executive should prepare a White Paper as soon as possible as it did in January 2006 about its legal basis for the NSA warrantless program after that program was revealed by The New York Times in December, 2005.

It is also essential to disclose the scope of the programs' collection and retention of information on Americans. As Professor Daniel Solove has pointed out: "secrecy at the level of

---

[2] In 1990, DOJ's Office of Intelligence Policy and Review wrote a memo to the Office of the Deputy Attorney General explaining that it had been "working with the National Security Agency for the past three years to develop possible amendments to the Foreign Intelligence Surveillance Act to meet a need created by technological advances." ... The 1990 memo ... identified several "policy and tactical issues" counseling against seeking new legislation. David S. Kris, "Modernizing the Foreign Intelligence Surveillance Act: Progress To Date and Work Still to Come," in *Legislating the War on Terror, An Agenda for Reform*, Ed. Benjamin Wittes, Georgetown University Law Center and The Brookings Institution, 217-251 (2009). These "policy and tactical" issues, included: "the fact that "committee jurisdiction in both the House and Senate is concurrent between the Intelligence and Judiciary Committees," and while the "problems giving rise to the possible amendments have all been discussed with the Intelligence Committees," they had not been discussed "with the Judiciary Committees"; "the risk of added congressional restrictions if the statute is opened up to amendment"; and " the fact that "the proposed amendment to FISA to resolve the NSA problem . . . *is certain to be written in such enigmatic terms that only those who have been briefed in executive session will understand them," thus risking "speculation in the media about what is really intended and probably deep suspicion that something sinister is going on*" (emphasis added). "Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Challenges," by David S. Kris, *Lawfare*, May 19, 2013, http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-challenges/#fn1. It is not clear that the Justice Department yet understands that the only antidote to media speculation and deep suspicion by the American public is openness about what is going on.

an individual suspect is different from keeping the very existence of massive surveillance programs secret." "Five myths about privacy," Daniel J. Solove, *The Washington Post,* June 13, 2013, http://www.washingtonpost.com/opinions/five-myths-about-privacy/2013/06/13/098a5b5c-d370-11e2-b05f-3ea3f0e7bb5a_story.html. Keeping secret the identification of any particular individual or group subjected to surveillance may be necessary in order to effectuate the goals of the surveillance, at least for so long as the surveillance and the underlying investigation continues. But to the extent that disclosure of the scope of U.S. government collection programs on Americans may make some investigations somewhat harder – and counterterrorism experts dispute that[3] – there is an overriding interest in public disclosure because it is essential to a democratic debate and decision on what is the proper scope of these programs. (Furthermore the rationale for keeping secret the legal interpretation of section 215 -- that disclosing the government's claim that legal authority exists for such a program, would reveal the existence of the program and thereby render it useless -- seems to have been undercut by the government's claim that the program continues to be necessary, even though its existence is now public.)

Public explanation and disclosure of related surveillance authorities, not just the 215 and 702 programs is also essential.

- For example, the press reports that there was a similar program to collect internet metadata that was halted in 2011. This Committee should insist that the Executive Branch publicly disclose whether such a program existed, what legal authorities were used; whether in its view existing legal authorities would allow the resumption of such program, and whether the government still maintains the metadata collected by that program.

- This Committee should demand public disclosure from the Executive Branch concerning whether section 215 or any other authority would allow mass collection of other kinds of records held by third parties, e.g., medical records, credit card records, or financial records. If not, then the Executive Branch should disclose why not.

- This Committee should also demand disclosure of any other FISA court opinions (or summaries) concerning legal authority for surveillance of Americans. The existence of such an opinion in 2007 has been hypothesized: "As far as I can determine, the government seems to have persuaded the FISA Court in January 2007 that the international gateway switches, which essentially are the junctions between the U.S.

[3] "The argument that this sweeping search must be kept secret from the terrorists is laughable. Terrorists already assume this sort of thing is being done. Only law-abiding American citizens were blissfully ignorant of what their government was doing." "Why you should worry about the NSA," Richard A. Clarke, *New York Daily News,* June 12, 2013, http://www.nydailynews.com/opinion/worry-nsa-article-1.1369705#ixzz2Z8OKOmUm.

and the rest of the world's telecommunications grids, are reasonably particular FISA "facilities," and that al Qaeda is using them. If that is right, it means that a handful of orders gave the government access to all, or almost all, of the international telecommunications traffic entering or leaving the United States. That is very speedy and agile. . . . The problem, of course, is that while al Qaeda is using those switches, so is everyone else. Even under the most extreme estimates, al Qaeda cannot account for more than a tiny percentage of calls transiting the switches." David Kris, "A Guide to the New FISA Bill, Part II," *Balkinization,* June 22, 2008, http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html.

- The scope of existing legal authorities can only be understood by understanding the history of FISA court opinions, even if such a 2007 opinion has been superseded by the 2008 enactment of the FISA Amendments Act.

- This Committee should demand public disclosure from the Executive Branch of a complete report concerning the overlapping authorities for collection of information about Americans' communications, e.g., national security letter authorities; pen register/trap and trace authorities. Without an understanding of how these authorities overlap and differ, it will be difficult to legislate adequate protections for privacy and First Amendment rights.

- This Committee should demand a complete public report from the Executive Branch concerning what rules apply to accessing, analyzing, data-mining, keeping, using or disseminating information concerning Americans' communications. That includes not only the "minimization rules" which have been classified without any apparent necessity for doing so, but rules and regulations issued by different agencies, for example, the FBI and DoD. As a former official and recognized expert in the field explains: "Today, a good deal of foreign intelligence collection is regulated by the Fourth Amendment and Executive Order 12333 and its subordinate procedures, *but not in any meaningful way by statute (emphasis added).*" David Kris, "Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach," *Lawfare,* May 20, 2013, http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/.

The number, complexity and overlap of authorities and rules is such, that a simple list of them will not be sufficient for the public to understand what its government is up to, nor for the Congress to exercise meaningful oversight. The Executive Branch, however is operating on the basis of an understanding concerning the standards and scope of legal collection and use of information about Americans. That understanding needs to be publicly shared with the Congress and the American public.

Substantive fixes to limit massive government surveillance and provide safeguards:

The current controversy provides an important opportunity to reexamine the existing surveillance regime. That examination depends upon a public accounting of what the government is doing, in order to have a debate regarding its risks and benefits and possible alternatives.

In order to ensure that such an accounting happens, we urge the Committee to consider revisiting the existing sunset for the FISA Amendments Act and to shorten it to align with the existing sunset for section 215 in mid-2015, so that these authorities will be revisited together. While there are some immediate fixes that could be adopted, it is crucial not to overlook the more fundamental questions at stake. For example, proposals to require more transparency of FISA court opinions or some kind of court advocate to oppose the government in secret , while perhaps useful, are not sufficient to address the fundamental change in judicial function wrought by giving the FISA court the job of approving programmatic surveillance or making constitutional rulings in situations where the individual whose rights are at stake not only never has an opportunity to appear before a court and challenge the ruling, but is never even informed that the government has amassed information about her.

There are also significant and complex technical questions that should be understood in evaluating these programs and designing safeguards, which questions have not yet been adequately discussed or analyzed. See for example Remarks of Steven M. Bellovin and Daniel Weitzner before the Privacy and Civil Liberties Oversight Board, July 9, 2013, http://www.pclob.gov/9-July-2013. A former NSA mathematician and analyst has also proposed a way whereby when the NSA collects and analyzes massive amounts of data on Americans without any particularized warrant, a warrant would be required before the identity of that American and the results of that analysis or information could be shared with other parts of the government and acted upon.[4]

Again, we appreciate the opportunity to appear before the Committee as part of this work and would be pleased to offer whatever further assistance might be useful.

[4] See William Binney's description in "The Secret Sharer, Is Thomas Drake an Enemy of the State?" Jane Mayer, *The New Yorker*, May 23, 2011, http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.

Mr. GOODLATTE. We will have more opportunity to speak in just a moment.

Ms. MARTIN. Thank you.

Mr. GOODLATTE. But we will begin with the questioning, and I will start with Mr. Jaffer. If the acquisition of metadata is the type of mosaic of information that Sotomayor warned about in the Jones case, how would you limit the Government from collecting it?

Mr. JAFFER. Well, one possibility would be to require the Government to get an individualized warrant for that information. And whatever the answer to that question is, I think that there have to be more safeguards than are in place right now.

Even the Government seems to concede that its surveillance of this kind of information has to be reasonable under the Fourth Amendment, and I just don't see you how can possibly justify the collection of everybody's phone records on that standard. And I think many Members rightly pointed out that no other court has ever granted a subpoena, has ever upheld a subpoena that sought records on that scale.

Mr. GOODLATTE. That is with regard to 215. One objection you have to 702 information collected is that information about Americans can be swept up in the search for foreign intelligence information. But isn't that the case with any Title III wiretap?

Mr. JAFFER. It is the case, and that is why the courts apply a reasonableness analysis. And all we have argued in the context of challenges to 702 is that the same reasonableness analysis has to be applied to the Government surveillance under that provision.

And the Government in our constitutional challenges happen to have actually conceded that point. The only dispute was whether these procedures were, in fact, reasonable, and we don't think they are.

Mr. GOODLATTE. If the FBI is conducting a wiretap of a business that is also part of a criminal conspiracy, innocent third parties sometimes are involved, and they are monitored. That information is minimized to protect the people's privacy. How is this different from Section 702 surveillance, which must be also minimized?

Mr. JAFFER. Right. I think that is a good question. I think that one of our concerns is that the word "minimization" is being used as a kind of talisman as if when the Government invokes the prospect of minimization, that should end the discussion. But you have to look at what the Government means when it says minimization.

And fortunately, we now have the Government's minimization procedures under 702. They were released by the Guardian and by the Washington Post, and they allow us to evaluate the extent to which those procedures actually protect Americans' privacy. And I think it is quite clear from the procedures that they don't protect Americans' privacy. They allow the Government to sweep up Americans' communications, both domestic and international, to retain those communications forever to the extent that they include foreign intelligence information, a term that is defined very broadly under the statute.

Even if the communications don't contain foreign intelligence information, they can be retained for as long as 5 years. So these are procedures that don't do very much to protect Americans' privacy.

Mr. GOODLATTE. Let me turn to Mr. Baker and Mr. Bradbury and ask them if they want to comment on Mr. Jaffer's observation and tell us why it is necessary to collect a broad set of metadata under Section 215. Does this help the Government connect the dots?

Mr. BAKER. The difficulty the Government faced is that each telecommunications company keeps its records as it chooses, and they may maintain the records for a year or two, but they won't keep it for a long time. And you can't easily chain from one database to the next to find out the communications of the people who are linked to the person that you are investigating.

And so, and to ask the companies to keep it for the Government's convenience, to consolidate the database for the Government's convenience is something that is really asking quite a bit of a private citizen just to help the Government do its job. So the Government did this and then acted——

Mr. GOODLATTE. But let me interject that depending upon the cost of the Government taking it and gathering it and holding it, we are asking all those phone companies' customers, who are also taxpayers of the United States, to bear that burden.

So I understand the problem with asking the phone companies to do it. But we also have to evaluate whether the benefits derived from this are justified by the costs of it.

Mr. BAKER. That is a perfectly fair point, although the rate payers and the customers of the phone companies will pay for it in the end if it is a cost to the companies. But I agree with you that it is a cost to the United States. I think it is a cost that we bear because we are trying to protect all Americans from terrorism, and that it is fair for the U.S. Government to bear that cost.

In the end, though, the searches can't be done without a reasonable and articulable suspicion, which in practice has turned out to be much tougher than the standard for serving a subpoena on an individual telephone company. As I said, there are hundreds of thousands, perhaps a million such subpoenas.

Mr. GOODLATTE. I understand. But that also leaves aside the question of whether the Congress intended to give the NSA the authority to gather the data in the fashion they did under the business record provision.

But let me ask Mr. Bradbury another question, and he can comment on this as well, if he'd like. Mr. Jaffer's testimony claims the Government is tracking all American phone calls under the 215 program. Is this what is happening?

Mr. BRADBURY. No. As I indicated, they are not tracking calls. They are not monitoring calls. The data sits in a database and is only accessed when there is a suspicious number, and you want to find the links and connections that that number has to other numbers.

But you need to have the whole database, and getting the whole database is relevant to the counterterrorism investigation because you cannot do the kind of sophisticated link analysis that the NSA does without having a comprehensive set of data.

It doesn't have to be every single call record, but it has to be the largest collection you can get in order to effectively find all of those connections. And that is because of the technical way that they do

it, but it is a super valuable tool, and getting the database is relevant.

It would be the same if we had a suspicion that a terrorist had come into the country, but we didn't know exactly on what flight or where. And you could use 215 to get the flight manifests of all flights in and out of the country during a period of time, and you could put it in a database and you could query the person's number, name to find out when he came in. It is relevant.

Mr. GOODLATTE. You raised a good analogy, but my debate professor said analogy was the weakest form of argument. So are you suggesting that it would be appropriate if the airlines did not keep that data for a sufficient period of time, that it would be appropriate for the Government to tell all the airlines to provide them with all of the flight records of all American citizens so they could hold it in a database and check it when they needed to?

Mr. BRADBURY. Well, it might be. It might be something that you have to do to find that particular flight that you need to protect——

Mr. GOODLATTE. Well, I wouldn't argue that there might be occasions when that information would be useful, but it would have to be weighed against both the cost of storing the data—and that is just not, you know, computer capability, but also people to manage that—and the risks that are entailed by those people abusing that system, if that, indeed, occurs.

Let me turn to Ms. Martin, however, and your testimony includes a number of suggestions for increasing the visibility into the—increasing visibility into the FISA programs. Which of these would you prioritize as a way to both preserve our national security efforts while also giving the public a better understanding of how the programs work?

Ms. MARTIN. I think that it is key to obtain an understanding of the court's understanding of its legal authorities, not just 215, but all of them and the Government's interpretation and understanding of those legal authorities. I think it is also key, and the second thing that I would prioritize is getting a report from the Government how the existing FISA Authorities complement, overlap, and differ, and—and what they allow and what they don't allow.

I think, otherwise, we are going to be in the situation where we are talking about fixing 215 with regard to phone metadata without knowing how the Government is going to use national security letters or pen traps or 702 to get the same kind of data. So I would prioritize knowing the law and understanding how that works and the Government's understanding of the legal authorities. And then after that, some idea—some idea, not the specifics—of the scope of the collection that is being done on Americans.

Mr. GOODLATTE. Thank you very much.

My time has expired. The Chair recognizes the gentleman from Michigan, the Ranking Member Mr. Conyers, for 5 minutes.

Mr. CONYERS. Thank you, Chairman Goodlatte.

This has been a very important hearing, and I wanted to begin by asking Professor Martin about the decision by Justice Alito, a 5-4 decision as usual, responding who dismissed a number of groups for lack of standing. Reasoning that respondents can't manufacture standing by choosing to make expenditures.

Is the harm alleged by, among others, Amnesty International and ACLU hypothetical, which was the basis of this conservative decision?

Ms. MARTIN. Thank you for that question, Mr. Conyers.

If I might answer it, that case, of course, was a challenge to the constitutionality of the 702 collection program. And one of the points that the Government made when it argued that the ACLU and Amnesty didn't have the kind of particularized standing or showing of harm that the Constitution required was that others would be able to challenge the constitutionality of 702 collection and, in particular, individuals who were prosecuted using the fruits of such 702 collection.

Well, now it turns out that the Government won't even tell such people that it used the fruits of 702 collection in making a criminal case against them, and they are not given that opportunity to challenge the 702 collection. I do think that it is an appropriate question for the Congress to worry about wether you have designed a system that allows the Government to collect massive amounts of information about Americans, in secret, but somehow you haven't set up any mechanism that the Supreme Court is going to recognize as granting standing to anybody to challenge the fact that information about them has been collected. That is a problem that Congress can solve and should solve.

And that is a fundamental difference, of course, between foreign intelligence collection authorities that we are talking about today and the kind of criminal justice collection authorities that were discussed, which is that there is the possibility of an open, adversarial court challenge to criminal collection, which doesn't exist in this context.

Mr. CONYERS. Can I ask——

Ms. MARTIN. And to tell my colleagues——

Mr. CONYERS. Can I ask, Mr. Jaffer, in addition to your four recommendations, is there a way that we can reconcile our concern against terrorism and at the same time permit the largest usefulness of privacy possible? You know, after all, if it hadn't been for a couple of people leaking, we wouldn't have known about any of this, as far as I am concerned.

Some say that somebody made a statement on the floor of the House. If you happen to have caught it, you could go back and track it. But I think I am more concerned about the collection legality than I am about the uses to which it is put.

Mr. JAFFER. Well, I think that you ought to be concerned about the collection. The collection in the first instance implicates privacy. It has a real effect on privacy. That is where the privacy intrusion happens in the first instance.

And it also has a chilling effect on activity protected under the First Amendment. It is the Government's collection of that information that has the chilling effect. If you remember during the 1960's and '70's, some State governments used subpoenas served on the NAACP as an effort to chill association with the NAACP.

And it was just the acquisition of that information that was chilling, and those governments knew it. And——

Mr. CONYERS. And more chilling now than anything is the fact that they have got information through phone numbers, which can

easily be attached to names, of everybody in the country for at least 6 years. And that is probably the most disturbing aspect of this matter to me that I have been hearing today.

Mr. JAFFER. Mr. Conyers, if I could just point out that even if you accept the Government's frame here and focus only on the uses, I don't think anybody should be misled by this 300 number, which makes it sound like this is a very targeted program. But if you think about the 300 number in relation to what was said on the previous panel about three hops, the first hop takes you to, say, 100 people whose communications are pulled up. The second one takes you to 10,000, and the third one takes you to 1 million.

And you do that 300 times. I think it is safe to say that every American's communications have been pulled up at least once.

Mr. CONYERS. Thank you very much.

Mr. GOHMERT [presiding]. I will recognize myself now, and I appreciate your being here.

It is intriguing, what we are talking about. We are talking about the privacy, the type of concerns that spawned a revolution back over 200 years ago. We hear all this information about the FISA courts, and that is the bulk of what you are being—you are talking about.

Anybody care to just briefly tell us what happened before there was a FISA court? We know there have been national security secrets since the revolution itself. What happened before there was a FISA court to protect us from ourselves?

Mr. JAFFER. It was left up to the executive. It was unilateral action by the executive in the area of foreign intelligence surveillance. And in fact——

Mr. GOHMERT. But here, we are talking about surveillance of Americans, in-country American citizens, and that is what I am talking about. If someone wanted to gather intelligence information about American citizens on American soil, normally, having been a judge and chief justice, it is my understanding, you went to a court.

You might be requesting in camera review of documents. You might request that the court documents be sealed. But we were able to work pretty well getting court orders before there was ever a FISA court was my understanding.

Mr. JAFFER. Actually, Mr. Chairman, prior to 1972, for any national security investigation, or many, they were done without court approval, without warrants. And the United States Supreme Court in the Keith case, 1972, said when it is a domestic security threat, there has to be a warrant.

Left a footnote was not deciding foreign security threats. Even if it is a U.S. citizen, but associated with a foreign power that is threatening to the United States. And the lower courts consistently held that the President could conduct warrantless surveillance for foreign intelligence purposes even of U.S. citizens and that the fruits of that surveillance could later be used in a criminal prosecution, even if it hadn't been supported by a warrant.

That is what the lower courts held. Of course, that did lead to abuses because the executive is making determinations about what he thought was a foreign threat, and lines were crossed and abuses occurred. That is why Congress and the executive branch reached a compromise in 1978 and created the FISA process to involve Arti-

cle III judges in the review and approval of those surveillance orders and also involve the Congress through the creation of the Special Intelligence Committees for oversight, which hadn't occurred before.

And so, we have this compromise situation where the branches have come together to involve all three branches. And of course, limitations were discovered after 9/11. A lot of debate occurred, and ultimately, Section 702 was passed in 2008 to enable a very broad programmatic order for foreign collection directed at non-U.S. persons outside the United States.

Mr. GOHMERT. And that is a great distinction because I know in my freshman term, '05 and '06, what we were told is this is only for you have to be a foreign agent, a foreign individual. And as long as it is an American citizen here on American soil with distinction for American citizen where intelligence gathering in another country didn't violate local law. There were all those distinctions being discussed.

But even through all of that, my experience with conservative and liberal judges would have indicated that you wouldn't have an order from a judge under our Constitution that requires specificity as to a place and information be gathered that would say something like this order from this court does. All call detail records between the United States and abroad or wholly within the United States, including local telephone calls.

I think that pretty much covers everything. I see no specificity here. Oh, yes, just get all the records. And you should be comforted by the fact that you can get this stuff. It is okay.

So I am just concerned. I have now seen the incredible abuse by the FISA court, in my opinion, and I am just wondering if we are better off going to a system where we don't require a FISA court. There is not this Star Chamber. What would be another alternative?

And that will be my last question.

Ms. MARTIN. If I might, Mr. Gohmert? I think that the original conception of the FISA court was quite limited and perhaps quite useful, which was that it would act as a kind of usual court in issuing a warrant, right, which is always done *ex parte*. Because the search that the FISA court was going to authorize—which had to be particularized—had to be based on probable cause, was never going to be revealed, Congress set up secret procedures for doing that.

But it was always recognized that what we are talking about is searches and seizures of Americans. And now the Government has taken the concept of a FISA court to kind of, in my view, put a fig leaf on a totally different kind of collection directed at Americans. It is not particularized. It is totally in secret. And that includes the 702 program, which——

Mr. GOHMERT. Right.

Ms. MARTIN. And so, you need to go back to the drawing board about are we really going to have unparticularized collection that is intended and does collect information about Americans?

Mr. GOHMERT. Well, let me tell you we have got votes coming up in just a few minutes. And so, I want to get to people who want to ask questions.

But I would ask the witnesses if you have any proposals, if you could provide that in writing to us, any alternatives, any major changes, because I think this justifies major changes.

And with that, who is next? Okay. Recognize the gentleman from New York, Mr. Nadler.

Mr. NADLER. Thank you.

Mr. Jaffer, various Administration officials have used comparison of Section 215 authority to what can be obtained through a grand jury subpoena, something we expressly include in the statute itself as a limiting principle. Are you aware of any examples where by virtue of grand jury subpoena, law enforcement has been able to engage in the type of ongoing bulk collection, what you described as dragnet collection of information done under Section 215?

Mr. JAFFER. No, not even close.

Mr. NADLER. Mr. Baker, are you aware of any such?

Mr. BAKER. There are plenty of subpoenas for massively overbroad collections of data so that the Government can be comfortable that it has gone through everything that might be relevant.

Mr. NADLER. There are subpoenas, grand jury subpoenas for, in effect, everything in the world without being specific, all metadata?

Mr. BAKER. Addressed to a particular case or database, there are plenty of cases where a single database has been subpoenaed.

Mr. NADLER. No, a single database. But has there ever been a grand jury subpoena that says let us see the outside of every postcard or letter sent in the United States? Or let us see the phone numbers of everybody who called anybody in the United States?

Mr. BAKER. So if I could go back to an example that the Chairman mentioned, as a practical matter, every flight that comes into the United States, every travel reservation on that flight is provided to the Government by the carrier, every single one.

Mr. NADLER. Has there ever been—has there been a subpoena for every flight record in the United States?

Mr. BAKER. Every flight record coming into the United States, yes.

Mr. NADLER. A subpoena for every flight record?

Mr. BAKER. No. It is under a law passed by the United States Congress that says you must provide this information to the Government so it can search for terrorists.

Mr. NADLER. You must provide the name of every individual on every flight?

Mr. BAKER. Yes. That was passed in 2002, and it has been enforced.

Mr. NADLER. And that is a subpoena?

Mr. BAKER. And it has caught a lot of terrorists.

Mr. NADLER. Excuse me. That was a subpoena?

Mr. BAKER. No.

Mr. NADLER. That is a law?

Mr. BAKER. It was a law.

Mr. NADLER. Well, that is a little different from a subpoena.

Okay. Mr. Bradbury, you talk about how the metadata that is acquired and kept under this program can be queried when there is responsible suspicion, as if that meets the statute. The statute

talks about collection. You seem to be talking about query. There is a difference between collection and query.

Mr. Jaffer, let me ask you this. Does the Fourth Amendment talk to collection or to queries?

Mr. JAFFER. Collection.

Mr. NADLER. Collections. So a broad—okay. Let me go to the next question because I have a bunch quickly.

Mr. Jaffer, you talked—Mr. Baker, rather, you talked about Section 702, as the discussion of Section 702 has really hurt us because it has told the Europeans and everybody else what we are doing for foreigners. But nothing, as I think you point out in your testimony, too, nothing that we have learned about Section 702—I can't think of anything we have learned about Section 702 from Mr. Snowden—or however you pronounce his name—that wasn't included in the debate in 2008 on Section 702, when we knew we were going to be collecting across the board on everybody.

And the question in that debate was—and I thought the resolution of that debate was inadequate, which is why I voted against it—how were we going to protect Americans against being caught up? And this is what we have been talking about.

But the assumption there was that foreigners have no constitutional right and no privacy rights. And we can get all the information on them anyway. So how is this information now harmful in a way that the congressional debate wasn't?

Mr. BAKER. I think that the congressional debate seeded what we are now seeing. It is a cost. It is a cost of having the debate we are having, and my point here is that Europe will extract that cost from companies that did nothing but their obligation under the law.

Mr. NADLER. But they would have extracted that cost just because of the congressional debate, if they were paying attention.

Mr. BAKER. What I say is that this Congress and this Administration has an obligation to stand between those companies and——

Mr. NADLER. That is a separate discussion, and that may be. But—okay. Ms. Martin, how can we—how can Congress solve the problem? We have a basic problem.

Every challenge to abuse of constitutional rights by the Bush administration and the Obama administration has been met in the same way. Either the use of the state secrets doctrine to say you can't go to court on that. The subject matter of the discussion is a state secret. Therefore, move to dismiss the case ab initio. Or you have no standing because you cannot prove that you personally were harmed by this.

Now Mr. Snowden may have done a public service in giving some people standing by proving that they were harmed by this because anyone who is a Verizon subscriber arguably can now go into court and say that. How can we deal with these two problems that an Administration, any Administration can violate constitutional rights from here to kingdom come, subject to no court review because of either the state secrets doctrine or the standing problems because they don't admit what they are doing in the first place. It is secret.

It is secret what we are doing to you. Therefore, you have no standing because you can't prove what we are doing to you.

Mr. GOHMERT. The time has expired, but you may answer briefly.

Ms. MARTIN. Well, I think one key way of doing it, which is outside the court system, is for the Congress to insist that the Administration disclose all that information. The Government then won't be able to claim state secrets because it has disclosed the information.

Mr. NADLER. Disclose what information?

Ms. MARTIN. Disclose the information about what it has done and who it has done it to, right? And something like that did happen and is happening in the context of the violations of the laws against torture, and that helps in creating a consensus that we know the Government violated the law.

We have some kind of public debate about what the Government shouldn't do, and whether or not we end up with an individual remedy in the court is a question that I would be glad to think about some more. I know there are now five lawsuits seeking individual remedies that have a better chance than they did before, but they all depend upon public disclosure by the Administration of information.

Mr. NADLER. Or by Mr. Snowden or somebody else.

Ms. MARTIN. Well, that is more difficult because then the Administration claims state secrets.

Mr. GOHMERT. We are going to have to—in order to get the other two Democrats and one Republican left, we are going to need to move on. But I would ask if you have additional information, if you would prove that in writing in response to that question.

And now at this time, we yield 5 minutes to the gentleman from Idaho, Mr. Labrador.

Mr. LABRADOR. Thank you, Mr. Chairman.

Mr. Jaffer, I am trying to figure out how we got from *Smith v. Maryland* to the moment that we are at today. Can you try to explain to me what exactly maybe the proponents of these laws and the interpretation of these laws are trying to say because I am not following *Smith v. Maryland* very well. I have read it a couple of times.

Mr. JAFFER. Right.

Mr. LABRADOR. But I am not sure that you can get to the collection of metadata all over the United States.

Mr. JAFFER. Well, I think that there is a vast chasm between Smith and the kind of surveillance that is going on now. Smith was a case about a specific criminal investigation. It was a pen register installed on one person's phone for 2 days.

We are now talking about 7 years of surveillance of every American's phone calls. So I don't think it is a serious argument to say that Smith justifies what the Government is doing now. I think that the more relevant case is Jones, which was decided just last year. A 9-0 court found that the tracking of individuals' location over the long term constituted a search under the Fourth Amendment, and even in Jones, the surveillance was narrower and shallower than the kind of surveillance we are talking about today.

Mr. LABRADOR. And they said that the tracking of individuals over a long period of time resulted in a search and seizure. Can you

explain why they said that? Because there is now an argument that collecting all this data actually gives you very personal information about the individual.

Mr. JAFFER. That is right. Sometimes we talk about metadata as if it is less sensitive, and that is not really true. Using this kind of metadata, in Jones, for example, the court noted that you could, just tracking somebody's location over a long period of time, you could draw all sorts of accurate conclusions about their medical history, about their intimate relationships, about their professional life, about their personal life.

And the same is true of phone calls. If the Government has access to your call records over a long period of time, the Government can draw all those conclusions in the same way.

Now that is not to say that the Government should never have access to the phone records. There are circumstances in which the Government has to have that access, but we just want to make sure that that is limited to cases, specific cases in which the call records are, in fact, relevant to an investigation.

Mr. LABRADOR. And in *Smith v. Maryland*, there was a specific reason why it was relevant. Correct?

Mr. JAFFER. That is correct. Even in Jones, there was that specificity.

Mr. LABRADOR. Okay. So because what concerns me is that, I think as a Government official, as a legislator, I would like to stop gang membership, for example, or I would like to stop child pornography, or I would like to stop bank robberies. And I could maybe pass a law that would require the Government to collect everybody's data, right, everybody's metadata so we can stop those crimes. What do you think about that, Ms. Martin?

Ms. MARTIN. I think that is the proven solution of countries like the Soviet Union and China.

Mr. LABRADOR. Exactly.

Ms. MARTIN. I mean, and I think there have actually been studies showing that you can stop crime by that kind of government surveillance and collection.

Mr. LABRADOR. So, Mr. Baker, what is the difference? I want to stop all these crimes, and I would think that everybody in this Congress would think that that would be inappropriate for me to pass a law that would allow me to collect all the metadata of every American so I could stop child pornography.

What is the difference between that and what is happening here in this instance?

Mr. BAKER. We are responding, in the case of the 215 programs, to the fact that there is a well-organized, offshore conspiracy seeking to carry out attacks on us.

Mr. LABRADOR. I understand that, but—and I agree with that. And that is why maybe I don't have as much problem with the 702 program.

But you are collecting the data or the Government is collecting the data of American citizens and saying that it may become relevant after we collect it. Why not just collect the data of every American because it might become relevant in a child pornography case later?

Mr. BAKER. All of these searches, there is really two issues here. First, is it a search at all? And Smith suggests it isn't. And if it is a search, is it reasonable? And that depends in part on the nature of the justification and the problem that you are trying to solve.

In this case, we are trying to solve a problem that requires classified tools and is a national security threat. That is different from trying to stop bank robberies, frankly.

Mr. LABRADOR. Well, and I just find it fascinating that the author of the PATRIOT Act and most of the Members of Congress who voted for the PATRIOT Act had no idea that the Government would go to these lengths to collect data. And I hope that we can continue to have these hearings.

Thank you very much for being here.

Mr. GOHMERT. The time has expired. Thank you very much.

Mr. LABRADOR. I yield back my time.

Mr. GOHMERT. I yield to the gentleman from Virginia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

I know we are trying to get three Members in in this very short period of time. So let me just pose a question for Mr. Jaffer real quick.

I am interested in what you can do with the data after you have gotten it. There is a real question as to whether you have the legal authority to get all the phone calls. But after you have got it, we found out in a DNA case that if you get someone's DNA legally and you find out it is not them, you can still run that DNA through the database without any probable cause, no articulable suspicion, anything. You have the data, and you can use it.

What is the limitation on the data after you have acquired it? Now they say you have to have articulable suspicion to query the data that you have obtained. But the Section 215 doesn't require any such limitation. It just tells you to describe what you are getting. This seems to be a little gratuitous policy, not a limitation by statute.

And so, can you say a word about where the limitation is after you have gotten the data what you can do with it?

Mr. JAFFER. Well, on the 215 program, we don't have the Government's minimization procedures. They haven't been released.

Mr. SCOTT. Well, let me just—and the minimization procedure specifically has—the witness before was a little murky on this—has—specifically has a criminal justice exception. So running a criminal justice investigation with data you now have can be done without articulable suspicion or probable cause or anything. You just go look to see, as the gentleman was suggesting, who has been committing gang crimes.

You got a gang member, you can spin his little thing around to find out who he is talking to. Is there a limitation on what you can do after you have gotten it?

Mr. JAFFER. No, almost certainly not. And we know that that the limitations are very weak because we have seen the 702 minimization procedures. Those were disclosed.

And if they are any guide, I think it is safe to assume that the 215 procedures don't protect Americans' privacy.

Mr. SCOTT. Now if you were running a criminal investigation without probable cause by virtue of getting information in the hands of the FBI, and we have removed that firewall that used to be there, what would be the sanction against improperly using that information? Would the exclusionary rule kick in?

Mr. JAFFER. Well, I don't think we will ever know because the Government doesn't notify criminal defendants that it is using these kinds of surveillance programs.

Mr. SCOTT. Would fruit of a poison tree kick in?

Mr. JAFFER. Well, it would if the Government disclosed. But it doesn't disclose. It keeps it secret from criminal defendants, and this is one of the things that we have been very frustrated with is that the Government told the Supreme Court that criminal defendants would be notified when information was introduced against them derived from these programs. And it is not, in fact, giving that kind of notice.

Mr. SCOTT. Thank you.

Mr. Chairman, as a courtesy to my colleagues, I will yield back at this time.

Mr. GOHMERT. Thank the gentleman from Virginia.

At this time, I will yield to Mr. Johnson for 5 minutes.

Ms. JACKSON LEE. Mr.—excuse me, Mr. Gohmert. This is regular order.

Mr. GOHMERT. Okay. Well, I was just going by the list that the clerk gave me here.

Ms. JACKSON LEE. The list goes from the beginning of the Committee. I think Mr. Johnson knows.

Thank you.

Mr. GOHMERT. Exactly. All right. Then we will yield 5 minutes to my friend from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. I thank you very much.

Let me just say that this has been not eye-opening, but it raises more questions than probably it gives answers. And I think I want to start immediately with the question, Mr. Jaffer, on the 215 PATRIOT Act, which grants the FBI broad authority, as we have seen in the previous hearing and what we have read, and could put and does put civil liberties at risk. From your perspective, what danger might occur or what would happen if we did not renew Section 215?

Mr. JAFFER. Well, I think that is a good question to ask the Government. So far, they haven't been able to explain why the dragnet surveillance under this provision is actually necessary. They haven't been able to point to cases in which this particular surveillance program was crucial. I think it is a good question to put to them.

But I would just say that while I think that your concern about 215 is totally justified, I think that the Committee ought to be concerned about 702 as well. And the Government keeps emphasizing that this is a program directed at people abroad, and that is true. But in the course of surveillance of people abroad, the Government is building huge databases of Americans' phone calls, not just the metadata. But the——

Ms. JACKSON LEE. So you are saying that reverse targeting is occurring, even though language put in the bill to not have that occur?

Mr. JAFFER. I actually am not saying that the Government is violating the statute. I am saying that they are using the statute precisely as it was designed to be used, but the statute allows them to gather Americans' communications so long as they are not targeting a specific American.

Ms. JACKSON LEE. So to hold them until they believe something rises to the top?

Mr. JAFFER. That is right.

Ms. JACKSON LEE. So it is sort of like storing in your Internet or storing pictures in your iPhone or something of the sort?

Mr. JAFFER. That is exactly right.

Ms. JACKSON LEE. Let me to go Mr. Baker. You sat before Homeland Security a number of years. Thank you for your service. Thank all of you for your service. But you made the point that on your blog, that you thought that the FBI could have caught the people on 9/11, but there was too liberal—civil liberties was too much in the way.

What are you suggesting when the idea of 9/11 was, one, these were foreign nationals. So the FBI had opportunity to deal with them in the construct of our civil liberties, and it was basically connecting the dots or not finding out that guys were learning to take off and not land in a plane training place down in Florida. What civil liberties need to be violated in order to have protected us from 9/11?

Mr. BAKER. The problem is that there were two al-Qaeda operatives in the country for 2 weeks. We knew—the FBI, the CIA all knew they were here, but the FBI's task force that was organized for the Cole bombing, as I remember, was not allowed to go looking for them, even though they had by far the most resources of anybody to find them.

And the reason they were not allowed to do it was because the FISA court had made up a doctrine that led to the wall that said we are going to keep law enforcement over here and intelligence over here and not allow them to talk. And out of fear that the FISA court would punish them for talking and for going to look for these guys, the Cole task force stood down.

We lost our best chance to catch those guys at that time, and it was because the FISA court was so aggressively enforcing a doctrine that, frankly, it shouldn't have adopted in the first place, but which it adopted pretty clearly for civil liberties reasons.

Ms. JACKSON LEE. Well, let me ask your comment on that.

Ms. MARTIN. I think the record is much more complex. There were many times that the Government dropped the ball when it might have stopped 9/11, and most of them had absolutely nothing to do with the law. The CIA, for example, knew for many months the names of the hijackers. They knew that they wanted to carry out an attack against the United States. They knew that they had gotten visas, and they didn't tell the FBI to go find those people inside the United States.

And the wall had nothing to do with preventing the CIA from telling the FBI to go find known al-Qaeda terrorists in the United

States. The record is just much more complicated than Mr. Baker is making it out.

Ms. JACKSON LEE. Well, let me just finish. So let me just make this comment. Maybe I will be short of the red light.

One, I maintain that we have too many contractors unknown and unbeknownst in the intelligence community. I thank them for their service, but they need to rein in this rampant proliferation of contracts, even though the Government tried to defend its satellites as this, and really have a profound staff that is here in the United States Government.

The last point is the FISA court can stand a lot of review. One, I think there should be something about the balance of Democratic appointed judges and Republican. But I also think the release of opinions should be something that we should be able to allow to the public and, therefore, find a way to rein in all of this.

I yield back.

Mr. GOHMERT. Thank you.

We have 4½ minutes left—4 minutes, 20 seconds left in the vote. So I yield to the gentleman for such time. Mr. Johnson?

Mr. JOHNSON. I will be brief. Thank you, Mr. Chairman.

Section 702, collecting foreign data, intelligence data, metadata content of communications, and so forth. Is that correct?

Mr. JAFFER. Not quite. Section 702 is surveillance directed at people outside the United States, but it is surveillance of Americans' communications with those people outside the United States.

Mr. JOHNSON. Yes, and collection of the scope you don't disagree with. In other words, content metadata?

Mr. JAFFER. That is right.

Mr. JOHNSON. And minimalization procedures in place that perhaps may not be as stringent as they should. Perhaps. I am not saying that that is the case or not.

But with respect to the data collected under 702 of Americans that are just incidentally caught up in foreign-to-foreign communications or a foreign target that is communicating with someone in the U.S., who owns that data? Is it the person who initiates the call? Is it the person who accepts the call? Or is it both or——

Mr. JAFFER. My guess is——

Mr. JOHNSON. Or is it the provider, the service provider who owns the data?

Mr. JAFFER. I think that Americans have a reasonable expectation of privacy in their international communications.

Mr. JOHNSON. Have there been court cases specifically on that point?

Mr. JAFFER. Yes. On the content of communications, yes.

Mr. JOHNSON. Yes. Okay. So now, I would submit that when you are talking about surveillance, when you look at the definition of the word "surveillance," it includes keeping a close watch on people or things. And so, you can surveil a thing. That thing may not have a constitutional right, but a person certainly does.

I think we should make or I think we should be prepared to distinguish between surveillance, what kind of surveillance we are talking about. That is a term that kind of gets everybody excited.

That is about really all I have to say. Anybody got any comments about that?

[No response.]

Mr. JOHNSON. I will yield back, Mr. Chairman.

Mr. GOHMERT. The time has been yielded back. And at this time, this concludes today's hearing.

Thanks to all of our witnesses for attending. We know it has been a long day for you, and we appreciate you bearing with it. It is an important subject. It is only our future, our security, and our privacy.

So thank you, and we look forward to your comments that we anticipate receiving back in writing, things that you wished you had said or wanted to say, and to direct us. So thank you very much.

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

This hearing is now adjourned.

[Whereupon, at 2:32 p.m., the Committee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Questions for the Record submitted to James Cole, United States Department of Justice; Robert S. Litt, Office of Director of National Intelligence; John C. Inglis, National Security Agency; and Stephanie Douglas, FBI National Security Branch*

Questions for the Record from Representative Steve Cohen (TN-09)

For: Mr. James Cole, United States Department of Justice;
Mr. John C. Inglis, National Security Agency;
Mr. Robert S. Litt, Office of Director of National Intelligence; and
Ms. Stephanie Douglas, National Security Branch, Federal Bureau of Investigation

FISA Court

Throughout the hearing, you assured the Committee that the surveillance programs that Members expressed concerns about are legal and proper, in large part because the Foreign Intelligence Surveillance Court, or FISA Court, has ruled that they are. However, it is critical the Members have a fuller understanding of how this court operates and who sits on the court since we entrust it to make such important decisions about the proper balance between national security and personal privacy.

1. In the last five years, how many of the FISA Court's decisions, orders, and opinions were made by only one judge acting alone?

2. How many of these decisions, orders and opinions were made by a three-judge panel?

3. How many of these decisions, orders and opinions were made by the court acting *en banc*?

4. How many cases were appealed to the Foreign Intelligence Surveillance Court of Review?

5. When the FISA Court acts as a three-judge panel or *en banc* or the Foreign Intelligence Surveillance Court of Review hears cases, is a simple majority sufficient to issue an order or decision?

6. How many dissents were issued by judges acting in a three-judge panel, *en banc*, or on the Foreign Intelligence Surveillance Court of Review?

7. Given the enormous power that the Government seeks when obtaining permission from the FISA Court, shouldn't there be a third party specifically assigned to argue against the Government so that the Court can hear the other side?

8. Wouldn't the public be more accepting of the programs you are defending if they could read at least a summary of the FISA Court's decisions? Would you support publishing unclassified summaries of these decisions?

9. Under current law, the FISA Court need only deliver to Congress those decisions, orders, and opinions that involve a "significant construction or interpretation" of law. Who determines what is a significant construction or interpretation of law and what will be transmitted to Congress?

*The Committee had not received a response to these questions at the time this hearing record was finalized and submitted for printing on December 12, 2013.

Privacy and Civil Liberties Oversight Board

Back in 2004, this Committee's Subcommittee on Commercial and Administrative Law spearheaded the effort to create the Privacy and Civil Liberties Oversight Board.

After some reorganization and confirmation of its chairman, it is now up and running and has held a number of hearings and have issued its semi-annual report.

1. To what extent have your agencies been working with the Board to ensure that intelligence programs do not unduly infringe on privacy and civil liberties?

2. Will you commit to working closely and cooperatively with the board going forward?

Response to Questions from the Hearing from Stewart A. Baker, Steptoe & Johnson, LLP

Oversight Hearing on the Administration's use of FISA Authorities
Committee on the Judiciary

United States House of Representatives

Held July 17, 2013

September 13, 2013 Response to Supplemental Question by Stewart A. Baker
Partner, Steptoe & Johnson LLP

Question:

> Mr. GOHMERT. . . . But I would like to ask the witnesses if you have any proposals, if you could provide them in writing to us, any alternatives, any major changes, because I think this justifies major changes.

Response:

It is becoming increasingly obvious from the nature of the documents that have been leaked that Mr. Snowden and some of those working with him are quite prepared to release material that harms U.S. security, even when the material reveals no misconduct. While it is always useful to periodically review oversight mechanisms like the FISA court, in the present climate, I would caution against radically changing how we provide oversight of foreign intelligence surveillance. To respond in knee-jerk fashion to revelations that may be more advocacy than journalism would make bad law and reward Mr. Snowden's illegal actions.

Response to Questions for the Record from Jameel Jaffer, American Civil Liberties Union (ACLU)

Answers to Questions for the Record of
The House Judiciary Committee

Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy
Director, Washington Legislative Office
American Civil Liberties Union

NSA Data Collection and Surveillance Oversight

July 17, 2013

QUESTION FROM REP. STEVE COHEN

Are there ways to enhance the role of the Privacy and Civil Liberties Oversight Board so as to ensure a better balance between legitimate national security needs on the one hand and privacy, civil liberties, and public transparency on the other?

Congress should enhance the PCLOB in at least four ways in order to ensure that the Board plays a meaningful role in overseeing the impact of government policies on privacy, civil liberties, and public transparency. First, Congress should grant the Board the authority to challenge the classification decisions of other agencies when it finds reason to believe classification powers have been abused to cover up wrongdoing, to prevent embarrassment, or to stifle legitimate public debate. Second, the Board should enjoy a set of enforcement powers that could be used to implement its recommendations. Third, Congress must ensure that the Board is given sufficient resources—in terms of both staff and budget—to pursue its mandate on an ongoing basis. And finally, assuming all three prior enhancements have been achieved, Congress should consider broadening the Board's mandate so that its oversight authority ranges to other areas of policymaking such as certain law enforcement programs that raise serious privacy and civil-liberties issues. In broadening the mandate, however, it is critically important not to dilute the time, attention and resources devoted to counterterrorism programs.

Response to Questions from the Hearing and for the Record from Kate Martin, Center for National Security Studies

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

Answers from Kate Martin to Members' questions from the hearing on July 17, 2013 and for the record.

Representative Goodlatte (p. 122):

"Let me turn to Ms. Martin, however, and your testimony includes a number of suggestions for increasing the visibility into the – increasing visibility into the FISA programs. Which of these would you prioritize as a way to both preserve our national security efforts while also giving the public a better understanding of how the programs work?

Since the hearing, the government has disclosed additional opinions by the FISC court and a White Paper concerning the 215 program, which disclosures are welcome and useful. Nevertheless, we still do not have a complete understanding of the FISA court's views on the law, nor of the executive's interpretation of the law. Accordingly, I would prioritize obtaining disclosure of the following information:

1. All FISA court opinions concerning the law, including those authorizing bulk collection of internet meta-data, and the government's pleadings containing legal arguments submitted to the court. Any operational details which are still a secret could be redacted from these documents.
2. In light of the government's disclosure of the 215 program, there should be a new declassification review and public release of the Inspectors Generals' report required by the FISA Amendments Act (Report on the President's Surveillance Program, Offices of the Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, July 10, 2009. Unclassified version available at http://www.justice.gov/oig/special/s0907.pdf). This report is crucial for understanding the legal history and scope of the current surveillance programs.
3. Equally important, this Committee should demand a *comprehensive public report* from the Executive Branch concerning government collection of information about Americans for national security or foreign intelligence purposes. The report should detail:
    - the overlapping authorities for collection of information about Americans' communications, e.g., national security letter authorities, pen register/trap and trace authorities, other FISA authorities;
    - the rules governing accessing, analyzing, data-mining, keeping, using or disseminating information concerning Americans' communications;

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 cnss@cnss.org

- in addition to existing authorities, the report should identify existing prohibitions, if any, on collecting or data-mining information on Americans, and all restrictions, if any, on sharing information with the White House, including the National Security Council, or foreign governments;
- which agencies may exercise which authorities and what information may be may be shared between each agency; and
- the scope of the collection of Americans' personal information, including the kinds of information, the amount of information collected and the approximate number of Americans whose information has been collected.

Representative Gohmert (p. 125-126):

"I have now seen the incredible abuse by the FISA court, in my opinion, and I am just wondering if we are better off going to a system where we don't require a FISA court. There is not this Star Chamber. What would be another alternative?"

. . .

"But I would ask the witnesses if you have any proposals, if you could provide that in writing to us, any alternatives, any major changes, because I think this justifies major changes."

Since its creation, the FISA court has issued particularized orders based on a finding of probable cause and those authorities do not raise the concerns you have articulated. I would urge the Congress, however, to examine carefully whether the new authorities, in particular the FISA Amendments Act, section 702 of the FISA, which do not require any particularity in collection activities, but are specifically intended to collect information on Americans, (even though they may not be technically "targeted") should be limited or repealed. Doing so would address some of the more problematic authorities of the FISA court. *As a first step, Congress should shorten the current sunset for those authorities from the current date of 2017 to align with the current mid 2015 sunset date for section 215.* In addition, Congress should amend section 215 to make clear that it does not authorize bulk collection of information on Americans.

There have been some proposals to provide for an "independent" advocate to participate in the secret proceedings before the FISA court. Such an advocate might prove helpful to the judges on the court, who do not have the benefit of briefing by two parties. (FISA court judges could perhaps be consulted on how helpful such a position would be.) But providing such an advocate would be no substitute for reinstating *public adversarial* judicial review. The essence of judicial review of the legality of the government's action is that such review is transparent, a court acts openly, and that the individual whose rights are at stake participates in the proceeding. The current proposals would not address either of these key requirements—transparency or adversarialness -- for restoring real judicial review.

Accordingly, this Committee should examine other ways to provide adversarial judicial review of individual instances of foreign intelligence surveillance. Such judicial review could like judicial review of searches and seizure done for law enforcement purposes, take place after the fact, when the surveillance is finished. While the original FISA contained a provision for such review, 50 U.S.C. 1806, that provision does not apply to all current collection authorities under FISA. Moreover, it has not proved sufficient to provide a real opportunity for a subject of surveillance to challenge the surveillance in an open and adversarial proceeding before a judge.

Representative Nadler (p. 127):

"Ms. Martin, how can we—how can Congress solve the problem? We have a basic problem. Every challenge to abuse of constitutional rights by the Bush administration and the Obama administration has been met in the same way. Either the use of the state secrets doctrine to say you can't go to a court on that. The subject matter of the discussion is a state secret. Therefore, move to dismiss the case ab initio. Or you have no standing because you cannot prove that you personally were harmed by this.

Now Mr. Snowden may have done a public service in giving some people standing by proving that they were harmed by this because anyone who is a Verizon subscriber arguable can no go into court and say that. How can we deal with these two problems that an administration, any administration can violate constitutional rights from here to kingdom come, subject to no court review because of either the state secrets doctrine or the standing problems because they don't admit what they are doing in the first place. It is secret.

It is secret what we are doing to you. Therefore, you have no standing because you can't prove what we are doing to you."

There are several steps the Congress could take to ameliorate the problem that individuals cannot challenge the government's actions against them in court, when the government refuses to acknowledge its activities and claims that the state secrets privilege or other doctrine prevents litigation.

First, the Congress should insist on public disclosure of information concerning the government's activities. In addition to public disclosure concerning the legal authorities and scope of surveillance programs generally, Congress should also require investigation of specific instances of surveillance, where there are credible allegations that individual rights have been violated, either by congressional committees, an inspector general or other body. That investigation could then inform additional public disclosures concerning questionable instances of government surveillance. And those disclosures in turn would facilitate judicial challenges by the affected individuals. In particular, the government would not be able to seek dismissal of such challenges on state secrets grounds, because the information relevant to pursuing the case would be public.

In addition, I would urge the Congress to examine the possibility of creating a statutory cause of action for violation of an individual's constitutional rights. Doing so would make it more difficult for the government to secure dismissal of a challenge on technical grounds, and help insure that the court considers the merits of whether the government has violated someone's rights.

Representative Cohen:

"Are there ways to enhance the role of the Privacy and Civil Liberties Oversight Board so as to ensure a better balance between legitimate national security needs on the one hand and privacy, civil liberties and public transparency on the other?"

Congress should ensure that the Privacy and Civil Liberties Oversight Board receives adequate funding to enable it to carry out its statutory mandate. At the same time, the Congress and the federal courts have the ultimate constitutional responsibility for ensuring privacy, civil liberties and public transparency while protecting the national security.

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

The Honorable Bob Goodlatte
Chair
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Goodlatte,

Thank you for the opportunity to testify before the Committee at its hearing on oversight of the Administration's Use of FISA Authorities, Wednesday, July 17, 2013. Enclosed please find written answers to the Members' questions asked during the hearing and for the record.

Sincerely,

Kate Martin
Director

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 cnss@cnss.org

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

Answers from Kate Martin to Members' questions from the hearing on July 17, 2013 and for the record.

Representative Goodlatte (p. 178-179):

"Let me turn to Ms. Martin, however, and your testimony includes a number of suggestions for increasing the visibility into the – increasing visibility into the FISA programs. Which of these would you prioritize as a way to both preserve our national security efforts while also giving the public a better understanding of how the programs work?

Since the hearing, the government has disclosed additional opinions by the FISC court and a White Paper concerning the 215 program, which disclosures are welcome and useful. Nevertheless, we still do not have a complete understanding of the FISA court's views on the law, nor of the executive's interpretation of the law. Accordingly, I would prioritize obtaining disclosure of the following information:

1. All FISA court opinions concerning the law, including those authorizing bulk collection of internet meta-data, and the government's pleadings containing legal arguments submitted to the court. Any operational details which are still a secret could be redacted from these documents.
2. In light of the government's disclosure of the 215 program, there should be a new declassification review and public release of the Inspectors Generals' report required by the FISA Amendments Act (Report on the President's Surveillance Program, Offices of the Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, July 10, 2009. Unclassified version available at http://www.justice.gov/oig/special/s0907.pdf). This report is crucial for understanding the legal history and scope of the current surveillance programs.
3. Equally important, this Committee should demand a *comprehensive public report* from the Executive Branch concerning government collection of information about Americans for national security or foreign intelligence purposes. The report should detail:

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 cnss@cnss.org

- the overlapping authorities for collection of information about Americans' communications, e.g., national security letter authorities, pen register/trap and trace authorities, other FISA authorities;
- the rules governing accessing, analyzing, data-mining, keeping, using or disseminating information concerning Americans' communications;
- in addition to existing authorities, the report should identify existing prohibitions, if any, on collecting or data-mining information on Americans, and all restrictions, if any, on sharing information with the White House, including the National Security Council, or foreign governments;
- which agencies may exercise which authorities and what information may be may be shared between each agency; and
- the scope of the collection of Americans' personal information, including the kinds of information, the amount of information collected and the approximate number of Americans whose information has been collected.

Representative Gohmert (p. 186 -87):

"I have now seen the incredible abuse by the FISA court, in my opinion, and I am just wondering if we are better off going to a system where we don't require a FISA court. There is not this Star Chamber. What would be another alternative?"

. . .

"But I would ask the witnesses if you have any proposals, if you could provide that in writing to us, any alternatives, any major changes, because I think this justifies major changes."

Since its creation, the FISA court has issued particularized orders based on a finding of probable cause and those authorities do not raise the concerns you have articulated. I would urge the Congress, however, to examine carefully whether the new authorities, in particular the FISA Amendments Act, section 702 of the FISA, which do not require any particularity in collection activities, but are specifically intended to collect information on Americans, (even though they may not be technically "targeted") should be limited or repealed. Doing so would address some of the more problematic authorities of the FISA court. *As a first step, Congress should shorten the current sunset for those authorities from the current date of 2017 to align with the current mid 2015 sunset date for section 215.* In addition, Congress should amend section 215 to make clear that it does not authorize bulk collection of information on Americans.

There have been some proposals to provide for an "independent" advocate to participate in the secret proceedings before the FISA court. Such an advocate might prove helpful to the judges on the court, who do not have the benefit of briefing by two parties. (FISA court judges could perhaps be consulted on how helpful such a position would be.) But providing such an advocate would be no substitute for reinstating *public adversarial* judicial review. The essence of judicial review of the legality of the government's action is that such review is transparent, a

court acts openly, and that the individual whose rights are at stake participates in the proceeding. The current proposals would not address either of these key requirements—transparency or adversarialness -- for restoring real judicial review.

Accordingly, this Committee should examine other ways to provide adversarial judicial review of individual instances of foreign intelligence surveillance. Such judicial review could like judicial review of searches and seizure done for law enforcement purposes, take place after the fact, when the surveillance is finished. While the original FISA contained a provision for such review, 50 U.S.C. 1806, that provision does not apply to all current collection authorities under FISA. Moreover, it has not proved sufficient to provide a real opportunity for a subject of surveillance to challenge the surveillance in an open and adversarial proceeding before a judge.

Representative Nadler (p. 191-192):

"Ms. Martin, how can we—how can Congress solve the problem? We have a basic problem. Every challenge to abuse of constitutional rights by the Bush administration and the Obama administration has been met in the same way. Either the use of the state secrets doctrine to say you can't go to a court on that. The subject matter of the discussion is a state secret. Therefore, move to dismiss the case ab initio. Or you have no standing because you cannot prove that you personally were harmed by this.

Now Mr. Snowden may have done a public service in giving some people standing by proving that they were harmed by this because anyone who is a Verizon subscriber arguable can no go into court and say that. How can we deal with these two problems that an administration, any administration can violate constitutional rights from here to kingdom come, subject to no court review because of either the state secrets doctrine or the standing problems because they don't admit what they are doing in the first place. It is secret.

It is secret what we are doing to you. Therefore, you have no standing because you can't prove what we are doing to you."

There are several steps the Congress could take to ameliorate the problem that individuals cannot challenge the government's actions against them in court, when the government refuses to acknowledge its activities and claims that the state secrets privilege or other doctrine prevents litigation.

First, the Congress should insist on public disclosure of information concerning the government's activities. In addition to public disclosure concerning the legal authorities and scope of surveillance programs generally, Congress should also require investigation of specific instances of surveillance, where there are credible allegations that individual rights have been violated, either by congressional committees, an inspector general or other body. That investigation could then inform additional public disclosures concerning questionable instances of government surveillance. And those disclosures in turn would facilitate judicial challenges by

the affected individuals. In particular, the government would not be able to seek dismissal of such challenges on state secrets grounds, because the information relevant to pursuing the case would be public.

In addition, I would urge the Congress to examine the possibility of creating a statutory cause of action for violation of an individual's constitutional rights. Doing so would make it more difficult for the government to secure dismissal of a challenge on technical grounds, and help insure that the court considers the merits of whether the government has violated someone's rights.

Representative Cohen:

"Are there ways to enhance the role of the Privacy and Civil Liberties Oversight Board so as to ensure a better balance between legitimate national security needs on the one hand and privacy, civil liberties and public transparency on the other?"

Congress should ensure that the Privacy and Civil Liberties Oversight Board receives adequate funding to enable it to carry out its statutory mandate. At the same time, the Congress and the federal courts have the ultimate constitutional responsibility for ensuring privacy, civil liberties and public transparency while protecting the national security.

○