

EXAMINING RECOMMENDATIONS TO REFORM FISA AUTHORITIES

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES ONE HUNDRED THIRTEENTH CONGRESS SECOND SESSION

FEBRUARY 4, 2014

Serial No. 113-62

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

86-549 PDF

WASHINGTON : 2014

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	JOHN CONYERS, JR., Michigan
HOWARD COBLE, North Carolina	JERROLD NADLER, New York
LAMAR SMITH, Texas	ROBERT C. "BOBBY" SCOTT, Virginia
STEVE CHABOT, Ohio	ZOE LOFGREN, California
SPENCER BACHUS, Alabama	SHEILA JACKSON LEE, Texas
DARRELL E. ISSA, California	STEVE COHEN, Tennessee
J. RANDY FORBES, Virginia	HENRY C. "HANK" JOHNSON, JR., Georgia
STEVE KING, Iowa	PEDRO R. PIERLUISI, Puerto Rico
TRENT FRANKS, Arizona	JUDY CHU, California
LOUIE GOHMERT, Texas	TED DEUTCH, Florida
JIM JORDAN, Ohio	LUIS V. GUTIERREZ, Illinois
TED POE, Texas	KAREN BASS, California
JASON CHAFFETZ, Utah	CEDRIC RICHMOND, Louisiana
TOM MARINO, Pennsylvania	SUZAN DELBENE, Washington
TREY GOWDY, South Carolina	JOE GARCIA, Florida
RAÚL LABRADOR, Idaho	HAKEEM JEFFRIES, New York
BLAKE FARENTHOLD, Texas	DAVID N. CICILLINE, Rhode Island
GEORGE HOLDING, North Carolina	
DOUG COLLINS, Georgia	
RON DeSANTIS, Florida	
JASON T. SMITH, Missouri	
[Vacant]	

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

CONTENTS

FEBRUARY 4, 2014

Page

OPENING STATEMENTS

The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary	1
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary	4

WITNESSES

The Honorable James Cole, United States Department of Justice	
Oral Testimony	7
Prepared Statement	10
Peter P. Swire, Review Group on Intelligence and Communications Technology	
Oral Testimony	17
Prepared Statement	19
David Medine, Privacy and Civil Liberties Oversight Board	
Oral Testimony	49
Prepared Statement	51
Steven G. Bradbury, Dechert, LLP	
Oral Testimony	121
Prepared Statement	124
David Cole, Georgetown University Law Center	
Oral Testimony	145
Prepared Statement	147
Dean C. Garfield, Information Technology Industry Council	
Oral Testimony	158
Prepared Statement	160

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Material submitted by the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary	184
--	-----

OFFICIAL HEARING RECORD

MATERIAL SUBMITTED FOR THE HEARING RECORD BUT NOT REPRINTED

Report from the Privacy and Civil Liberties Oversight Board, January 23, 2014, submitted by the Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Member, Committee on the Judiciary. This report is available at the Committee and can also be accessed at:

<http://www.pcllob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf>

EXAMINING RECOMMENDATIONS TO REFORM FISA AUTHORITIES

TUESDAY, FEBRUARY 4, 2014

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to call, at 10:14 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, Issa, Forbes, King, Franks, Gohmert, Jordan, Poe, Chaffetz, Gowdy, Labrador, Farenthold, Holding, Collins, DeSantis, Smith of Missouri, Conyers, Nadler, Scott, Lofgren, Jackson Lee, Cohen, Johnson, Chu, Deutch, DelBene, Garcia, Jeffries, and Cicilline.

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

Before we begin today's hearing, I would like to take a moment to welcome the newest Member of the House Judiciary Committee, David Cicilline of Rhode Island's First Congressional District.

Born in Providence, Congressman Cicilline moved to Washington, D.C., shortly after law school to work as a public defender before returning to Rhode Island. In 1994, he was elected to the Rhode Island State legislature and ultimately elected Mayor of Providence in 2002 and again in 2006.

He was elected to the U.S. House of Representatives in 2010 and is also a Member of the House Committee on Foreign Affairs. And we welcome you to the Judiciary Committee. [Applause.]

Mr. CONYERS. Mr. Chairman?

Mr. GOODLATTE. And I would like to recognize the Ranking Member for any comments that he would like to make.

Mr. CONYERS. Thank you.

On behalf of all of us on this side of the aisle, we join Chairman Goodlatte in welcoming our newest Member to the Committee,

Congressman David Cicilline, First District, Rhode Island. A Mayor, a public defender, practiced law in Rhode Island, and I am confident that his depth of experience will be a great asset to this Committee.

Mr. Cicilline, we welcome you and look forward to working with you. [Applause.]

Thank you.

Mr. GOODLATTE. And we welcome everyone to this afternoon's hearing on Examining Recommendations to Reform FISA Authorities, and I will begin by recognizing myself for an opening statement.

Today's hearing will examine the various recommendations to reform programs operated under the Foreign Intelligence Surveillance Act, or FISA. Last summer's unauthorized public release of these classified programs has sparked a national debate about the extent of these programs and whether they pose a threat to Americans' civil liberties and privacy.

There have been myriad proposals to reform or end these programs. We are here today to vet these proposals and discuss their impact on America's national security and their value in enhancing civil liberty protections.

Following last year's leaks, Obama administration officials appeared before this and other Committees in Congress to defend these programs and urge Congress not to shut them down, including the bulk metadata collection program operated under Section 215 of the PATRIOT Act. But just 2 weeks ago, President Obama announced that he supports "a transition that will end Section 215 bulk metadata program as it currently exists and establish a mechanism that preserves the capabilities we need without the Government holding this bulk metadata."

I am glad the President has finally acknowledged what I and many others concluded long ago, namely that the Section 215 bulk metadata program is in need of significant reform in order to restore the trust of the American people and to protect Americans' civil liberties. But I am disappointed that the President was unable or unwilling to clearly articulate to Congress and the American people the value of this information in thwarting terror plots.

Instead, he simply declared that it is "important that the capability that this program is designed to meet is preserved," while simultaneously announcing that he was ending the program as it currently exists.

The 5-year storage of bulk metadata by the NSA is arguably the most critical and the most controversial aspect of the Section 215 program. But transferring storage to private companies could raise more privacy concerns than it solves.

We need to look no further than last month's Target breach or last week's Yahoo breach to know that private information held by private companies is susceptible to cyber attacks. And transferring storage to private companies would require the Government to request data from multiple companies to connect the dots it currently stores, thereby complicating its ability to quickly and efficiently compile valuable intelligence.

Of equal importance is the impact such a storage mandate would have on the ability of American companies to compete in a global

market. American technology companies are experiencing a lack of customer trust and a loss of international business as a result of the Snowden leaks, based upon the fear that information about their customers is readily and routinely turned over to the American Government.

I suspect requiring these companies to now house the data specifically so the Government can access it will only reinforce those fears. American companies, in fact, have sought permission to publicly report national security requests from the Government to inform and, hopefully, assuage the concerns of their American and foreign customers.

To that end, I am pleased the Justice Department worked jointly with American companies to identify information that can be publicly reported about the size and scope of national security requests. This is one step that will help provide greater transparency to the American people about the nature of our intelligence gathering programs.

On January 17th, President Obama also announced his desire to transfer the query approval of metadata from the NSA to the FISA court. I am interested to hear from today's witnesses whether such a reform will, in fact, result in greater privacy protections without weakening national security.

President Obama also endorsed additional privacy protections for foreigners overseas. He instructed the Attorney General and Director of National Intelligence to take the unprecedented step of extending certain protections that we have for the American people to people overseas. Specifically, President Obama called for limiting the duration that personal information about foreign nationals is stored while also restricting the use of this information. Is it wise to restrain our national security agencies by extending to foreigners the rights and privileges afforded Americans?

In addition to President Obama's proposed reforms, two panels, the President's Review Group on Intelligence and Communications Technology and the Privacy and Civil Liberties Oversight Board, have issued reports with their own proposals and conflicting legal analysis. On December 12th, the review group issued its report.

While the review group questioned the value of the bulk collection of telephone metadata by the Government, the review group did conclude that the program is constitutional, legal, and has not been abused and recommended the program continue with third-party or company storage.

A majority of the PCLOB, however, issued a report on January 23 that questioned whether the program is constitutional and concluded operated illegally under the statute since 2006. And recommended the metadata program end entirely.

I look forward to a discussion today of the constitutional and statutory analysis and recommendations of these two panels. The House Judiciary Committee has primary jurisdiction over the legal framework of these programs and has conducted aggressive oversight on this issue.

Any reforms Congress enacts must ensure our Nation's intelligence collection programs effectively protect our national security and include real protections for Americans' civil liberties, robust oversight, and additional transparency.

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

Mr. CONYERS. Thank you.

I welcome the witnesses today, the Deputy Attorney General in the first panel, and the witnesses coming up in the second panel.

Now the 9/11 Commission, observing that Congress had “vested substantial new powers in the investigative agencies of the Government” with the passage of the PATRIOT Act, argued that it would be healthy for the country to engage in full and informed debate on these new authorities.

The commission concluded that when that debate eventually takes place, the burden of proof for retaining a particular Government power should be on the executive to explain that the power actually and materially enhances security. Today, we are now engaged in that debate.

For the first time, the public understands that our Government is engaged in widespread domestic surveillance. This surveillance includes, but isn’t limited to, the Government’s collection of records on virtually every phone call placed in the United States under Section 215 of the PATRIOT Act.

Consensus is growing that this telephone metadata program is largely ineffective, inconsistent with our national values, and inconsistent with the statute as this Committee wrote it. As the 9/11 Commission proposed, the burden rests with the Government to convince us otherwise.

Reasonable people can disagree with me about whether or not the Government has met that burden, but there are several points to guide us in this debate that I believe are incontrovertible. First, the status quo is unacceptable. President Obama, his own Review Group on Intelligence and Communication Technology, and the Privacy and Civil Liberties Oversight Board all agree that the telephone metadata program, as currently exists, must end.

The review group had full access to the leadership of the intelligence community. It concluded that there has been no instance in which the National Security Agency could say with confidence that the outcome of a case would have been different without the Section 215 metadata program.

The Privacy and Civil Liberties Oversight Board came to the same conclusion and also observed that the operation of the bulk telephone record program bears almost no resemblance to the actual text of the statute.

In his remarks at the Department of Justice, President Obama observed that because expanding technological capabilities place fewer and fewer technical restraints on what we can do, we have a special obligation to ask tough questions about what we should do. The President ordered immediate changes to the telephone metadata program and asked the Attorney General and the Director of National Security to develop options for a new approach that takes these records out of Government hands.

I commend President Obama for his willingness to make these necessary changes. It cannot be easy for a sitting President to restrain his own intelligence capabilities, even if it is the right thing to do. After all, in the President’s own words, there is an inevitable

bias within the intelligence community to collect more information about the world, not less.

My second point is that the Administration cannot solve this problem without Congress. The House Judiciary Committee must act. We are the primary Committee of jurisdiction in the House for the Foreign Intelligence Surveillance Act, the exclusive means by which the Government may conduct domestic surveillance.

We are the proper forum for a debate about constitutional rights and civil liberties. More acutely, the Government is dependent on this Committee to renew the legal authorities now under review.

Section 215 is scheduled to sunset on June 1, 2015. If it expires, all Section 215 programs, not merely bulk collection, expire with it. We should address bulk collection today, or we risk losing all of Section 215 this time next year. Unless this Committee acts and acts soon, I fear we will lose valuable counterterrorism tools, along with the surveillance programs many of us find objectionable.

And finally, as this Committee moves forward, H.R. 3361, the USA FREEDOM Act, represents a reasonable consensus view and remains the right vehicle for reform. I am struck by the growing partisan—bipartisan consensus here. More and more of us seem to agree that the Congress should end bulk collection under Section 215 but allow the FBI's continued use of normal business records orders on a case-by-case basis.

We should retain the basic structure of Section 702 of the Foreign Intelligence Surveillance Act but enact additional protections for United States persons whose communications are intercepted without a warrant. We should create an opportunity for an independent advocate to represent privacy and civil liberties interests before the FISA court.

And in the service of meaningful public debate, we should declassify significant opinions of the FISA court, enhance reporting to the Congress, and allow companies to disclose more about their cooperation with the Government.

These reforms are consistent with the President's remarks, the recommendations of the review group, and the report of the Privacy and Civil Liberties Oversight Board. They are also, point for point, the main objectives of the measure called the USA FREEDOM Act.

Our colleague and former Chairman of this Committee, Mr. Sensenbrenner, is credited as the original author of the PATRIOT Act, is our lead on this bill in the House. Senator Leahy has introduced an identical measure in the Senate.

The USA FREEDOM Act enjoys the support of 130 Members in the House, evenly divided between Democrats and Republicans. More than half of this Committee now supports the bill, and our numbers grow every week.

And so, Mr. Chairman, I urge that you bring this bill up for consideration before the House Judiciary Committee as soon as possible because our mandate is clear. We have heard from the President, from his panel of experts, and from an independent oversight board. We will examine their proposals today, but the time for reform is now.

And so, at the risk of making too much reference to the attacks of September 11, 2001, I close my remarks with another passage from the 9/11 Commission report.

"We must find ways of reconciling security with liberty since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home.

"Our history has shown that insecurity threatens liberty. Yet if our liberties are curtailed, we lose the values that we are struggling to defend."

I thank you and yield back my time.

Mr. GOODLATTE. Thank you, Mr. Conyers.

And without objection, all other Members' opening statements will be made a part of the record.

It is now our pleasure to welcome our first panel today, and if the members of the panel would rise, I will begin by swearing in the witnesses.

[Witnesses sworn.]

Mr. GOODLATTE. Let the record reflect that all of the witnesses responded in the affirmative.

Thank you, and I will begin by introducing 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 J.D. from the University of California at Hastings.

Our second witness is Mr. Peter Swire, a member of the Review Group on Intelligence and Communications Technologies. The review group's mission is to review and provide recommendations on how, in light of advancements in communications technologies, the United States can employ its technical collection capabilities in a manner that optimally protects national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure.

Mr. Swire is also a senior fellow at the Future of Privacy Forum and the Center for American Progress, and policy fellow at the Center for Democracy and Technology. Mr. Swire is a professor at the Scheller College of Business at Georgia Tech, having previously served as a C. William O'Neill Professor of Law at the Ohio State University.

Mr. Swire worked for the Clinton administration as chief counselor for privacy in the U.S. Office of Management and Budget, where he held Government-wide responsibility for privacy policy. In 2009 and 2010, Mr. Swire served as Special Assistant to President Obama for Economic Policy, serving in the National Economic Council with Lawrence Summers. Mr. Swire earned his undergraduate degree from Princeton and his juris doctor from Yale Law School.

Our third witness is Mr. David Medine, the chairman of the Privacy and Civil Liberties Oversight Board. Mr. Medine started full time as chairman on May 27, 2013. Prior to serving as chairman, he was an attorney fellow for the Securities and Exchange Commission and a special counsel at the Consumer Financial Protection Bureau.

From 2002 to 2012, he was a partner in the law firm Wilmer Hale, having previously served as a senior adviser to the White House National Economic Council from 2000 to 2001. From 1992 to 2000, Mr. Medine was the Associate Director for Financial Practices at the Federal Trade Commission. Before joining the FTC, he taught at Indiana University School of Law and the George Washington University School of Law.

Mr. Medine received his bachelor's degree from Hampshire College and his juris doctor from the University of Chicago Law School.

I want to welcome all of you. I would ask each of you summarize your testimony in 5 minutes or less, 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 the witness' 5 minutes have expired.

And we will begin with Deputy Attorney General Cole. Welcome.

**TESTIMONY OF THE HONORABLE JAMES COLE,
UNITED STATES DEPARTMENT OF JUSTICE**

Mr. JAMES COLE. Thank you, Mr. Chairman, Ranking Member Conyers, and Members of the Committee, for inviting us here to continue the discussion of certain intelligence collection activities and our efforts to protect privacy and civil liberties at the same time.

We have all invested a considerable amount of energy over these past few months in reviewing specific intelligence collection programs and the legal framework under which they are conducted. I think it is fair to say that all of us—the members of the Privacy and Civil Liberties Oversight Board, the members of the Presidential review group, the Administration, and the Congress—want the same thing—to maintain our national security while upholding the liberties that we all cherish.

It is not always easy to agree on how best to accomplish these objectives, but we will continue to work in earnest to advance our common interests, and we appreciate the good faith in which everyone has engaged in this endeavor.

We have benefited from the consideration of these difficult issues by the PCLOB and the PRG, and it's a pleasure to appear with them today. In his speech on January 17th, the President laid out a series of measures to reform our surveillance activities that draw upon many of the core recommendations issued by the PCLOB and the PRG.

The work to develop or carry out these measures is well underway, and I would like to highlight just a few of the most significant initiatives announced by the President that the Department of Justice is working to implement in close coordination with the intelligence community.

First, we are examining alternatives to the collection of bulk telephony metadata under Section 215, which, as you noted, the President has said will end as it currently exists. The President has said that the capability that this program was designed to provide is important and must be preserved, but we must find a new approach that does not require the Government to hold this bulk metadata.

The Section 215 program, as currently constituted, is subject to an extensive framework of laws and judicial orders and to oversight by all three branches of Government, designed to prevent abuse. Neither the PCLOB nor the PRG has questioned the rigor of that oversight system, nor has anyone identified any intentional misuse of the telephony metadata.

Nevertheless, we recognize that any time large amounts of data are collected, whether by the Government or private companies, there is a potential for misuse, and it will be important that the new approach remains subject to a rigorous oversight regime. Insofar as the legality of the program is concerned, it is important to remember that the courts, the final arbiters of the law, have repeatedly found the program lawful, including 15 separate judges of the Foreign Intelligence Surveillance Court and two District Courts. There has been only one contrary District Court ruling, which is now on appeal.

The PCLOB undertook its own analysis of the legality, but the members were unable to agree on whether it was authorized under the statute. Although we continue to believe the program is lawful, we recognize that it has raised significant controversy and legitimate privacy concerns. And as I have said, we are working to develop a new approach, as the President has directed.

Second, we are working to develop additional restrictions on Government's ability to retain, search, and use in criminal cases U.S. person information incidentally collected when we target non-U.S. persons overseas under Section 702 of FISA.

Third, the President recognized that our global leadership position requires us to take steps to maintain the trust and cooperation of people not only here at home, but around the world. Accordingly, he has also determined that as a matter of policy, certain privacy safeguards afforded for signals intelligence containing U.S. person information will be extended to non-U.S. persons where consistent with national security. We will be working with our colleagues in the intelligence community to implement that policy directive.

Fourth, the department is working to change how we use national security letters so that the nondisclosure requirements authorized by statute will terminate within a fixed time unless the Government demonstrates a need for further secrecy. Although these nondisclosure obligations are important in preserving the viability of national security investigations, these reforms will ensure that secrecy extends no longer than necessary.

Fifth, the President called upon Congress to authorize the establishment of a panel of advocates from outside the Government to provide an independent voice in significant cases before the FISC. We believe the ex parte process has functioned well. The court, however, should be able to hear independent views in certain FISA matters that present significant or novel questions. We will provide

our assistance to Congress as it considers legislation on this subject.

Sixth, we have already taken steps to promote greater transparency about the number of national security orders issued to technology companies, the number of customer accounts targeted under those orders, and the legal authorities behind those requests. As a result of the procedures that we have adopted in this regard, technology companies have withdrawn their lawsuit concerning this issue.

Through these new reporting methods, technology companies will be permitted to disclose more information to their customers than ever before. We look forward to consulting with Congress as we work to implement the reforms outlined by the President and as you consider various legislative proposals to address these issues.

I'll be happy to take any questions you may have.

[The prepared statement of Mr. James Cole follows:]

**Opening Statement of
Deputy Attorney General James Cole
Before the House Judiciary Committee
February 4, 2014, 10:00 A.M.**

Thank you, Mr. Chairman, Ranking Member Conyers, and Members of the Committee, for inviting us here to continue the discussion of certain intelligence collection activities and our efforts to protect privacy and civil liberties. We have all invested a considerable amount of energy over these past few months in reviewing specific intelligence collection programs and the legal framework under which they are conducted. I think it's fair to say that all of us—the members of the Privacy and Civil Liberties Oversight Board (PCLOB), the members of the Presidential Review Group (PRG), the Administration, and the Congress—want the same thing: to maintain our national security while upholding the liberties that we all cherish. It is not always easy to agree on how best to accomplish these

objectives, but we will continue to work in earnest to advance our common interests, and we appreciate the good faith in which everyone has engaged in this endeavor.

We have benefited from the consideration of these difficult issues by the PCLOB and the PRG and it is a pleasure to appear with them today. In his speech on January 17th, the President laid out a series of measures to reform our surveillance activities that draw upon many of the core recommendations issued by the PCLOB and PRG. The work to develop or carry out these measures is well underway, and I would like to highlight just a few of the most significant initiatives announced by the President that the Department of Justice is working to implement in close coordination with the Intelligence Community (IC).

First, we are examining alternatives to the collection of bulk telephony metadata under Section 215, which the President

has said will end as it currently exists. The President has said that the capability that this program was designed to provide is important and must be preserved, but we must find a new approach that does not require the government to hold this bulk metadata. The Section 215 program as currently constituted is subject to an extensive framework of laws and judicial orders and to oversight by all three branches of government designed to prevent abuse. Neither the PCLOB nor the PRG has questioned the rigor of that oversight system. Nor has anyone identified any intentional misuse of the telephony metadata. Nevertheless, we recognize that any time large amounts of data are collected, whether by the government or private companies, there is a potential for misuse, and it will be important that the new approach remain subject to a rigorous oversight regime.

Insofar as the legality of the program is concerned, it is important to remember that the courts—the final arbiters of the

law—have repeatedly found the program lawful, including 15 separate judges of the Foreign Intelligence Surveillance Court (FISC) and two district courts. There has been only one contrary district court ruling which is now on appeal. The PCLOB undertook its own analysis of the legality, but its members were unable to agree on the whether it was authorized under the statute. Although we continue to believe the program is lawful, we recognize that it has raised significant controversy and legitimate privacy concerns, and as I have said we are working on developing a new approach as the President has directed.

Second, we are working to develop additional restrictions on the government's ability to retain, search, and use in criminal cases U.S. person information incidentally collected when we target non-U.S. persons overseas under Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Third, the President recognized that our global leadership position requires us to take steps to maintain the trust and cooperation of people not only here at home but around the world. Accordingly, he has also determined that, as a matter of policy, certain privacy safeguards afforded for signals intelligence containing U.S. person information will be extended to non-U.S. persons, where consistent with national security. We will be working with our colleagues in the IC to implement that policy directive.

Fourth, the Department is working to change how we use National Security Letters so that the nondisclosure requirements authorized by statute will terminate within a fixed time, unless the government demonstrates a need for further secrecy. Although these nondisclosure obligations are important in preserving the viability of national security investigations, these

reforms will ensure that secrecy extends no longer than necessary.

Fifth, the President called upon Congress to authorize the establishment of a panel of advocates from outside the government to provide an independent voice in significant cases before the FISC. While we believe the ex parte process has functioned well, the court should be able to hear independent views in certain FISA matters that present significant or novel questions. We will provide our assistance to Congress as it considers legislation on this subject.

Sixth, we have already taken steps to promote greater transparency about the number of national security orders issued to technology companies, the number of customer accounts targeted under those orders, and the legal authorities behind those requests. As a result of the procedures we have adopted in this regard, technology companies have withdrawn their lawsuit

concerning this issue. Through these new reporting methods, technology companies will be permitted to disclose more information to their customers than ever before.

We look forward to consulting with Congress as we work to implement the reforms outlined by the President and as you consider various legislative proposals to address these issues. I would be happy to take any questions that you may have.

Mr. GOODLATTE. Thank you.
Mr. Swire, welcome.

**TESTIMONY OF PETER P. SWIRE, REVIEW GROUP ON
INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY**

Mr. SWIRE. Thank you, Mr. Chairman and Ranking Member Conyers and Members of the Committee.

I appreciate the opportunity to testify today on behalf of the five members of the review group and the invitation and the request was rather than this being my personal statement, that it be reflecting the group's effort and our report that was issued in December.

The review group is a group of five people. I'll briefly describe them in the context of our work and how we came to our recommendations.

One of the members is Michael Morell, who had more than 30 years in the CIA as a professional intelligence officer, and he finished his time there as Deputy Director of the CIA. So we had the benefit in our group of somebody with many years of deep experience in the intelligence community.

Richard Clarke had been the senior cybersecurity and anti-terrorism adviser, both to President Clinton and President George W. Bush. So he came to this with both technological and Government experience in many different respects.

Cass Sunstein is, I think, the most cited law professor in the United States, a professor at Harvard right now, and he has spent 5 years as the Director of the Office of Information and Regulatory Affairs at OMB, with a detailed knowledge of the Government and how it operates.

And Geoffrey Stone is the former dean of the University of Chicago Law School, and he's an expert, among other things, on civil liberties in the time of war.

So I felt privileged to be working with these four distinguished gentlemen. My own background is primarily in the area of privacy, technology, and law, how these come together, and I'll mention two parts of the background that are relevant to today's hearing.

For one, when I worked under President Clinton, I was asked to chair an administration process to propose legislation on how to update wiretap laws for the Internet. And in the fall of 2000, this cleared administration proposal came before this Committee for a hearing where the Department of Justice testified, and some of the people here today asked questions of that. So how to do the law around wiretaps on the Internet is something we've been wrestling with for quite some time.

The second thing is that in 2004, I published an extensive article on the history and issues surrounding FISA, which touches on some of the issues we'll address today.

In terms of the review group, in August, the five of us were invited to come meet with the President and be named to the review group, and I'd like to just take a moment on the charter of our group. The charter was to try to bring together things that are hard to bring together.

How do we do national security? How do we maintain our foreign allies and relationships with other countries, including commercial

relationships? How do we preserve privacy and civil liberties in this new technological age? How do we maintain public trust? And finally, how do we address the insider threat, which we've seen can be a very—a big problem in terms of maintaining classified secrets?

So, within these national security, commercial, civil liberties and public trust things, how do we put this all together in a package? The—our job was to be—as tasked by the President, was to be forward looking. Where should we go from here? So I'd like to emphasize we did not do a constitutional analysis of any of the programs. That was not what we thought our job was.

We also did not do a specific statutory analysis of whether something was or was not lawful that was being done specifically around 215. Others have taken on those tasks. Our group did not do that constitutional or statutory analysis. We thought putting these five major goals together into a report was plenty for us to take on during the fall.

One of the things about our group is that we, in addition to being forward looking, were not limited to counterterrorism in our mission. And so, the PCLOB, as David Medine will talk about, has statutory authorities specifically focused on counterterrorism. We were asked to take on broader issues around foreign affairs, et cetera, that in some cases go beyond that scope.

We met during the fall each week. We got briefed extensively on a classified basis from the agencies. We had detailees from the agencies. Every question we asked for, we got answered. The agencies were outstanding in their cooperation.

We presented our preliminary findings orally to the President's top advisers during the fall and, on December 11th, transmitted our report to the White House. This was our report. It was submitted for declassification review to make sure we weren't releasing classified secrets, but the recommendations were the group of five, it was our own.

And as it turned out, after we did this work together, the civil liberties people in our group, the anti-terrorism, the CIA people in the group, all of us came to consensus. So every sentence of the report turned out to be agreed to by all five of us. As I testify and as I answer your questions today, my effort will be to accurately reflect the report that brought these disparate views together.

Our—we met with the President after the report was submitted. Our report was released in mid December, has been extensively discussed in the press and elsewhere, and the review group formally ceased to exist after the President's speech.

So I'm here as a private citizen, but doing my very best to reflect the views of the five people on the review group. So I look forward to taking questions from you all.

Thank you.

[The prepared statement of Mr. Swire follows:]

Testimony of Peter P. Swire

Review Group on Intelligence and
Communications Technology

Before the
HOUSE COMMITTEE ON THE JUDICIARY

Hearing on:
Examining Recommendations to Reform FISA Authorities
February 4, 2014

Executive Summary

Overview

The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future. These threats include international terrorism, the proliferation of weapons of mass destruction, and cyber espionage and warfare. A robust foreign intelligence collection capability is essential if we are to protect ourselves against such threats. Because our adversaries operate through the use of complex communications technologies, the National Security Agency, with its impressive capabilities and talented officers, is indispensable to keeping our country and our allies safe and secure.

At the same time, the United States is deeply committed to the protection of privacy and civil liberties—fundamental values that can be and at times have been eroded by excessive intelligence collection. After careful consideration, we recommend a number of changes to our intelligence collection activities that will protect these values without undermining what we need to do to keep our nation safe.

Principles

We suggest careful consideration of the following principles:

1. *The United States Government must protect, at once, two different forms of security: national security and personal privacy.*

In the American tradition, the word “security” has had multiple meanings. In contemporary parlance, it often refers to *national security* or *homeland security*. One of the government’s most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: “The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ” (emphasis added). Both forms of security must be protected.

2. The central task is one of risk management; multiple risks are involved, and all of them must be considered.

When public officials acquire foreign intelligence information, they seek to reduce risks, above all risks to national security. The challenge, of course, is that multiple risks are involved. Government must consider all of those risks, not a subset, when it is creating sensible safeguards. In addition to reducing risks to national security, public officials must consider four other risks:

- Risks to privacy;
- Risks to freedom and civil liberties, on the Internet and elsewhere;
- Risks to our relationships with other nations; and
- Risks to trade and commerce, including international commerce.

3. The idea of “balancing” has an important element of truth, but it is also inadequate and misleading.

It is tempting to suggest that the underlying goal is to achieve the right “balance” between the two forms of security. The suggestion has an important element of truth. But some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.

4. The government should base its decisions on a careful analysis of consequences, including both benefits and costs (to the extent feasible).

In many areas of public policy, officials are increasingly insistent on the need for careful analysis of the consequences of their decisions, and on the importance of relying not on intuitions and anecdotes, but on evidence and data. Before they are undertaken, surveillance decisions should depend (to the extent feasible) on a careful assessment of the anticipated consequences, including the full range of relevant risks. Such decisions should also be subject to continuing scrutiny, including retrospective analysis, to ensure that any errors are corrected.

Surveillance of US Persons

With respect to surveillance of US Persons, we recommend a series of significant reforms. Under section 215 of the Foreign Intelligence Surveillance Act (FISA), the government now stores bulk telephony meta-data, understood as information that includes the telephone numbers that both originate and receive calls, time of call, and date of call. (Meta-data does not include the content of calls.). We recommend that Congress should end such storage and transition to a system in which such meta-data is held privately for the government to query when necessary for national security purposes.

In our view, the current storage by the government of bulk meta-data creates potential risks to public trust, personal privacy, and civil liberty. We recognize that the government might need access to such meta-data, which should be held instead either by private providers or by a private third party. This approach would allow the government access to the relevant information when such access is justified, and thus protect national security without unnecessarily threatening privacy and liberty. Consistent with this recommendation, we endorse a broad principle for the future: as a general rule and without senior policy review, the government should not be permitted to collect and store mass, undigested, non-public personal information about US persons for the purpose of enabling future queries and data-mining for foreign intelligence purposes.

We also recommend specific reforms that will provide Americans with greater safeguards against intrusions into their personal domain. We

endorse new steps to protect American citizens engaged in communications with non-US persons. We recommend important restrictions on the ability of the Foreign Intelligence Surveillance Court (FISC) to compel third parties (such as telephone service providers) to disclose private information to the government. We endorse similar restrictions on the issuance of National Security Letters (by which the Federal Bureau of Investigation now compels individuals and organizations to turn over certain otherwise private records), recommending prior judicial review except in emergencies, where time is of the essence.

We recommend concrete steps to promote transparency and accountability, and thus to promote public trust, which is essential in this domain. Legislation should be enacted requiring information about surveillance programs to be made available to the Congress and to the American people to the greatest extent possible (subject only to the need to protect classified information). We also recommend that legislation should be enacted authorizing telephone, Internet, and other providers to disclose publicly general information about orders they receive directing them to provide information to the government. Such information might disclose the number of orders that providers have received, the broad categories of information produced, and the number of users whose information has been produced. In the same vein, we recommend that the government should publicly disclose, on a regular basis, general data about the orders it has issued in programs whose existence is unclassified.

Surveillance of Non-US Persons

Significant steps should be taken to protect the privacy of non-US persons. In particular, any programs that allow surveillance of such persons even outside the United States should satisfy six separate constraints. They:

- 1) must be authorized by duly enacted laws or properly authorized executive orders;
- 2) must be directed *exclusively* at protecting national security interests of the United States or our allies;
- 3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries;
- 4) must not target any non-United States person based solely on that person's political views or religious convictions;
- 5) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies; and
- 6) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

Setting Priorities and Avoiding Unjustified or Unnecessary Surveillance

To reduce the risk of unjustified, unnecessary, or excessive surveillance in foreign nations, including collection on foreign leaders, we recommend that the President should create a new process, requiring highest-level approval of all sensitive intelligence requirements and the methods that the Intelligence Community will use to meet them. This process should identify both the uses and the limits of surveillance on foreign leaders and in foreign nations.

We recommend that those involved in the process should consider whether (1) surveillance is motivated by especially important national security concerns or by concerns that are less pressing and (2) surveillance would involve leaders of nations with whom we share fundamental values and interests or leaders of other nations. With close reference to (2), we recommend that with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections).

Organizational Reform

We recommend a series of organizational changes. With respect to the National Security Agency (NSA), we believe that the Director should be a Senate-confirmed position, with civilians eligible to hold that position; the President should give serious consideration to making the next Director of NSA a civilian. NSA should be clearly designated as a foreign intelligence organization. Other missions (including that of NSA's Information Assurance Directorate) should generally be assigned elsewhere. The head of the military unit, US Cyber Command, and the Director of NSA should not be a single official.

We favor a newly chartered, strengthened, independent Civil Liberties and Privacy Protection Board (CLPP Board) to replace the Privacy and Civil Liberties Oversight Board (PCLOB). The CLPP Board should have broad authority to review government activity relating to foreign intelligence and counterterrorism whenever that activity has implications for civil liberties and privacy. A Special Assistant to the President for Privacy should also be designated, serving in both the Office of Management and Budget and the National Security Staff. This Special Assistant should chair a Chief Privacy Officer Council to help coordinate privacy policy throughout the Executive branch.

With respect to the FISC, we recommend that Congress should create the position of Public Interest Advocate to represent the interests of privacy and civil liberties before the FISC. We also recommend that the government should take steps to increase the transparency of the FISC's

decisions and that Congress should change the process by which judges are appointed to the FISC.

Global Communications Technology

Substantial steps should be taken to protect prosperity, security, and openness in a networked world. A free and open Internet is critical to both self-government and economic growth. The United States Government should reaffirm the 2011 International Strategy for Cyberspace. It should stress that Internet governance must not be limited to governments, but should include all appropriate stakeholders, including businesses, civil society, and technology specialists.

The US Government should take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage. Among other measures relevant to the Internet, the US Government should also support international norms or agreements to increase confidence in the security of online communications.

For big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties.

Protecting What We Do Collect

We recommend a series of steps to reduce the risks associated with “insider threats.” A governing principle is plain: Classified information should be shared only with those who genuinely need to know. We recommend specific changes to improve the efficacy of the personnel vetting system. The use of “for-profit” corporations to conduct personnel investigations should be reduced or terminated. Security clearance levels should be further differentiated. Departments and agencies should institute a Work-Related Access approach to the dissemination of sensitive, classified information. Employees with high-level security clearances should be subject to a Personnel Continuous Monitoring Program. Ongoing security clearance vetting of individuals should use a risk-management approach and depend on the sensitivity and quantity of the programs and information to which individuals are given access.

The security of information technology networks carrying classified information should be a matter of ongoing concern by Principals, who should conduct an annual assessment with the assistance of a “second opinion” team. Classified networks should increase the use of physical and logical separation of data to restrict access, including through Information Rights Management software. Cyber-security software standards and practices on classified networks should be at least as good as those on the most secure private-sector enterprises.

Recommendations

Recommendation 1

We recommend that section 215 should be amended to authorize the Foreign Intelligence Surveillance Court to issue a section 215 order compelling a third party to disclose otherwise private information about particular individuals only if:

- (1) it finds that the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 2

We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:

- (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 3

We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders.

Recommendation 4

We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.

Recommendation 5

We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intelligence Surveillance Court that meets the requirements set forth in Recommendation 1.

Recommendation 6

We recommend that the government should commission a study of the legal and policy options for assessing the distinction between meta-data and other types of information. The study should include

technological experts and persons with a diverse range of perspectives, including experts about the missions of intelligence and law enforcement agencies and about privacy and civil liberties.

Recommendation 7

We recommend that legislation should be enacted requiring that detailed information about authorities such as those involving National Security Letters, section 215 business records, section 702, pen register and trap-and-trace, and the section 215 bulk telephony meta-data program should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves.

Recommendation 8

We recommend that:

- (1) legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten

the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;

- (2) nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and
- (3) nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality.

Recommendation 9

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 10

We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National

Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 11

We recommend that the decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance. A program of this magnitude should be kept secret from the American people only if (a) the program serves a compelling governmental interest and (b) the efficacy of the program would be *substantially* impaired if our enemies were to know of its existence.

Recommendation 12

We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United States, and if the communication either includes a United States person as a participant or reveals information about a United States person:

- (1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;
- (2) any information about the United States person may not be used in evidence in any proceeding against that United States person;
- (3) the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism.

Recommendation 13

We recommend that, in implementing section 702, and any other authority that authorizes the surveillance of non-United States persons who are outside the United States, in addition to the safeguards and oversight mechanisms already in place, the US Government should reaffirm that such surveillance:

- (1) must be authorized by duly enacted laws or properly authorized executive orders;
- (2) must be directed *exclusively* at the national security of the United States or our allies;

- (3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries; and
- (4) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies.

In addition, the US Government should make clear that such surveillance:

- (1) must not target any non-United States person located outside of the United States based solely on that person's political views or religious convictions; and
- (2) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

Recommendation 14

We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

Recommendation 15

We recommend that the National Security Agency should have a limited statutory emergency authority to continue to track known targets of counterterrorism surveillance when they first enter the United States,

until the Foreign Intelligence Surveillance Court has time to issue an order authorizing continuing surveillance inside the United States.

Recommendation 16

We recommend that the President should create a new process requiring high-level approval of all sensitive intelligence requirements and the methods the Intelligence Community will use to meet them. This process should, among other things, identify both the uses and limits of surveillance on foreign leaders and in foreign nations. A small staff of policy and intelligence professionals should review intelligence collection for sensitive activities on an ongoing basis throughout the year and advise the National Security Council Deputies and Principals when they believe that an unscheduled review by them may be warranted.

Recommendation 17

We recommend that:

- (1) senior policymakers should review not only the requirements in Tier One and Tier Two of the National Intelligence Priorities Framework, but also any other requirements that they define as sensitive;
- (2) senior policymakers should review the methods and targets of collection on requirements in any Tier that they deem sensitive; and
- (3) senior policymakers from the federal agencies with responsibility for US economic interests should participate in

the review process because disclosures of classified information can have detrimental effects on US economic interests.

Recommendation 18

We recommend that the Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees.

Recommendation 19

We recommend that decisions to engage in surveillance of foreign leaders should consider the following criteria:

- (1) Is there a need to engage in such surveillance in order to assess significant threats to our national security?
- (2) Is the other nation one with whom we share values and interests, with whom we have a cooperative relationship, and whose leaders we should accord a high degree of respect and deference?
- (3) Is there a reason to believe that the foreign leader may be being duplicitous in dealing with senior US officials or is attempting to hide information relevant to national security concerns from the US?
- (4) Are there other collection means or collection targets that could reliably reveal the needed information?

- (5) What would be the negative effects if the leader became aware of the US collection, or if citizens of the relevant nation became so aware?

Recommendation 20

We recommend that the US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection.

Recommendation 21

We recommend that with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections). The criteria should include:

- (1) shared national security objectives;
- (2) a close, open, honest, and cooperative relationship between senior-level policy officials; and
- (3) a relationship between intelligence services characterized both by the sharing of intelligence information and analytic thinking and by operational cooperation against critical targets of joint national security concern. Discussions of such understandings or arrangements should be done between relevant intelligence communities, with senior policy-level oversight.

Recommendation 22

We recommend that:

- (1) the Director of the National Security Agency should be a Senate-confirmed position;
- (2) civilians should be eligible to hold that position; and
- (3) the President should give serious consideration to making the next Director of the National Security Agency a civilian.

Recommendation 23

We recommend that the National Security Agency should be clearly designated as a foreign intelligence organization; missions other than foreign intelligence collection should generally be reassigned elsewhere.

Recommendation 24

We recommend that the head of the military unit, US Cyber Command, and the Director of the National Security Agency should not be a single official.

Recommendation 25

We recommend that the Information Assurance Directorate—a large component of the National Security Agency that is not engaged in activities related to foreign intelligence—should become a separate agency within the Department of Defense, reporting to the cyber policy element within the Office of the Secretary of Defense.

Recommendation 26

We recommend the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget.

Recommendation 27

We recommend that:

- (1) The charter of the Privacy and Civil Liberties Oversight Board should be modified to create a new and strengthened agency, the Civil Liberties and Privacy Protection Board, that can oversee Intelligence Community activities for foreign intelligence purposes, rather than only for counterterrorism purposes;
- (2) The Civil Liberties and Privacy Protection Board should be an authorized recipient for whistle-blower complaints related to privacy and civil liberties concerns from employees in the Intelligence Community;
- (3) An Office of Technology Assessment should be created within the Civil Liberties and Privacy Protection Board to assess Intelligence Community technology initiatives and support privacy-enhancing technologies; and
- (4) Some compliance functions, similar to outside auditor functions in corporations, should be shifted from the National Security Agency and perhaps other intelligence agencies to the Civil Liberties and Privacy Protection Board.

Recommendation 28

We recommend that:

- (1) Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court;
- (2) the Foreign Intelligence Surveillance Court should have greater technological expertise available to the judges;
- (3) the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards; and
- (4) Congress should change the process by which judges are appointed to the Foreign Intelligence Surveillance Court, with the appointment power divided among the Supreme Court Justices.

Recommendation 29

We recommend that, regarding encryption, the US Government should:

- (1) fully support and not undermine efforts to create encryption standards;
- (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
- (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called “Zero Day” attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

Recommendation 31

We recommend that the United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications. Among those measures to be considered are:

- (1) Governments should not use surveillance to steal industry secrets to advantage their domestic industry;
- (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;

- (3) Governments should promote transparency about the number and type of law enforcement and other requests made to communications providers;
- (4) Absent a specific and compelling reason, governments should avoid localization requirements that (a) mandate location of servers and other information technology facilities or (b) prevent trans-border data flows.

Recommendation 32

We recommend that there be an Assistant Secretary of State to lead diplomacy of international information technology issues.

Recommendation 33

We recommend that as part of its diplomatic agenda on international information technology issues, the United States should advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments.

Recommendation 34

We recommend that the US Government should streamline the process for lawful international requests to obtain electronic communications through the Mutual Legal Assistance Treaty process.

Recommendation 35

We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are

statistically reliable, cost-effective, and protective of privacy and civil liberties.

Recommendation 36

We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies.

Recommendation 37

We recommend that the US Government should move toward a system in which background investigations relating to the vetting of personnel for security clearance are performed solely by US Government employees or by a non-profit, private sector corporation.

Recommendation 38

We recommend that the vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data from Insider Threat programs and from commercially available sources, to note such things as changes in credit ratings or any arrests or court proceedings.

Recommendation 39

We recommend that security clearances should be more highly differentiated, including the creation of "administrative access" clearances that allow for support and information technology personnel

to have the access they need without granting them unnecessary access to substantive policy or intelligence material.

Recommendation 40

We recommend that the US Government should institute a demonstration project in which personnel with security clearances would be given an Access Score, based upon the sensitivity of the information to which they have access and the number and sensitivity of Special Access Programs and Compartmented Material clearances they have. Such an Access Score should be periodically updated.

Recommendation 41

We recommend that the "need-to-share" or "need-to-know" models should be replaced with a Work-Related Access model, which would ensure that all personnel whose role requires access to specific information have such access, without making the data more generally available to cleared personnel who are merely interested.

Recommendation 42

We recommend that the Government networks carrying Secret and higher classification information should use the best available cyber security hardware, software, and procedural protections against both external and internal threats. The National Security Advisor and the Director of the Office of Management and Budget should annually report to the President on the implementation of this standard. All networks carrying classified data, including those in contractor corporations, should be subject to a Network Continuous Monitoring

Program, similar to the EINSTEIN 3 and TUTELAGE programs, to record network traffic for real time and subsequent review to detect anomalous activity, malicious actions, and data breaches.

Recommendation 43

We recommend that the President's prior directions to improve the security of classified networks, Executive Order 13587, should be fully implemented as soon as possible.

Recommendation 44

We recommend that the National Security Council Principals Committee should annually meet to review the state of security of US Government networks carrying classified information, programs to improve such security, and evolving threats to such networks. An interagency "Red Team" should report annually to the Principals with an independent, "second opinion" on the state of security of the classified information networks.

Recommendation 45

We recommend that all US agencies and departments with classified information should expand their use of software, hardware, and procedures that limit access to documents and data to those specifically authorized to have access to them. The US Government should fund the development of, procure, and widely use on classified networks improved Information Rights Management software to control the dissemination of classified data in a way that provides greater restrictions on access and use, as well as an audit trail of such use.

Recommendation 46

We recommend the use of cost-benefit analysis and risk-management approaches, both prospective and retrospective, to orient judgments about personnel security and network security measures.

Mr. GOODLATTE. Thank you.
Mr. Medine, welcome.

**TESTIMONY OF DAVID MEDINE,
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD**

Mr. MEDINE. Thank you, Mr. Chairman, Ranking Member Conyers.

Mr. GOODLATTE. You want to hit the button there on your—good. Pull it close to you as well.

Mr. MEDINE. There we go. Thank you, Mr. Chairman, Ranking Member Conyers, and Members of the Committee, for the opportunity to testify regarding recommendations to reform the Nation's intelligence gathering program.

I'm the chairman of the Privacy and Civil Liberties Oversight Board, an independent, bipartisan agency in the executive branch tasked with ensuring that our Nation's counterterrorism efforts are balanced with the need to protect privacy and civil liberties.

I'd like to offer both my statement and the board's report for the record. The board's report focuses on the 215 program and the operations of the Foreign Intelligence Surveillance Court. And most of the recommendations are unanimous in our report. I will highlight some of the areas where there was lack of unanimity.

But before I start, I'd like to express the board's respect and admiration for the men and women in the intelligence community, who work tirelessly to protect our country day and night and uphold our values. We hold them in the highest regard, based on everything we have observed during the course of conducting our study.

In June, many Members of Congress and the President asked us to prepare a report on the 215 and 702 programs conducted by NSA. Our 702 report will be issued in a couple of months.

In the course of conducting our study, we had briefings with a number of intelligence agencies and had an opportunity to see the 215 program in action. We held two public events to get public input, as well as soliciting public comment, and met with industry groups, trade associations, and advocates regarding this program. This culminated in our release on January 23 of our report addressing, again, the 215 program and reforms to the FISC.

With regard to the 215 program, we conducted a statutory analysis and concluded that the program lacks a viable foundation in the law. We also looked at the First and Fourth Amendment of the Constitution and concluded that the program raised serious concerns under both of those amendments.

We examined the privacy and civil liberties consequences of the program and found them serious because the program contains highly sensitive information. Citizens may be chilled in exercising their associational rights, in engaging with reporters or religious groups or political organizations, knowing that the Government is collecting information about them.

This is also information that's subject to potential abuse. We did not see any abuse now, but we certainly know lessons from the 20th century where there were abuses of surveillance of civil rights leaders and anti-war activists and others. And so, gathering this

information by the Government does raise serious privacy and civil liberties consequences.

But we also looked at the efficacy of the program, and we looked at each of the instances in which there were claimed successes in the program. We had classified information, and we checked our facts with the intelligence community. And after that analysis, we concluded that the benefits of the program are modest at best, and they are outweighed by the privacy and civil liberties consequences.

As a result, a majority of the board recommended that the program be discontinued, and the entire board recommended that there be immediate changes to the program to add privacy and civil liberties protections. The dissenting members of the board felt that the Government's interpretation of the program in the law was reasonable and that with the privacy changes that we are proposing on the interim basis, that they would be comfortable with having the program continue with those changes.

Turning to the Foreign Intelligence Surveillance Court, the board unanimously recommends changes to the operation of the court, both to bolster the court's confidence with the public and as well as let the court benefit from adversary proceedings, which are the heart of the judicial process.

So, accordingly, the board recommends that a panel of special advocates be created, made up of private attorneys appointed by the court in cases involving significant legal and policy issues and new technologies so that there is another side presented besides the Government's position, to argue on both statutory and constitutional grounds.

We also recommend that there be an opportunity to appeal decisions of the court by the advocate. There have only been two appeals ever to the Foreign Intelligence Surveillance Court of Review, and we think there's a benefit from the appellate process and, therefore, recommend a mechanism by which we think you can constitutionally have the special advocate obtain appellate review of the decisions.

And then we also encourage the court to obtain more technical assistance and outside legal views because these are complex issues that the court is confronting, and the court could benefit from technology advice.

And lastly, the board focused on transparency issues. In our democracy, there's a tension between openness and secrecy with regarding our intelligence programs. We've made recommendations that we believe serve both of those values, and most of those recommendations are unanimous as well.

So thank you very much for the opportunity to appear, and I'd be happy to answer your questions.

[The prepared statement of Mr. Medine follows:]



PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

STATEMENT
OF
DAVID MEDINE, CHAIRMAN
PRIVACY AND CIVIL LIBERTIES OVERSIGHT
BOARD
BEFORE THE
HOUSE JUDICIARY COMMITTEE
HEARING ENTITLED
"RECOMMENDATIONS TO REFORM FOREIGN
INTELLIGENCE PROGRAMS"

FEBRUARY 4, 2014

STATEMENT OF DAVID MEDINE
CHAIRMAN, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
BEFORE THE HOUSE JUDICIARY COMMITTEE
HEARING ENTITLED
"RECOMMENDATIONS TO REFORM FOREIGN INTELLIGENCE PROGRAMS"
FEBRUARY 4, 2014

I. Introduction

Thank you for the opportunity to appear today before the House Judiciary Committee as you evaluate potential reforms to government surveillance programs.

I am the chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent executive branch agency tasked with ensuring that our nation's counterterrorism efforts are balanced with the need to protect civil liberties and privacy. On January 23, 2014, the Board released a comprehensive public report addressing the bulk telephone records program conducted by the National Security Agency ("NSA") under Section 215 of the USA PATRIOT Act, as well as the operations of the Foreign Intelligence Surveillance Court.¹ The report, which is available at www.pclob.gov, contains an in-depth examination of the Section 215 program, including its operation, history, legality, constitutionality, and an analysis of whether it appropriately balances national security with privacy and civil liberties. The report also addresses the operations of the Foreign Intelligence Surveillance Court and the issue of transparency in government surveillance programs. The Board has made twelve specific recommendations for reform in these areas, ten of which were unanimous among the Board's five members.²

The Board looks forward to working with Congress and the executive branch in the coming months as reforms to the government's surveillance practices are being considered.³

¹ See Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Jan. 23, 2014), *available at* <http://www.pclob.gov/>.

² The Board's next public report will examine the surveillance program being conducted by the National Security Agency under Section 702 of the FISA Amendments Act of 2008, addressing whether, in the Board's view, the program is consistent with statutory authority, complies with the Constitution, and strikes the appropriate balance between national security and privacy and civil liberties.

³ While these prepared remarks describe the views of the full Board, as reflected in its January 23, 2014 report (including the separate minority statements included with that report), my spoken comments at the hearing represent my own personal views.

II. The PCLOB

The PCLOB is an independent bipartisan agency within the executive branch. The Board's creation was a recommendation of the 9/11 Commission, which advised in its final report that "there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."⁴

The Board was established in its present form as an independent agency by the Implementing Recommendations of the 9/11 Commission Act of 2007,⁵ but it did not become fully operational with all five Board members until May of last year.⁶ It is comprised of four part-time members and a full-time chairman, each serving staggered six-year terms, all appointed by the President and confirmed by the Senate.⁷ The Board's authorizing statute gives it two primary responsibilities: (1) to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties," and (2) to "ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."⁸

⁴ THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at 395 (2004). The National Commission on Terrorist Attacks on the United States (known as the 9/11 Commission) was a bipartisan panel established to "make a full and complete accounting of the circumstances surrounding" the September 11, 2001, terrorist attacks, and to provide "recommendations for corrective measures that can be taken to prevent acts of terrorism." Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, § 602(4), (5), 116 Stat. 2383, 2408 (2002).

⁵ Pub. L. No. 110-53, § 801(a), 121 Stat. 266, 352-58 (2007).

⁶ In August 2012, the Board's four part-time members were confirmed by the Senate, providing the reconstituted Board with its first confirmed members and a quorum to begin operations. I was confirmed as chairman of the Board (its only full-time member) on May 7, 2013, and sworn in on May 29, five days before news stories based upon the NSA leaks began to appear.

⁷ The five members of the Board, and their respective terms, are as follows:

- Rachel L. Brand, whose term ends January 29, 2017.
- Elisebeth Collins Cook, whose first term ended January 29, 2014. On January 6, 2014, Ms. Cook was nominated for a second term ending January 29, 2020. Under the Board's authorizing statute, as a result of this nomination, Ms. Cook can continue to serve through the end of the Senate's current session and, if confirmed before then, through January 29, 2020.
- James X. Dempsey, whose term ends January 29, 2016.
- David Medine (chairman), whose term ends January 29, 2018.
- Patricia M. Wald, whose term ends January 29, 2019.

⁸ 42 U.S.C. § 2000ee(c).

III. The Board's Report on the Section 215 Telephone Records Program and the FISA Court

Last June, shortly after the first news articles appeared disclosing the existence of a previously unknown NSA program conducted under Section 215, as well as details regarding surveillance conducted under Section 702 of the FISA Amendments Act, a bipartisan group of thirteen U.S. Senators asked the PCLOB to investigate those programs and to produce an unclassified report, "so that the public and the Congress can have a long overdue debate" about the privacy issues they raised.⁹ A subsequent letter from House Minority Leader Nancy Pelosi requested that the Board also consider the operations of the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"), which approved the two programs. On June 21, 2013, the Board met with President Obama and his senior staff at the White House, and the President asked the Board to review "where our counterterrorism efforts and our values come into tension."¹⁰

In response to these congressional and presidential requests, the Board initiated a study of the Section 215 and 702 programs and the operation of the FISA court.¹¹ This study included classified briefings with officials from the Office of the Director for National Intelligence ("ODNI"), NSA, Department of Justice, Federal Bureau of Investigation ("FBI"), and Central Intelligence Agency ("CIA"). Board members also met with White House staff, a former presiding judge of the FISA court, academics, privacy and civil liberties advocates, technology and communications companies, and trade associations. In addition, the Board received a demonstration of the Section 215 program's operation and capabilities at the NSA. The Board has been provided access to classified opinions by the FISA court, various inspector general reports, and additional classified documents relating to the operation and effectiveness of the programs. At every step of the way, the Board has received the full cooperation of the intelligence agencies.

As part of its study, and consistent with our statutory mandate to operate publicly where possible, the Board held two public forums. The first was a day-long public workshop held in Washington, D.C., on July 9, 2013, comprised of three panels addressing different aspects of the Section 215 and 702 programs. The panelists provided input on the legal, constitutional, technology, and policy issues implicated by the two programs. The

⁹ Letter from Senator Tom Udall *et al.* to the Privacy and Civil Liberties Oversight Board (June 12, 2013), available at <http://www.pclob.gov/>.

¹⁰ See Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), available at <http://www.pclob.gov/>; Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>.

¹¹ Prior to my confirmation as chairman, the four part-time Board members already had identified implementation of the FISA Amendments Act as a priority for oversight. As a result, the Section 702 program already was familiar to the majority of the Board by June 2013.

first panel addressed the legality of the programs, and included comments from a former FISA court judge regarding the operation of that court. Because technological issues are central to the operations of both programs, the second panel was comprised of technology experts. The third panel included academics and members of the advocacy community; panelists were invited to provide views on the policy implications of the NSA programs and what changes, if any, would be appropriate.

As the Board's study of the NSA surveillance programs moved forward, the Board began to consider possible recommendations for program changes. At the same time, the Board wanted to try to identify any unanticipated consequences of reforms it was considering. Accordingly, on November 4, 2013, the Board held a public hearing in Washington, D.C. The hearing began with a panel of current government officials who addressed the value of the programs and the potential impact of proposed changes. The second panel, designed to explore the operation of the FISA court, consisted of another former FISC judge, along with a former government official and a private attorney who both had appeared before the FISC. Finally, the Board heard from a diverse panel of experts on potential Section 215 and 702 reforms.¹²

Based on the information and input made available to the Board, we conducted a detailed analysis of applicable statutory authorities, the First and Fourth Amendments to the Constitution, and privacy and civil liberties policy issues raised by the Section 215 program. The Board provided its draft description of the operation of the FISA court (but not our recommendations) to the court's staff to ensure that this description accurately portrayed the court's processes. The Board also provided draft portions of its analysis regarding the effectiveness of the Section 215 program (but not our conclusions and recommendations) to the U.S. Intelligence Community to ensure that our factual statements were correct and complete. While the Board's report was subject to classification review, none of the changes resulting from that process affected our analysis or recommendations. There was no outside review of the substance of our analysis or recommendations.

During the time that the PCLOB was conducting its study, members of Congress introduced a variety of legislative proposals to address the Section 215 and 702 programs, and the executive branch simultaneously was engaging in several internal reviews of the programs. To ensure that the PCLOB's recommendations would be considered as part of this ongoing debate, the Board divided its study into two separate reports. The first report, issued on January 23, 2014, covers the PCLOB's analysis and recommendations concerning operation of the Section 215 program and the FISA court. The second report, which also

¹² Transcripts of the Board's July 2013 public workshop and its November 2013 public hearing are available at <http://www.pclob.gov/>.

will be public and unclassified,¹³ will contain the PCLOB's analysis and recommendations concerning the Section 702 program.

Proposals for modifications to the Section 215 program and the operation of the FISA court also were under active consideration by the White House while we were conducting our study. Pursuant to the Board's statutory duty to advise the President and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of legislation and policies, and to provide advice on proposals to retain or enhance a particular counterterrorism power, the PCLOB briefed senior White House staff on the Board's tentative conclusions on December 5, 2013. We provided a near-final draft of the Board's conclusions and recommendations on Section 215 and the operations of the FISA court to the White House on January 3, 2014. On January 8, the full Board met with the President, the Vice President, and senior officials to present the Board's conclusions and the views of individual Board members.

Our first report consists of seven sections, five of which address the Section 215 telephone records program. The report begins by describing in detail how the program works. To put the present-day operation of the program in context, the report also recounts its history, including its evolution from predecessor intelligence activities. Turning to the Board's analysis, the report then addresses whether the telephone records program is consistent with applicable statutory requirements. It then addresses the constitutional issues raised by the program under both the First and Fourth Amendments. Finally, the report examines the potential benefits of the Section 215 program, its efficacy in achieving its purposes, and the impact of the program on privacy and civil liberties, before presenting the Board's conclusion that reforms are needed.

In addition to examining the Section 215 program, the Board's report also addresses the operations of the FISA court, proposing a new approach that, in appropriate cases, would allow the judges serving on that court to hear from a Special Advocate. The final section of the report addresses the issue of transparency as it relates to government surveillance activities. The report also includes separate statements by Board members Rachel Brand and Elisebeth Collins Cook. Although these two members joined in ten of the twelve recommendations made in the report, as outlined below, they wrote separately to explain their disagreement with the remaining two recommendations and with some of the Board's analysis.

While the Board's report includes a number of detailed conclusions and recommendations, it does not purport to answer all questions. The Board welcomes the

¹³ It is possible that the report on the Section 702 program will also include a classified annex.

opportunity for further dialogue within the executive branch and with Congress about the issues raised in its report and how best to implement the Board's recommendations.

IV. The Board's Findings and Analysis

A. Background: Description and History of the Section 215 Program

The NSA's telephone records program is operated under an order issued by the FISA court pursuant to Section 215 of the Patriot Act, an order that is renewed approximately every ninety days. The program is intended to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the United States. When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks. The FISC order authorizes the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifies detailed rules for the use and retention of these records. Call detail records typically include much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers. Such information is commonly referred to as a type of "metadata." The records collected by the NSA under this program do not, however, include the content of any telephone conversation.

After collecting these telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through "queries" of the database. A query is a search for a specific number or other selection term within the database. Before any specific number is used as the search target or "seed" for a query, one of twenty-two designated NSA officials must first determine that there is a reasonable, articulable suspicion ("RAS") that the number is associated with terrorism. Once the seed has been RAS-approved, NSA analysts may run queries that will return the calling records for that seed, and conduct "contact chaining" to develop a fuller picture of the seed's contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number (the "first hop"), but also numbers in contact with all first hop numbers (the "second hop"), as well as all numbers in contact with all second hop numbers (the "third hop").

In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to

process its calling records.¹⁴ The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store." The ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three "hops" of every currently approved selection term.¹⁵

The Section 215 telephone records program has its roots in counterterrorism efforts that originated in the immediate aftermath of the September 11 attacks. The NSA began collecting telephone metadata in bulk as one part of what became known as the President's Surveillance Program. From late 2001 through early 2006, the NSA collected bulk telephony metadata based upon presidential authorizations issued every thirty to forty-five days. In May 2006, the FISC first granted an application by the government to conduct the telephone records program under Section 215.¹⁶ The government's application relied heavily on the reasoning of a 2004 FISA court opinion and order approving the bulk collection of Internet metadata under a different provision of FISA.¹⁷

On June 5, 2013, the British newspaper *The Guardian* published an article based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA, which revealed the telephone records program to the public. On August 29, 2013, FISC Judge Claire Eagan issued an opinion explaining the court's rationale for approving the Section 215 telephone records program.¹⁸ Although prior authorizations of the program had been accompanied by detailed orders outlining applicable rules and minimization procedures, this was the first judicial opinion explaining the FISA court's legal reasoning in authorizing the bulk records collection. The Section 215 program was reauthorized most recently by the FISC on January 3, 2014.

Over the years, a series of compliance issues were brought to the attention of the FISA court by the government. However, none of these compliance issues involved significant intentional misuse of the system. Nor has the Board seen any evidence of bad faith or misconduct on the part of any government officials or agents involved with the

¹⁴ This "automated query process" was first approved for use by the FISA court in late 2012. Primary Order at 11 n.11.

¹⁵ See Primary Order at 11.

¹⁶ See Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006).

¹⁷ See Opinion and Order, No. PR/TT [redacted] (FISA Ct.).

¹⁸ See Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

program.¹⁹ Rather, the compliance issues were recognized by the FISC — and are recognized by the Board — as a product of the program's technological complexity and vast scope, illustrating the risks inherent in such a program.

B. Statutory and Constitutional Considerations Regarding the Section 215 Program

The Board has concluded that Section 215 of the Patriot Act does not provide an adequate legal basis to support the NSA's bulk telephone records program. Section 215 is designed to enable the FBI to acquire records that a business has in its possession, as part of an FBI investigation, when those records are relevant to the investigation. Yet the operation of the NSA's bulk telephone records program bears almost no resemblance to that description. While the Board believes that this program has been conducted in good faith to vigorously pursue the government's counterterrorism mission and appreciates the government's efforts to bring the program under the oversight of the FISA court, it concludes that the program is not authorized by Section 215.

There are four grounds upon which we have concluded that the NSA's program fails to comply with Section 215. First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk — potentially encompassing all telephone calling records across the nation — they cannot be regarded as “relevant” to any FBI investigation as required by the statute without redefining that word in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession) — an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything.

In addition, we conclude that the program violates the Electronic Communications Privacy Act. That statute prohibits telephone companies from sharing customer records with the government except in response to specific enumerated circumstances, which do not include Section 215 orders.

¹⁹ Neither has the Board seen any evidence that would suggest any telephone providers did not rely in good faith on orders of the FISC when producing metadata to the government.

Finally, we do not agree that the NSA's program can be considered statutorily authorized because Congress twice delayed the expiration date of Section 215 during the operation of the program without amending the statute. The "reenactment doctrine," under which Congress is presumed to have adopted settled administrative or judicial interpretations of a statute, does not trump the plain meaning of a law, and cannot save an administrative or judicial interpretation that contradicts the statute itself. Moreover, the circumstances presented here differ in pivotal ways from any in which the reenactment doctrine has ever been applied, and applying the doctrine here would undermine the public's ability to know what the law is and hold their elected representatives accountable for their legislative choices.

The Board also believes that the NSA's bulk telephone records program raises concerns under both the First and Fourth Amendments to the United States Constitution. Our report explores those concerns, explaining that while government officials are entitled to rely on existing Supreme Court doctrine in formulating policy, the existing doctrine does not fully answer whether the Section 215 program is constitutionally sound. In particular, the scope and duration of the program are beyond anything ever before confronted by the courts, and as a result of technological developments, the government possesses capabilities to collect, store, and analyze data not available when existing Supreme Court doctrine was developed. Without seeking to predict the direction of changes in that doctrine, the Board urges as a policy matter that the government consider how to preserve underlying constitutional guarantees in the face of modern communications technology and surveillance capabilities.

C. Policy Considerations Regarding the Section 215 Program

The Section 215 telephone records program was intended to function as a unique tool to help combat the very real threat of terrorism faced today by the United States — a tool that, it was hoped, would help investigators piece together the networks of terrorist groups and the patterns of their communications with a speed and comprehensiveness not otherwise available. However, the Board has concluded that the program has shown only minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, the Board is aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect (a suspect who was not involved in planning a terrorist attack, and who might have been discovered by the FBI without the contribution of the NSA's program).

The Board's review suggests that where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways: by offering additional leads regarding the contacts of terrorism suspects already known to investigators, and by demonstrating that foreign terrorist plots do *not* have a U.S. nexus. While the former can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target, our review suggests that the Section 215 program offers little unique value but largely duplicates the FBI's own information-gathering efforts. And while eliminating a U.S. nexus to foreign plots can help the intelligence community focus its limited investigatory resources in time-sensitive situations by channeling efforts where they are needed most, our report questions whether the American public should accept the government's routine collection of all of its telephone records because it helps in cases where there is no threat to the United States.

The Board also has analyzed the implications of the Section 215 program for privacy and civil liberties and has concluded that these implications are serious. Because telephone calling records can reveal intimate details about a person's life, particularly when aggregated with other information and subjected to sophisticated computer analysis, the government's collection of a person's entire telephone calling history has a significant and detrimental effect on individual privacy. The circumstances of a particular call can be highly suggestive of its content, such that the mere record of a call potentially offers a window into the caller's private affairs. Moreover, when the government collects *all* of a person's telephone records, storing them for five years in a government database that is subject to high-speed digital searching and analysis, the privacy implications go far beyond what can be revealed by the metadata of a single telephone call.

Beyond such individual privacy intrusions, permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens. With its powers of compulsion and criminal prosecution, the government poses unique threats to privacy when it collects data on its own citizens. Government collection of personal information on such a massive scale also courts the ever-present danger of "mission creep." An even more compelling danger is that personal information collected by the government will be misused to harass, blackmail, or intimidate, or to single out for scrutiny particular individuals or groups. While the danger of such abuse may seem remote today — we have seen no indication that anything of this sort is occurring at the NSA²⁰ — the risk is more than merely theoretical, given the history of the government's abuse of personal information during the twentieth century.

²⁰ The Board's report emphasizes that we have seen no evidence suggesting that the NSA is misusing the telephone records it acquires under this program for any purpose other than legitimate efforts to combat terrorism. The agency's incidents of non-compliance with the rules approved by the FISA court have generally involved unintentional mistakes resulting from the scope and complexity of the program.

Furthermore, the government's bulk collection of telephone records can be expected to have a chilling effect on the free exercise of speech and association, because individuals and groups engaged in sensitive or controversial work have less reason to trust in the confidentiality of their relationships as revealed by their calling patterns. Inability to expect privacy vis-à-vis the government in one's telephone communications means that people engaged in wholly lawful activities — but who for various reasons justifiably do not wish the government to know about their communications — must either forgo such activities, reduce their frequency, or take costly measures to hide them from government surveillance. The telephone records program thus hinders the ability of advocacy organizations to communicate confidentially with members, donors, legislators, whistleblowers, members of the public, and others. For similar reasons, awareness that a record of all telephone calls is stored in a government database may have debilitating consequences for communication between journalists and sources.

Detailed rules limit the NSA's *use* of the telephone records it collects, and the Board's report describes them at length. But while those rules offer many valuable safeguards designed to curb the intrusiveness of the program, in the Board's view they cannot fully ameliorate the implications for privacy, speech, and association that follow from the government's ongoing *collection* of virtually all telephone records of every American.

Any governmental program that entails such costs to privacy and civil liberties requires a strong showing of efficacy. As the 9/11 Commission recommended: "The burden of proof for retaining a particular governmental power should be on the executive, to explain," among other things, "that the power actually materially enhances security."²¹ The Board has concluded that the NSA telephone records program conducted under Section 215 does not meet that standard, and that its modest contribution to counterterrorism efforts is outweighed by its implications for privacy, speech, and association.

D. Issues Concerning Operation of the Foreign Intelligence Surveillance Court and Transparency of Surveillance Programs

The Board's report also addresses the operation of the FISA court. The FISA court was created by the Foreign Intelligence Surveillance Act of 1978 ("FISA"), to provide a procedure under which the Attorney General could obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Over time, the scope of FISA and the jurisdiction of the FISA court have evolved. Initially, the FISC's sole role was to approve individualized FISA warrants for electronic surveillance relating to a specific person, a specific place, or a specific communications account or

²¹ 9/11 Commission Report, *supra*, at 394-95.

device. Beginning in 2004, the role of the FISC changed when the government approached the court with its first request to approve a program involving what is now referred to as “bulk collection.” In conducting this study, the Board was told by former FISA court judges that they were quite comfortable hearing only from government attorneys when evaluating individual surveillance requests but that the judges’ decision-making would be greatly enhanced if they could hear opposing views when ruling on requests to establish new surveillance programs.

The classified and *ex parte* nature of the court’s proceedings have raised concerns that it does not take adequate account of positions other than those of the government. But it is critical to the integrity of the court’s process that the public have confidence in its impartiality and rigor. Therefore, the Board believes that some reforms are appropriate and would help bolster public confidence in the operation of the court. The most important reforms proposed by the Board are: (1) creation of a panel of private attorneys (or “Special Advocates”) who can be brought into cases involving novel and significant issues by FISA court judges; (2) development of a process facilitating appellate review of FISA court decisions; and (3) increased opportunity for the FISA court to receive technical assistance and legal input from outside parties. We believe that our proposal successfully ensures the ability of the court to hear opposing views while not disrupting the court’s operation or raising constitutional concerns about the role of the advocate.

Finally, our report discusses transparency — the tension between the competing imperatives of openness and secrecy, and the challenges of developing and implementing intelligence programs in ways that serve both values. Beyond the controversies that have arisen from the Section 215 and 702 programs, the Board believes that the government must take the initiative and formulate long-term solutions that promote greater transparency for government surveillance policies in order to inform public debate on technology, national security, and civil liberties. In this effort, all three branches have a role.

For the executive branch, disclosures about key national security programs that involve the collection, storage, and dissemination of personal information — such as the operation of the National Counterterrorism Center — show that it is possible to describe secret practices and policies publicly without damage to national security or operational effectiveness. With regard to the legislative process, even where classified intelligence operations are involved, the purposes and framework of a program for domestic intelligence collection should be debated in public. While some hearings and briefings may need to be conducted in secret during the process of developing legislation, to ensure that policymakers fully understand the intended use of a particular authority, the government should not base an ongoing program affecting the rights of Americans on an interpretation of a statute that is not apparent from a natural reading of the text. In the case of Section 215, for instance, the government should have made it publicly clear during the

reauthorization process that occurred in 2006 that it intended for Section 215 to serve as legal authority to collect data in bulk on an ongoing basis.

There also is a need for greater transparency in the operations of the FISA court. Prospectively, we encourage the judges on the court to continue the recent practice of writing opinions with an eye toward declassification, separating sensitive facts particular to the case at hand from broader legal analyses. The Board also believes that there is significant value in producing declassified versions of earlier FISA court opinions, and it recommends that the government undertake a classification review of all significant FISA court opinions and orders involving novel interpretations of law. We realize that the process of redacting opinions not drafted for public disclosure will be difficult and will burden individuals with other pressing duties, but we believe that it is appropriate to make the effort where those opinions and orders complete the historical picture of the development of legal doctrine regarding matters within the jurisdiction of the court. In addition, should the government adopt our recommendation for a Special Advocate in the FISA court, the nature and extent of that advocate's role must be transparent to be effective.

It is also important to promote transparency through increased reporting to the public on the scope of surveillance programs. The Board's report urges the government to work with Internet service providers and other companies to reach agreement on standards allowing reasonable disclosures of aggregate statistics that would be meaningful without revealing sensitive government capabilities or tactics. We note that the government recently announced an agreement with providers as a step in this direction. We recommend that the government should also increase the level of detail in its unclassified reporting to Congress and the public regarding surveillance programs.

V. The Board's Recommendations

Based upon the findings and analysis described above, the PCLOB has made twelve specific recommendations regarding the Section 215 telephone records program, the operation of the FISA court, and transparency in intelligence activities. Ten of those recommendations are unanimous, as discussed further below. The Board's recommendations can be summarized as follows.

Recommendation 1: The government should end its Section 215 bulk telephone records program.

The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth

Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value. As a result, the Board recommends that the government end the program.

Without the current Section 215 program, the government would still be able to seek telephone calling records directly from communications providers through other existing legal authorities. The Board does not recommend that the government impose data retention requirements on providers in order to facilitate any system of seeking records directly from private databases.

Once the Section 215 bulk collection program has ended, the government should purge the database of telephone records that have been collected and stored during the program's operation, subject to limits on purging data that may arise under federal law or as a result of any pending litigation.

The Board also recommends against the enactment of legislation that would merely codify the existing program or any other program that collects bulk data on such a massive scale regarding individuals with no suspected ties to terrorism or criminal activity. Moreover, the Board's constitutional analysis should provide a message of caution, and as a policy matter, given the significant privacy and civil liberties interests at stake, if Congress seeks to provide legal authority for any new program, it should seek the least intrusive alternative and should not legislate to the outer bounds of its authority.

The Board recognizes that the government may need a short period of time to explore and institutionalize alternative approaches, and believes it would be appropriate for the government to wind down the 215 program over a brief interim period. If the government does find the need for a short wind-down period, the Board urges that it should follow the procedures under Recommendation 2 below.

Recommendation 2: The government should immediately implement additional privacy safeguards in operating the Section 215 bulk collection program.

The Board recommends that the government immediately implement several additional privacy safeguards to mitigate the privacy impact of the present Section 215 program. The recommended changes can be implemented without any need for congressional or FISC authorization. Specifically, the government should:

- (a) reduce the retention period for the bulk telephone records program from five years to three years;
- (b) reduce the number of "hops" used in contact chaining from three to two;

- (c) submit the NSA's "reasonable articulable suspicion" determinations to the FISC for review after they have been approved by NSA and used to query the database; and
- (d) require a "reasonable articulable suspicion" determination before analysts may submit queries to, or otherwise analyze, the "corporate store," which contains the results of contact chaining queries to the full "collection store."

Recommendation 3: Congress should enact legislation enabling the FISC to hear independent views, in addition to the government's views, on novel and significant applications and in other matters in which a FISC judge determines that consideration of the issues would merit such additional views.

Congress should authorize the establishment of a panel of outside lawyers to serve as Special Advocates before the FISC in appropriate cases. The presiding judge of the FISC should select attorneys drawn from the private sector to serve on the panel. The attorneys should be capable of obtaining appropriate security clearances and would then be available to be called upon to participate in certain FISC proceedings.

The decision as to whether the Special Advocate would participate in any particular matter should be left to the discretion of the FISC. The Board expects that the court would invite the Special Advocate to participate in matters involving interpretation of the scope of surveillance authorities, other matters presenting novel legal or technical questions, or matters involving broad programs of collection. The role of the Special Advocate, when invited by the court to participate, would be to make legal arguments addressing privacy, civil rights, and civil liberties interests. The Special Advocate would review the government's application and exercise his or her judgment about whether the proposed surveillance or collection is consistent with law or unduly affects privacy and civil liberties interests.

Recommendation 4: Congress should enact legislation to expand the opportunities for appellate review of FISC decisions by the Foreign Intelligence Surveillance Court of Review, and for review of those decisions by the Supreme Court of the United States.

Providing for greater appellate review of rulings by the FISC and by its companion appellate court, the Foreign Intelligence Surveillance Court of Review ("FISCR"), will strengthen the integrity of judicial review under FISA. Providing a role for the Special Advocate in seeking that appellate review will further increase public confidence in the integrity of the process.

Recommendation 5: The FISC should take full advantage of existing authorities to obtain technical assistance and expand opportunities for legal input from outside parties.

FISC judges should take advantage of their ability to appoint Special Masters or other technical experts to assist them in reviewing voluminous or technical materials, either in connection with initial applications or in compliance reviews. In addition, the FISC and the FISCR should develop procedures to facilitate amicus participation by third parties in cases involving questions that are of broad public interest, where it is feasible to do so consistent with national security.

Recommendation 6: To the maximum extent consistent with national security, the government should create and release with minimal redactions declassified versions of new decisions, orders and opinions by the FISC and FISCR in cases involving novel interpretations of FISA or other significant questions of law, technology or compliance.

FISC judges should continue their recent practice of drafting opinions in cases involving novel issues and other significant decisions in the expectation that declassified versions will be released to the public. The government should promptly create and release declassified versions of these FISC opinions.

Recommendation 7: Regarding previously written opinions, the government should perform a declassification review of decisions, orders and opinions by the FISC and FISCR that have not yet been released to the public and that involve novel interpretations of FISA or other significant questions of law, technology or compliance.

Although it may be more difficult to declassify older FISC opinions drafted without expectation of public release, the release of such older opinions is still important to facilitate public understanding of the development of the law under FISA. The government should create and release declassified versions of older opinions in novel or significant cases to the greatest extent possible consistent with protection of national security. This should cover programs that have been discontinued, where the legal interpretations justifying such programs have ongoing relevance.

Recommendation 8: The Attorney General should regularly and publicly report information regarding the operation of the Special Advocate program recommended by the Board. This should include statistics on the frequency and nature of Special Advocate participation in FISC and FISCR proceedings.

These reports should include statistics showing the number of cases in which a Special Advocate participated, as well as the number of cases identified by the government as raising a novel or significant issue, but in which the judge declined to invite Special Advocate participation. The reports should also indicate the extent to which FISC decisions have been subject to review in the FISCR and the frequency with which Special Advocate requests for FISCR review have been granted.

Recommendation 9: The government should work with Internet service providers and other companies that regularly receive FISA production orders to develop rules permitting the companies to voluntarily disclose certain statistical information. In addition, the government should publicly disclose more detailed statistics to provide a more complete picture of government surveillance operations.

The Board urges the government to pursue discussions with communications service providers to determine the maximum amount of information that companies could voluntarily publish to show the extent of government surveillance requests they receive per year in a way that is consistent with protection of national security. In addition, the government should itself release annual reports showing in more detail the nature and scope of FISA surveillance for each year.

Recommendation 10: The Attorney General should fully inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress. This should include providing the PCLOB with copies of the FISC decisions required to be produced under Section 601(a)(5).²²

Recommendation 11: The Board urges the government to begin developing principles and criteria for transparency.

The Board urges the Administration to commence the process of articulating principles and criteria for deciding what must be kept secret and what can be released as to existing and future programs that affect the American public.

Recommendation 12: The scope of surveillance authorities affecting Americans should be public.

In particular, the Administration should develop principles and criteria for the public articulation of the legal authorities under which it conducts surveillance affecting

²² Section 601(a)(5), which is codified at 50 U.S.C. § 1871(a)(5), requires the congressional intelligence and judiciary committees to be provided with decisions, orders, and opinions from the FISC, and from its companion appellate court, that include significant construction or interpretation of FISA provisions.

Americans. If the text of the statute itself is not sufficient to inform the public of the scope of asserted government authority, then the key elements of the legal opinion or other documents describing the government's legal analysis should be made public so there can be a free and open debate regarding the law's scope. This includes both original enactments such as 215's revisions and subsequent reauthorizations. While sensitive operational details regarding the conduct of government surveillance programs should remain classified, and while legal interpretations of the application of a statute in a particular case may also be secret, the government's interpretations of statutes that provide the basis for ongoing surveillance programs affecting Americans can and should be made public.

VI. Minority Views

While ten of the Board's twelve recommendations are unanimous, two are not. Board members Rachel Brand and Elisebeth Collins Cook did not join Recommendation 1 (that the government end its Section 215 bulk telephone records program) or Recommendation 12 (that the scope of surveillance authorities affecting Americans be made public). In addition, Ms. Brand and Ms. Cook did not join the Board's statutory or constitutional analysis. Both members explained their views in separate statements that are incorporated in the Board's report.²³

Ms. Brand and Ms. Cook both reached a different judgment than did the Board majority about how the value of the program weighs against its implications for privacy and civil liberties. Ms. Brand stressed that the usefulness of the program "may not be fully realized until we face another large-scale terrorist plot against the United States or our citizens abroad," and that "if that happens, analysts' ability to very quickly scan historical records from multiple service providers to establish connections (or avoid wasting precious time on futile leads) could be critical in thwarting the plot."²⁴ Ms. Cook emphasized the value of a tool that allows investigators to "triage and focus on those who are more likely to be doing harm to or in the United States," "more fully understand our adversaries in a relatively nimble way," and "verify and reinforce intelligence gathered from other programs or tools."²⁵

With respect to potential intrusions on privacy and civil liberties, Ms. Brand and Ms. Cook emphasized that the NSA does not acquire the contents of telephone calls or any personally identifying information about callers under this program, as well as the strict

²³ See Separate Statement by Board Member Rachel Brand (Jan. 23, 2014) ("Brand Statement"), and Separate Statement by Board Member Elisebeth Collins Cook (Jan. 23, 2014) ("Cook Statement"), available at <http://www.pclob.gov/>. Both statements are included as annexes to the Board's report.

²⁴ Brand Statement at 5-6.

²⁵ Cook Statement at 4.

safeguards and limitations governing the NSA's *use* of the records it obtains. While agreeing that certain additional privacy safeguards nevertheless are warranted (spelled out in the Board's second recommendation), in their judgment the value of the program, with those safeguards in place, outweighs its intrusions on privacy and civil liberties. Ms. Brand, however, noted that "if an adequate alternative that imposes less risk of privacy intrusions can be identified, the government should adopt it,"²⁶ and Ms. Cook recommended that the Intelligence Community devise "metrics for assessing the efficacy and value of intelligence programs, particularly in relation to other tools and programs," as well as conduct periodic assessments to gauge the relative value of such programs.²⁷

Ms. Brand and Ms. Cook also declined to join the Board's legal conclusion that the bulk telephone records program is unauthorized by Section 215 of the Patriot Act. They concluded that the government's interpretation of the statute is "at least a reasonable reading, made in good faith by numerous officials in two Administrations of different parties," as Ms. Brand put it,²⁸ representing "a good faith effort to subject a potentially controversial program to both judicial and legislative oversight," as Ms. Cook put it,²⁹ and stressed that the government's interpretation has been upheld by numerous Article III judges.

With respect to Recommendation 12 (regarding transparency in the scope of surveillance authorities affecting Americans), Ms. Brand explained that she does not believe "that an intelligence program or legal justification for it must necessarily be known to the public to be legitimate or lawful."³⁰ Ms. Cook similarly expressed her view that in a representative democracy "it is simply not the case that a particular use or related understanding of a statutory authorization is illegitimate unless it has been explicitly debated in an open forum."³¹

While the majority of the Board did not obtain unanimity on these two recommendations (among twelve recommendations overall), it believes that the reasoned and transparent disagreement on those points reflected in the Board's report and its minority statements can assist the Administration, Congress, and the public as they debate the future of our nation's surveillance practices.

²⁶ Brand Statement at 6.

²⁷ Cook Statement at 4.

²⁸ Brand Statement at 3.

²⁹ Cook Statement at 2.

³⁰ Brand Statement at 2.

³¹ Cook Statement at 4.

VII. Conclusion

Thank you for the opportunity to testify before the House Judiciary Committee today regarding the Board's report. As already noted, the Board welcomes the opportunity for further dialogue within the executive branch and with Congress about the issues raised in its report and how best to implement the Board's recommendations.

Mr. GOODLATTE. Thank you, Mr. Medine.

I will begin the questioning and will start with Deputy Attorney General Cole. Both the PCLOB and the review group have questioned the value of the bulk metadata program. Congress has been waiting for a long time for the Administration to explain exactly why bulk collection is crucial to national security.

So, Deputy Attorney General Cole, this is the Administration's opportunity to explain to Congress why bulk collection, as opposed to other intelligence measures, is necessary to protect our citizens.

Mr. JAMES COLE. Well, Mr. Chairman, I think to understand this, we first have to understand the value of trying to make the connections, connect the dots between people who we know are involved in terrorist activity or have reasonable, articulable suspicion to believe are, and the other people that they may be acting with, both inside and outside of the United States.

That's a very useful tool. It's not the only piece of evidence you would need in an investigation. And in fact, in my years as a prosecutor, there is rarely one piece of evidence that makes the case. It's a whole fabric of evidence that's woven together, small pieces that relate to each other that become useful once they're compared with and connected with many others.

This is a tool that gives us one of those pieces of information, the connections from one person to another. And in order to be able to get it in a useful way, the initial view and the most expeditious way to do it was to have the bulk collection of the mass of telephone records with significant restrictions on how we could access it.

So that we could, when we find a phone number associated with a certain terrorist group, we can search through the other records and find those connections. Now we can find other ways, and we are finding other ways to try and approximate and gain that same kind of information.

Mr. GOODLATTE. Let me ask you about one subset of that that is very, very important and seems to be the thing that concerns many people the most. The President's review group has recommended that the storage of bulk metadata be transferred to a third party or to company storage. The President also indicated that it is his preference as well.

How does third-party storage protect Americans' privacy more than Government storage, and does the President have additional ideas for reform beyond third-party storage?

Mr. JAMES COLE. Well, Mr. Chairman, we're trying to work through the best way to go about this, and the President has given us this direction, and we are looking for all the possible alternatives. The President's review group made that recommendation. The PCLOB noted that there are issues with all of the different alternatives that you can use here.

I think one of the issues that comes to mind is that the Government has certain powers that private groups don't have, and there is a concern among the American people when the Government has possession of all of those records and the powers that go with the Government, that they would prefer that the Government not have those records, that some private party have them.

Obviously, we need to make sure that strict controls are put on, as they were when the Government possessed the bulk data, to make sure that they're not abused. And it's very, very important to make sure that those strict controls, as had been done under the bulk collection, are continued regardless of where these records reside.

Mr. GOODLATTE. Let me ask you one follow up to that. That is really a critical question here. The third-party storage is really an idea that is still in progress.

If the Administration finds that third-party storage is not a viable option, what would be the President's recommendation for moving forward, continue the bulk collection program or ending it?

Mr. JAMES COLE. I think that's the process we're going through right now. I don't want to try and get too far ahead of it and hypothesize about where we may end up by the time we have to make recommendations to the President and he makes a decision. But obviously, the providers already—

Mr. GOODLATTE. You have heard the Ranking Member. There is legislation before the Committee. There are other legislative ideas than the one he referenced. But he and many others are chomping at the bit to move forward, and having the Administration's position on this critical aspect of this is important.

So we need to know the answer to that sooner rather than later.

Mr. JAMES COLE. And we're working on trying to get that answer, and we'll provide it to you. The providers already keep these records for a certain period of time, and some keep it longer than what is required under regulations.

And so, we have to work through what we think is the optimal period of time that the records need to be kept if there's going to be a provider keeping it solution.

Mr. GOODLATTE. And I want to direct one question to Mr. Medine before my time expires. The PCLOB majority recommends ending the bulk collection of telephony metadata under Section 215. The majority also recommends, however, that the program continue with certain modifications.

Why did the majority not recommend the immediate end to the program?

Mr. MEDINE. The majority looked to how other programs have been continued when, say, courts have struck them down. Even the Supreme Court has found programs unconstitutional and, nonetheless, gave the Government an opportunity to transition to a new program.

And so, rather than shut it off, we felt we followed the approach that the courts have taken, which is to say let's quickly transition into another program, either keeping the information with providers or some other mechanism as developed.

Mr. GOODLATTE. Well, you are talking about courts in other cases because the court—

Mr. MEDINE. Nothing—not in this case.

Mr. GOODLATTE. I haven't heard them say that in this case.

Mr. MEDINE. But we've looked at precedent of how, if a program has been found to be illegal or unconstitutional, courts oftentimes don't just shut it down. They give an opportunity to transition, and we thought that—especially since we're not a court, that it was rea-

sonable to recommend that there be a period of transition, hopefully brief, to a different program.

Mr. GOODLATTE. Thank you.

The gentleman from Michigan, Mr. Conyers, is recognized for 5 minutes.

Mr. CONYERS. Thank you.

And I thank the witnesses.

I would like to begin by asking Mr. Medine about the telephone metadata program. Let us get right to it. Is the telephone metadata program consistent with the plain text of Section 215?

Mr. MEDINE. Ranking Member Conyers, in the view of the majority of the board, it is not for a number of reasons. As I think you indicated in your statement, in many ways, it barely reflects the language of the statute.

Mr. CONYERS. And it also makes it clear that it must be relevant, and relevant does not mean everything. And I think that that is a very important way for us to begin looking at this.

Mr. Swire, the review group's report proposes the Government only seek business records under Section 215 on a case-by-case basis. Why is targeted collection a preferable and sufficient alternative to bulk collection?

Mr. SWIRE. Thank you, Congressman.

The review group in many instances thinks that targeted collection to face serious threats is traditional law enforcement and national security practice. When you identify particular people who create risks, it's wise to follow up on those.

We also, on bulk collection, on 215 in particular, found that there had not been any case where it had been essential to preventing an attack. The review group did find, as a group, that there was usefulness in Section 215 bulk collection, and we thought that transitioning it away from Government holding of the data was better within our system of checks and balances than having it held by the Government.

Mr. CONYERS. Thank you.

The report also says that the Government should no longer hold telephone metadata. If the Government can only collect metadata with a particularized showing of suspicion and the Government cannot hold information in bulk, what is left of the telephone metadata program?

Mr. SWIRE. Well, what's left is similar to metadata in other circumstances. This Committee knows about trap and trace and pen register authorities, which are done under standards much less than probable cause. It's much easier to get the metadata as step one to an investigation, and everything in our approach is consistent with using a judicial step, but a step with less than probable cause to go forward with the investigations.

Mr. CONYERS. Mr. Deputy Attorney General, in his January 17th remarks, President Obama asked the Justice Department to develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the Government holding this metadata itself.

What range of options might we consider as alternatives to the Government storing this information, if your group has gotten that far in its work?

Mr. JAMES COLE. Well, certainly, Mr. Ranking Member, there are three options that come to mind just off the top of my head, which is—or two options. One is a third party who would gather all of the data together so that the access could be across providers, which was the—one of the efficient and effective aspects of the metadata bulk collection program.

The other is to have the providers keep it. At this point, under regs, they're required to keep it for about 18 months. It might require legislation, if we deem that not to be a sufficient amount of time, to require them to keep it longer. I don't think they really favor that option.

We're also trying to think outside the box and see if there are any other options that we can come up with. There's a lot of very talented and very capable people trying to think through this problem and trying to find whatever creative solutions we can.

Mr. CONYERS. Thank you.

And my last question is to Mr. Medine. Both your board and the review group find that the bulk collection program has never disrupted a terrorist—a terror plot. The report also closely examines the 12 cases in which the Government says the telephone metadata program has contributed to a success story in a counterterrorism investigation.

What were those contributions, and do any of them to you justify a massive domestic call records database?

Mr. MEDINE. Mr. Ranking Member, we have analyzed carefully all of the success stories and, as you indicate, did not find any instance in which a plot was disrupted or an unknown terrorist was identified. However, there are some aspects of the program that have produced some benefits. One, a material assistance case benefited from use of the 215 program.

And there are also the “peace of mind” concept, which is sometimes it's helpful to know there isn't a U.S. connection to a potential plot that's underway overseas. But we found in those and any other instances where the program had had successes, that those successes could have been replicated using other legal authorities without the need to collect bulk telephone metadata and all of the privacy and civil liberties problems associated with that collection.

Mr. CONYERS. Mm-hmm. Thank you, Mr. Chairman.

Mr. GOODLATTE. Thank you.

The Chair recognizes the gentleman from Wisconsin, the Chairman of the Crime, Terrorism, Homeland Security, and Investigations Subcommittee, Mr. Sensenbrenner, for 5 minutes.

Mr. SENSENBRENNER. Thank you very much, Mr. Chairman.

I was the principal author of the PATRIOT Act that was signed by President Bush in 2001, and I also was the principal author of the two reauthorizations in 2006 and in 2011. Let me say that the revelations about Section 215 were a shock and that if the bulk collection program was debated by the Congress in each of these three instances, it never would have been approved.

And I can say that without qualification. Congress never did intend to allow bulk collections when it passed Section 215, and no fair reading of the text would allow for this program.

The PCLOB said, “The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates

constitutional concerns under the First and Fourth Amendments, raises serious threat to privacy and civil liberties as a policy matter, and has shown only limited value.”

I agree with that. Now the Administration, the argument that they use under Section 215 is essentially that if the Administration and the intelligence community wants something, it is relevant. And that is not a limiting principle, which everybody thought relevant was, it is a vacuum cleaner, and that is why there has been such outrage, both here and overseas, that has impacted our intelligence community and also implicated the commercial relationship between us and foreign countries, particularly major trading partners in the European Union.

And I am very worried about an intelligence review structure where the Administration and the FISCs could sanction this. That is why Mr. Conyers and I, together with a lot of Members equally divided between Republicans and Democrats, have sponsored the USA FREEDOM Act.

We attempted to make the FREEDOM Act a balance between the civil liberties concerns that have been expressed in the last 7 months, as well as the need to have an active intelligence operation. Now Section 215 expires in June of next year. And unless Section 215 is fixed, you, Mr. Cole, and the intelligence community will end up getting nothing because I am absolutely confident that there are not the votes in this Congress to reauthorize Section 215.

Now the FREEDOM Act is the only piece of legislation that attempts to comprehensively address this problem in a way that I think will get the support of a majority of the Members of both the House and the Senate. The Feinstein bill I think is a joke because it basically prohibits bulk collection, except as authorized under a subsection, which authorizes the intelligence community to keep on doing business as usual.

Mr. Cole, I think that we are smart enough to recognize that for what it is. And it is a joke. There hasn't been anything else that has come from the Administration or elsewhere to deal with this issue, and the clock, sir, is a-ticking. And it is ticking rapidly, and this is going to have to be addressed in this year, even though it is an election year.

Now will the Department of Justice, Mr. Cole, support the FREEDOM Act? And all I need is a “yes” or “no” answer.

Mr. JAMES COLE. Uh—

Mr. SENSENBRENNER. Not “yes, but” or, “no, of course.” But “yes” or “no.”

Mr. JAMES COLE. The Department of Justice is a big place, Senator, and at this point, we have not taken a position on the FREEDOM Act. We'd be more than happy to—

Mr. SENSENBRENNER. Well, then I—

Mr. JAMES COLE [continuing]. Work with you on that.

Mr. SENSENBRENNER. Well, then—well, I haven't seen any indication of that to date, and I would urge you to hurry up and to get the big place together. Because the FREEDOM Act are reasonable reforms that have been emphasized as necessary and responsible by both the PCLOB and the review panel. There is nothing else out there to fix this up.

So you have a choice between reaching something that will be supported by a majority of the Congress or letting the clock tick, and come June 1 of next year, there will be no authority for anything under Section 215.

Now if the Administration has got problems with the Leahy-Sensenbrenner-Conyers bill, let us talk about it. But it is past time for genuine reform, and I can tell you, sir, that if the Administration doesn't want to weigh in on this, I am sure that Congress will do so. And I don't want to hear any ex post facto complaining.

My time is up.

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

Mr. NADLER. Thank you very much, Mr. Chairman.

Let me first do something I rarely do, which is to express my complete and total agreement with the gentleman from Wisconsin. [Laughter.]

Both in his analysis of the misuse and abuse of Section 215 and of what will happen to Section 215 if it is not substantially modified either this year or early next year.

Mr. Conyers and I and various others opposed the Section 215 version that was adopted back in 2001 and again in 2006 and 2011. We thought it was too broad. But now we have even that very broad version completely taken over the side by the Administration, by two Administrations, actually, and by the FISC.

And the fact that the FISC several times determined that the use of Section 215 as authorization for what amounts to a general warrant, all right? You can collect all data, and then you can access that data without a specific warrant to access it or even a court order to access it, based on reasonable and articulable suspicion, but simply by an NSA or CIA officer saying, "We really need to look at that particular phone," is a derogation of all of American history, frankly, since 17—it is why we put the Fourth Amendment in because we objected to the British general warrants.

And we have, in effect, reestablished that here. And that will not stand. It cannot be allowed to stand.

So let me simply echo that it has got to change. There is no excuse for picking everything and then allowing access to that without some sort of a specific court order.

And the fiction that the warrant that the FISA court grants and says Verizon or AT&T shall give the Government access, you know, all telephone metadata over a 3-month period is a warrant, is a specific warrant that negates the necessity for a warrant or a court order for more specific information is just that, a fiction, and it is a general warrant. And it cannot be permitted to stand, and it won't be permitted to stand.

So I will second Mr. Sensenbrenner and urge you to swiftly get the department together and to if you don't want the FREEDOM Act to pass it the way it is or Section 215 simply to not be extended, which might be the best solution, frankly, from my point of view, you better come in with very specific recommendations.

Now let me say last week in testimony before the Senate, some Administration officials suggested that terrorist plots thwarted is not the appropriate metric for evaluating the effectiveness of the

program. And yet for months, the Administration has made precisely the opposite argument.

For example, in a September letter to NSA employees, General Alexander wrote that the agency has “contributed to keeping the U.S. and its allies safe from 54 terrorist plots.”

We have heard this 54 terrorist plots line repeated on several other occasions, although PCLOB and a lot of others have discredited it. Why has the argument changed? Why are we now to apply a different set of metrics to the program?

Mr. JAMES COLE. I assume that’s directed to me, Mr. Nadler.

Mr. NADLER. Yes, it is.

Mr. JAMES COLE. Well, first of all, I think to a degree you’re going to have to ask the people who made those statements. I don’t think any of them were from the Department of Justice.

We have been, and actually, some of the members of the PCLOB have agreed that that is—the past success or failure is not the only metric to use, or necessarily the best one. That there are many different ways to assess the utility of the 215 program that doesn’t always have to be, as I said earlier, the smoking gun or the nail in the coffin that gives you the single piece of evidence that will lead to success. It’s one piece of evidence.

Mr. NADLER. Okay. Thank you.

I am sorry to cut you off, but I have another question I must get in. National security letters empower the FBI and other Government agencies to compel individuals and organizations to turn over many of the same records that can be obtained by Section 215. But NSLs are issued by FBI officials, not by a judge or by a prosecutor in the context of a grand jury investigation.

As the Government has explained their use of this to this Committee, NSLs are used primarily to obtain telephone records, email subscriber information, and banking and credit card records. The FBI issued 21,000 NSLs in fiscal year 2012. The oversight and minimization requirements for these NSLs are far less rigorous than those in place for Section 215 orders.

The review group recommends “that all statutes authorizing the use of national security letters should be amended to require the use of the same oversight minimization, retention, and dissemination standards that currently govern the use of Section 215 orders.”

Should we adopt that recommendation? Is there any reason that the two programs should not be harmonized? For that matter, is there any reason that NSLs should exist in addition to Section 215 authorization in whatever form we extend it, if we do?

Mr. JAMES COLE. Well, actually, under the NSL program, you can’t get the same records you can get with 215. It’s much more limited under NSLs as to just specific categories of records. Whereas, 215, grand jury subpoenas, things like that, the records are almost unlimited as to the nature or the type that you can get.

So there’s a restriction in NSLs. They’re used really in the main as part of preliminary inquiries—

Mr. NADLER. Yes, but my point is if you can get it as under 215, if, in fact, 215 is broader, why do you need NSLs ever?

Mr. JAMES COLE. It may just be a question of, again, how many times you need that information and whether or not you go to a court. In a grand jury situation, subpoenas are issued without the

involvement of the court many, many, many times, probably as frequently, if not more so, as NSLs.

Mr. SENSENBRENNER [presiding]. The gentleman's time has expired.

Mr. NADLER. Thank you.

Mr. SENSENBRENNER. The gentleman from North Carolina, Mr. Coble?

Mr. COBLE. I thank the Chairman.

Gentlemen, good to have you all with us.

Mr. Cole, I was going to talk to you about bulk collection, but I think that has been pretty thoroughly examined.

Mr. Swire, let me go to you. The review group's report recommended a transition of Section 215 bulk metadata from Government storage to storage providers or third parties. This recommendation is consistent with recent guidance put forth by the Administration after its own review.

Last week, it was reported by Yahoo that information relating to email accounts and passwords, likely in the hands of such a party database, had been compromised due to a security breach. Are you concerned that Section 215 metadata could be similarly compromised after transitioning to a private provider or third-party storage?

Mr. SWIRE. Thank you, Congressman.

A couple of observations. One is, of course, that the National Security Agency itself has had leaks and lack of complete security for its documents. So we're not comparing perfect with perfect. We face these challenges for databases in each case.

A second observation is that the telephone companies hold telephone records. That's part of what they do and have done, and one of the options that we put forward is that the telephone companies would continue to hold these.

So it's not a question of some new risk that we bring into the world. It's a risk that we face both from the Government side and the private sector side when we have these databases.

I'm not sure if I—your—

Mr. COBLE. I think that was appropriate. Thank you, sir.

Mr. SWIRE. Okay.

Mr. COBLE. Mr. Medine? The FISA court has repeatedly upheld through its orders approving the NSA metadata program production of records to an agency other than the FBI. Did the privacy and civil liberties oversight majority take this into account?

Mr. MEDINE. Yes, sir. Section 215, on its face, only permits the FBI to make requests and obtain access to telephone records, despite the fact that under the current system it is the NSA that obtains that information. And so, we think that was one of a number of respects in which the current program does not match the requirements of Section 215.

Mr. COBLE. So you have no discomfort with that?

Mr. MEDINE. Excuse me?

Mr. COBLE. You have no discomfort or problem with that?

Mr. MEDINE. Yes. We have discomfort with a number of aspects of compliance. As was discussed earlier, the scope of relevance under the statute, the fact that information has to be linked to a specific investigation, and something that we haven't touched on

yet, which is the Electronic Communications Privacy Act does not permit telephone companies to provide information to the Government under the 215 program at all in either an individual request or on a bulk basis.

The Electronic Communications Privacy Act only has an exception for national security letters and a few other areas. So we think that it makes sense to discontinue—the majority does, to discontinue the 215 program and move to other legal authorities.

Mr. COBLE. Thank you again, gentlemen, for being with us this morning.

I yield back, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman from Virginia, Mr. Scott?

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Cole, you offered several procedural changes as recommendations. To paraphrase President Reagan, we need to trust, but codify. Would you object to those recommendations being codified rather than just remaining as administrative process?

Mr. JAMES COLE. I think as the President mentioned in his speech, he's anxious to work with Congress on many of these things to try and find the right solutions that we have. I know the USA FREEDOM Act, many of the goals that are set out there are goals that we share.

As I said in my opening, sometimes we have different ways of getting there, but we all seem to share the right goal together.

Mr. SCOTT. And follow-up, several other questions. We frequently hear that the information gathered was helpful. I find that legally irrelevant. So let me just ask a question. If a collection of data were illegal, would a finding that it was helpful provide retroactive immunity for illegally collecting evidence?

Mr. JAMES COLE. No, Mr. Scott, it would not. If the collection is illegal, the standard would not be met.

Mr. SCOTT. Thank you.

Mr. Swire, there was a case a couple of months ago in DNA that found that if DNA is legally collected, that there is no—there is no prohibition against running it through the database to see if the person had committed another crime. If I were to go up to you, if a law enforcement agency would go up to you and say, "I would like some DNA to see if you have committed crime," that would be legally laughable.

There appears to be no statutory limitation on what you can do with this information. So I guess my question is under—you recommended under 702 that if you have collected information about a U.S. person, you can never use it in any proceeding. That would, of course, eliminate any incentive to get the information in the first place if it was for something other than foreign intelligence.

If that is your recommendation for 702, would that also be your recommendation on 215, that you cannot use this data for other proceedings?

Mr. SWIRE. Thank you, Congressman.

Under Section 702, the target, by statute, is supposed to be somebody outside the United States. But sometimes they're in communication with people in the United States, and the concern behind our recommendation here is the possibility, which we have not seen in practice, is the possibility that the 702, do it overseas, could

turn out to be a way to gather lots of information about United States people.

And so, we made a recommendation to say that that would not be used in evidence in court as a way to prevent that temptation to use the authority to go after U.S. persons.

In terms of 215, we don't have the same statute that's specifically targeted at overseas. 215 can be for domestic phone calls as well. So we didn't have this using our overseas authorities to get people domestically—

Mr. SCOTT. But you're using foreign intelligence excuse to gather information that is subsequently used for criminal investigation.

Mr. SWIRE. We did not make a recommendation about subsequent use, but we, I think—I think all of us recognize using foreign intelligence powers for purely domestic phone calls has been something that's drawn a huge amount of attention to these issues and is something that historically has been something that's been looked at carefully when the CIA or other agencies have done it.

So that's a concern using foreign intelligence issues authorities for domestic purposes.

Mr. SCOTT. Let me follow through with another question that has been kind of alluded to, and that is that you want to limit Section 215 by ensuring that there is reasonable grounds to believe that it is relevant to an authorized investigation and the order is reasonably focused in scope and breadth.

Can you explain how that recommendation varies from what everybody up here thought was present law?

Mr. SWIRE. Well, I think when we talk about like a subpoena, an order should be reasonable in focus, scope, and breadth.

Mr. SCOTT. We wouldn't have to put that in a statute to assume that to be the case, right?

Mr. SWIRE. Well this gets into the statutory interpretation of the current 215. Our group did not take a position on that. The Government and the Privacy and Civil Liberties Oversight Board have come to different views on that.

Mr. SCOTT. That we would have to put reasonable in scope and breadth in the statute for that to be assumed?

Mr. SWIRE. Our recommendation was that a judge be involved in these things and that there be a reasonable breadth requirement explicitly in statute so that it's clear from Congress that that's what you intend.

Mr. SCOTT. You also indicated a recommendation that the NSA not be involved in collection of data other than foreign intelligence. Can you explain what the NSA is doing that is not involved in foreign intelligence?

Mr. SWIRE. In our—in our report, we talk about two other areas the NSA currently has or bears very important responsibilities. Currently, the Director of the NSA is also the Director of Cyber Command, which is part of the military operation for combat-related activities in cyberspace. We thought that was quite a different function from foreign intelligence collection.

The NSA also has responsibilities for what's called information assurance, protecting our classified and other systems, and we thought that defensive role is quite different from the offensive role of gathering intelligence and recommended those functions be split.

The President has not decided to adopt either of those recommendations.

Mr. SCOTT. Thank you.

And Mr. Cole, are you aware of any abuses in the use of classified information? Things like I think there is a thing called LOVEINT. Are you familiar with that?

Mr. JAMES COLE. I've heard that phrase, yes, sir.

Mr. SCOTT. What is that?

Mr. JAMES COLE. I think it's when you have somebody who is dating somebody, and they have access to one of these databases or a database and uses it to look at their—the person they're dating and find out who they're talking to and who they're in contact with. That's what I understand it to mean.

Mr. SCOTT. And that happens?

Mr. JAMES COLE. I think there have been a few instances. I think the NSA had noted a few instances of it. I don't think they existed under 215. I think they may have existed under other authorities, but I think there has been just a handful of those over time.

Mr. SCOTT. And what happens?

Mr. JAMES COLE. And they've been dealt with immediately.

Mr. SCOTT. And what has happened to the culprits?

Mr. JAMES COLE. I know that most, if not all of them, lost their jobs. There were referrals in many of those cases to the Justice Department to consider whether or not prosecution would be appropriate.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. GOODLATTE [presiding]. Thank you.

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

Mr. BACHUS. Thank you.

I would ask all three of the panelists is relevancy for purposes of intelligence gathering different from relevancy for purposes of, say, a criminal investigation or civil investigation? Shouldn't it be a—shouldn't the standard be somewhat different, or is it? Start with Mr. Cole.

Mr. JAMES COLE. I think as you've seen from the court's opinions, they borrow both from criminal investigations, civil proceedings, and do that and use those as analogies to get to the standard in foreign intelligence. And they find it to be the same standard.

Mr. BACHUS. You know, as just a Member of Congress, I sort of have the opinion that it is much more urgent for us to defend ourselves as a country. But does sometimes applying a civil court standard of relevancy or even a criminal court standard of relevancy sort of diminish their ability at—in defending the country from terrorists?

Mr. JAMES COLE. Well, I think if you look at Judge Eagan's opinion from the FISA court, her view and her finding was that the term "relevancy" was very broad and was very useful in both criminal, civil, and foreign intelligence investigations and can be applied very broadly when it's necessary.

It's not without limitation. It's not completely unrestrained. It's only when there is an actual need to get a broad scope of documents that it's authorized under that standard. And so, I think she had corporately found that scope.

Mr. BACHUS. All right. Ask the other two gentlemen.

Mr. MEDINE. The majority of the PCLOB has also considered relevancy in the context of criminal and civil proceedings as the statute suggests. And we looked at every case cited by the Government and more on criminal discovery, and I'm using the relevance standard, grand jury subpoenas, as well as civil. And our conclusion was that the 215 program far exceeded in scope anything that had been previously approved ever, and even the Government's white paper acknowledges that.

And so, we in our—at least the majority's view, it goes well beyond the face of the statute and a reasonable reading of relevance.

Mr. BACHUS. Right. Now that was a majority opinion.

Mr. MEDINE. That's correct.

Mr. BACHUS. So did two members dissent from that?

Mr. MEDINE. Yes, they did. And they—and they felt that the Government's reading of the statute was a reasonable one, as was the court's interpretation.

Mr. BACHUS. Okay. Mr. Swire?

Mr. SWIRE. Yes, Congressman. So our group did not do that legislative history and statutory analysis as part of our work. In our forward-looking recommendation, we used the word "relevant" for the scope of a 215 order but said like a subpoena, it should be reasonable in focus, scope, and breadth. So we tried to hem it in with that reasonable scope language.

Mr. BACHUS. I just, if we are talking about an EPA violation or we are talking about a criminal offense, a minor criminal offense, just applying those standards in that case law to public enemy and our foreign enemies of the United States, I feel like that lacks somewhat.

Judge John Bates wrote a letter I think after both of you all's reviews came out, and I think he raised some very legitimate concerns over things you have assigned to the court, including reviewing every national security letter, a public advocate. He and I think others in judiciary believe that could be a hindrance.

After his letter, have you reviewed it, and do you agree that he brings up some very valid points that ought to be considered? Mr. Swire? Professor?

Mr. SWIRE. After our report was complete, we did receive the judge's letter. In terms of the public advocate, I'd make a following observation, which is the PCLOB report did extremely thorough analysis of the legality under the statute of 215 that was really much more detailed than anything any of the District Courts had done.

And I think for just myself, not speaking for the whole group, I think that that supports our group's recommendation that having detailed briefing with thorough analysis on these issues not just from the Government can really help us understand the statute better. So that's part of why we thought the advocate would be helpful in some way because there would be a sort of thoroughness of a position—

Mr. BACHUS. Could you—could you all review his letter and maybe give this Committee additional comments in view of his letter? Particularly with the increasing caseload, if you are going to

increase their caseload, you are going to have to increase their resources.

Mr. MEDINE. I should add that the PCLOB's recommendation is that there be a special advocate only in those cases which involve unique law and technology issues, not the everyday 215 order where judges are very well equipped to make those judgments.

Mr. BACHUS. Yes, but I am talking about their caseloads. You have assigned—under you all's—both of your all's proposals, it is going to increase quite a bit.

Mr. MEDINE. Yes. Sure.

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 thank you to all the witnesses for your appearance here today and for answering our questions.

I would like to concur with many of the comments made by our colleague Mr. Sensenbrenner as to the surprise that many of us had at the interpretation of the word "relevant" in Section 215. I would like to explore—we have talked a lot about the metadata for telephone records. But what I would like to explore with you, Mr. Cole, and perhaps others of you have an opinion, is not what is happening now, but what you believe the statute would authorize if, if the bulk collection of telephone data is relevant because there might be in that massive data information that would be useful for an investigation.

What other tangible items would the statute authorize, not saying that we are doing this, the Government to collect? Would we be authorized to collect bulk credit card records, Mr. Cole?

Mr. JAMES COLE. Ms. Lofgren, I think what you have to look at, which is a very important part of the analysis that Judge Eagan described, I thought, quite well, is that it's not everything. It's what is necessary to gather the relevant information.

Ms. LOFGREN. Well, let me—what we are trying to explore here is really the role of the Government versus the citizen.

Mr. JAMES COLE. Correct.

Ms. LOFGREN. And if you can compile the record of every communication between every American because within that massive data there might be something useful to keep us safe, I am trying to explore with you, if that is your reading of Section 215 vis-a-vis metadata and the phone company, would that include cookies?

Mr. JAMES COLE. Cookies?

Ms. LOFGREN. Yes. Could it?

Mr. JAMES COLE. Again, I think the issue here really is under 215 with telephony metadata, the issue that was presented to the court was we needed the connections from one phone number to another.

Ms. LOFGREN. Okay. Well, let me—

Mr. JAMES COLE. And so, that was necessary. In a credit situation—

Ms. LOFGREN. Let me ask you ask you this. Let me go to Mr. Swire because you are clearly not going to address this issue.

Mr. JAMES COLE. I'm trying to, Congresswoman.

Ms. LOFGREN. I think you are trying to use up my time. If relevance allows for the collection of mass data because within that haystack, to use General Alexander's words, there is the needle, would 215, under that reading of the act, allow for the collection of all the photos taken at ATM machines, all the cookies selected by commercial providers?

We have special standards for records of gun sales and credit card records, but it doesn't preclude their selection. Did your group look at that from a legal basis, not what we are actually doing?

Mr. SWIRE. Well, we did not go through that list. But what I would observe is that a judge would have to make that decision. So the Department of Justice would need to go to the judge and say—

Ms. LOFGREN. Right.

Mr. SWIRE [continuing]. We want ATM photographs for this reason, and the judge would have to say that it meets all the other standards for 215. So that's something beyond just the Justice Department on its own.

Ms. LOFGREN. Right. Let me ask about NSLs because NSL, as I think Rich Clarke gave some very pointed comments about how many were collected, thousands each day, with no supervision whatsoever. And that is directed to electronic communications.

Could you under the Section I think, what is it, 502, do mass collection under 502? It doesn't seem to be precluded as—

Mr. SWIRE. So I'm not remembering the section. Under NSLs, we were not aware of bulk collection under NSLs.

Ms. LOFGREN. I am not saying what is happening. Do you think it provides the legal authority to do so? It is not precluded.

Mr. SWIRE. I haven't seen a theory under which the NSL authority could be used in that bulk way. I'm not aware of such a document that would—

Ms. LOFGREN. All right. What about 702, and do you think that 702 provides the legal authority for bulk collection?

Mr. SWIRE. 702, that partly depends on your idea of bulk. 702 does allow targeting of people outside the United States and allows content and allows accumulation of allotted data about those individuals and the people they're in communication with.

That, by itself, would not be the way that we'd have the entire database of everything that happens. It has to be targeted to an individual overseas.

Ms. LOFGREN. Just a final question. Have the metadata of Senators and Members of Congress been collected?

Mr. SWIRE. I'm not aware of any way that they're scrubbed out of the database. So whatever databases exist, I don't know why your phone calls would be screened out. We haven't heard any evidence—I'm not aware of any evidence that that screening out happens.

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

Ms. LOFGREN. My time has expired. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentleman from California, Mr. Issa, for 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman.

Following up on that, the gentlelady's question was do you collect? Your answer apparently is, yes, you do because you scrub everything. Is that correct?

Mr. SWIRE. Is—so—

Mr. ISSA. You take it, yes?

Mr. SWIRE. In terms of whether Members of Congress' records are collected, first of all, the names are not listed. It's based on phone numbers.

Mr. ISSA. Well, no, but the simple question. 202-225 and four digits. Do you collect it?

Mr. SWIRE. At this point, I'm not the U.S. Government, and maybe—

Mr. ISSA. Okay. Mr. Cole, do you collect 202-225 and four digits afterwards?

Mr. JAMES COLE. Without going specifically, probably we do, Congressman.

Mr. ISSA. So separation of powers, this is the—another branch. You gather the logs of Members of the House and Senate in their official calls, including calls to James Rosen. Is that right?

Mr. JAMES COLE. We're not allowed to look at any of those, however, unless we make a reasonable, articulable suspicion finding that that number is associated with a terrorist organization. So while they may be in the database, we can't look at any of those numbers under the court order without violating the court order.

Mr. ISSA. Well, speaking of court orders, Mr. Rosen, is he, in fact, a criminal?

Mr. JAMES COLE. Is he, in fact, a criminal?

Mr. ISSA. Well, the Attorney General had said that James Rosen, a Fox reporter, you know, there was a wiretap placed on his family, he and his family. Correct? Not, and this was—

Mr. JAMES COLE. No, there was not a wiretap, sir.

Mr. ISSA. There wasn't? I am sorry. You collected personal emails. Let me get it correct.

There was a warrant for personal emails, but there was also the—they wiretapped his family.

Let me rephrase that. Let me go on, and I will come back to that because I want to make sure I get the terminology right.

Do you screen executive branch numbers?

Mr. JAMES COLE. We don't screen any numbers, as far as—

Mr. ISSA. So you collect all numbers? The President's phone call log record is in the NSA database?

Mr. JAMES COLE. I believe every phone number that is with the providers that get those orders comes in under the scope of that order.

Mr. ISSA. Would you get back to us for the record as to whether all phone calls of the executive branch, including the President, are in those logs?

Mr. JAMES COLE. Be happy to get that back to you, Congressman.

Mr. ISSA. Okay. Especially if he calls Chancellor Merkel, it would be good to know.

The freedom of association is a basic constitutional right, wouldn't you agree, Mr. Cole?

Mr. JAMES COLE. Yes, it is.

Mr. ISSA. And if you are looking at our associations, and then if we have associations with somebody that you believe is “a terrorist,” then you take the next step, right?

Mr. JAMES COLE. Well, we don’t look at your associations, Congressman.

Mr. ISSA. Well, what does the metadata do if it is not——

Mr. JAMES COLE. We don’t look at the metadata unless we have a reasonable, articulable suspicion that the specific phone number we want to query is associated with terrorists. That’s the only way we can get into that metadata.

Mr. ISSA. Do you collect the phone number metadata of all embassies here in Washington, all the foreign embassies?

Mr. JAMES COLE. I believe we would. Again, we don’t screen anything out, to my knowledge. But that’s something that NSA would know. My understanding is we don’t screen anything.

Mr. ISSA. And they have conversations with large amounts of numbers back in their home countries, right?

Mr. JAMES COLE. All the telephone numbers have large amounts of conversations with lots of other telephone numbers. We don’t look at them unless we have that reasonable, articulable suspicion for a specific——

Mr. ISSA. But isn’t it true that the reasonable, articulable suspicion goes a little like this? I talk to somebody in Lebanon, who talks to somebody in Lebanon, who talks to somebody in Lebanon, who talks to somebody in Lebanon, who talks to somebody in Lebanon.

If you gather all that data, then I have talked to somebody who has indirectly talked to a terrorist. Isn’t that right?

Mr. JAMES COLE. That’s not how it would work, Congressman, no.

Mr. ISSA. How do I know that? How do I know that a 12-step removed, somebody talked to somebody, who talked to somebody, who talked to somebody, who talked to somebody who is on the list wouldn’t occur? And I will just give you an example.

The Deputy Prime Minister of Lebanon at one time gave \$10,000 to a group associated with a Hezbollah element. If I called the Deputy Prime Minister, which I did, from my office, wouldn’t I have talked to somebody who was under suspicion of being connected to a terrorist organization?

The answer, by the way, is yes. But go ahead and give yours.

Mr. JAMES COLE. Well, we wouldn’t be querying your phone number, Congressman, unless we had evidence that you were, in fact, involved with a terrorist organization. That’s the requirement under the court order——

Mr. ISSA. But you would query the Deputy Prime Minister, who had made a contribution and was under suspicion, right?

Mr. JAMES COLE. If we queried his phone number, we might find that connection.

Mr. ISSA. And at that point, you would have a connection between somebody who you had a warrant for and me. So you could have a warrant for me. Is that right?

Mr. JAMES COLE. Well, I do not think we would necessarily have enough to have a warrant for you with just that one phone call, Congressman. That is not how it works. Again, there are a lot of

restrictions in those court orders and in the rest of the law as to what we can do, and we can get warrants for, and what we cannot get warrants for.

Mr. ISSA. Well, we will follow up with the James Rosen thing later. Thank you. I yield back.

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

Ms. JACKSON LEE. Let me thank the Chair and the Ranking Member for someone who was here, as a number of other Members, in the aftermath of 9/11 and the intensity of writing the PATRIOT Act that came out of this Committee in a bipartisan approach. Ultimately it did not reach the floor of the House in that way.

As I try to recollect, I do not remember testimony that contributes to the massive data collecting that we have now wound up with. So I will pose as quickly as I can a series of questions. And, first, thank everyone for their service. It is good to see you, General Cole, and all of the other witnesses, the head of the Privacy and Oversight Board, and Mr. Swire as well. We thank you.

Quickly, you have been, I think, a lifer to a certain extent, working for United States justice and the United States of America. Again, we thank you. Did you all have an immediate interpretation of mega collecting under the final passage of the PATRIOT Act? Was that what first came to mind?

Mr. JAMES COLE. I was not in the government at the time the PATRIOT Act was passed, so I can honestly tell you I did not really think about it at that moment.

Ms. JACKSON LEE. As you proceeded to be in government and as you have continued in service now and over these past couple of years, was that a firm conclusion that you could gather everything?

Mr. JAMES COLE. As I became aware of what was being done under 215, and looking at the prior court precedents that came out that it had been approved and the descriptions of it, and some of the notices that were given to Congress, I was of the view that it was lawfully authorized under the PATRIOT Act and under 215.

Ms. JACKSON LEE. Well, you are as well required to follow the law, but I note that justice is in the U.S. Department of Justice, and what you are suggesting is that no lawyers as far as you know may have gathered to say that this may be extreme?

Mr. JAMES COLE. I am not aware of anybody saying that at the time, but again, I was not in the Justice Department at the time.

Ms. JACKSON LEE. Not at that time. I am coming forward now in the time that you have been in the Justice Department.

Mr. JAMES COLE. As far as the legal basis, I think everyone that I have talked to has been comfortable with the legal basis.

Ms. JACKSON LEE. So as you have listened to Members of Congress, what is your commitment to coming back to us, working with the Department of Justice to address and to help change what we are presently dealing with?

Mr. JAMES COLE. Well, I can tell you is that the President's commitment, and we work for the President, and we are there to fulfill that commitment to try and change 215 on the telephony metadata as we know it and find another way where the government does not hold—

Ms. JACKSON LEE. So you have a commitment based upon the President's representation to come back and look at a better way of handling the trolling of Americans' data that may not be relevant.

Mr. JAMES COLE. We are looking for another way that will accomplish what we have been accomplishing under 215 as best we can and not involve the government holding the metadata.

Mr. GOODLATTE. You may want to use an adjoining microphone if you can get to one.

Ms. JACKSON LEE. Can you all hear me?

VOICE. No.

Ms. JACKSON LEE. You cannot hear?

VOICE. No, we cannot hear. We cannot hear.

Ms. JACKSON LEE. Testing, testing. Can you hear me now? Thank you. That is what happens when you start trolling and collecting data. [Laughter.]

I am sorry. Mr. Chairman, will I be indulged my time? Thank you.

Mr. GOODLATTE. No. [Laughter.]

Ms. JACKSON LEE. I did not hear that. [Laughter.]

Please indulge me, Mr. Chairman. Technological troubles here.

In the report, there was a comment, "The idea of balancing has an element of truth, but it is also inadequate and misleading." Mr. Swire, when we are talking about security and privacy, what do you think that means? And I am going to go ahead to my good friend over the Oversight Board, Mr. Medine. Thank you very much. I think it is going to be in your hands to be as aggressive as you possibly can be, and I want you to give me your interpretation of two things: the question of relevance and the question of the importance of having an advocacy for the people in the FISA Court. Mr. Swire?

Mr. SWIRE. The review group supported having an advocate, exactly. Had to have amicus versus party, so there are some tricky legal issues. And we did not make a legal decision about our view on the word "relevance."

Mr. GOODLATTE. Without objection, the gentlewoman will be granted an additional minute on her time.

Ms. JACKSON LEE. Thank you. Mr. Medine, could you answer the question as extensively as you can on that? Thank you, and thank you for your service.

Mr. MEDINE. You are welcome. Nice to see you again. On relevance, again, the majority of the board is concerned about the almost unlimited scope of relevance, and I think that we have heard questioning earlier today that it encompasses Members of Congress, the executive branch, and also dissidents, and protestors, and religious organizations. And so we think that it is written too broadly under this program, and there should be much more targeted requests for information, which can be legitimately done without the need to gather bulk information. Right now, relevance is almost whatever the government can pull in and analyze as the scope of relevance. And we think that there needs to be a narrower concept to protect privacy and civil liberties.

I mean, with regard to having an advocate in the Foreign Intelligence Surveillance Court, I think it is critical that there be an

other voice to respond to the government. As Mr. Swire mentioned earlier, if all the briefing that we have done on this program could have been presented to the Court, the Court could have made a more balanced decision. It was not until 2013 that the Court issued its first opinion regarding the legality of this program. We think in the adversary process, the Court would have carefully considered all the arguments pro and con, rendered its decision. And we also recommend that there be an opportunity for appeal to the FISCR, which is the Court of Appeals, and ultimately to the Supreme Court to resolve these important statutory and constitutional issues.

Ms. JACKSON LEE. Let me just indicate that in addition as an aside, the President put on the record that he thought that we needed to haul in, from another perspective, the contractors dealing with the vetting of all those who work in this area just as a protection. If we are so interested in trolling Americans, we need to also make sure that our contractors or our workers in the intelligence are fully vetted. Just in your own mindset, do you think the government can handle its vetting and narrow the sort of outside contractors that are doing that now?

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

Mr. MEDINE. And actually with due respect, that is not on our board's domain, but maybe the deputy attorney general might be able to address that.

Mr. GOODLATTE. Mr. Cole?

Mr. JAMES COLE. I am sorry, could you repeat the question?

Ms. JACKSON LEE. The President indicated that maybe we should reduce our outside contractors that are vetting those who have access to our security data. Would you be also in agreement with that approach?

Mr. JAMES COLE. I think we need to make sure that we take care of the insider threat. That has been something the President has talked about. We need to make sure that people who work for the government are suitable and have been vetted properly. We have always thought that from both a cost perspective and a security perspective, the more we can reduce contractors the better. But as we hire contractors, we hire employees as well. They just need to be vetted very well when they are given very sensitive and classified positions.

Ms. JACKSON LEE. I thank the Chairman, and I thank the witness. I yield back.

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

Mr. FORBES. Mr. Chairman, thank you, and, gentlemen, thank you so much for taking your time and your expertise to be here with us today.

Mr. Cole, it is my understanding that the review group's recommendation was that the use of private organizations to collect and store bulk telephony metadata should be implemented only if expressly authorized by the Congress. My question to you is not for the word "should," but we have watched the President when he was all in on healthcare and promised us all we could keep our insurance if we wanted it. It later changed. We listened to his words

say he could not change immigration laws without Congress. He changed. We listened to him about military force without congressional permission. He changed. We heard his State of the Union where he said he had a pen and he had a phone regardless of what Congress did.

My question to you is, in your professional opinion, do you believe that the President of the United States has the authority to use private organizations to collect and store bulk telephony metadata without the express approval of the Congress of the United States?

Mr. JAMES COLE. Congressman, that is an issue that is probably part of the mix that we are looking at—

Mr. FORBES. My question to you is do you have it, and we have seen you kind of slide off of the answers to the questions today. I am not asking you what ultimately would be determined. I am talking about your professional opinion today sitting there, is it your professional opinion that the President has authority or does not have the authority?

Mr. JAMES COLE. I am going to give you a lawyer's opinion.

Mr. FORBES. That is what we hired you for.

Mr. JAMES COLE. Okay. There may be ways we could find for him either through contract or executive order to do it. It could also be done through legislation. There may be a number of different ways that you can—

Mr. FORBES. So then basically if this Congress wants to avoid that, we had better to get to work and expressly prohibit the President from doing that, because he could do that the same way he is threatening to do certain other things.

Mr. JAMES COLE. I think the President has clearly indicated he is looking forward to working with Congress to achieve a lot of these things.

Mr. FORBES. Yes, but he also said that "working" means if Congress does not do what he says, he has got the pen, he will do it anyway.

Mr. Swire, if I could ask you, and I appreciate your comments about wanting to have specific and targeted collection, I believe, as opposed to bulk collection. Is that a fair representation?

Mr. SWIRE. Our report emphasizes the usefulness of the targeted collection.

Mr. FORBES. Mr. Swire, I represent a lot of people. We have a lot of communications from groups in the country who believe that even with specific and targeted collection, they are concerned because they have seen what the IRS, the Justice Department, and other agencies have done in targeting conservative groups and individuals in the faith community. What would you suggest that we do to try to protect those groups, because it is not going to be much consolation to them to say we can do specific and targeted collection if they have seen that they have been specifically targeted already by this Administration. Any suggestions that your group might have for that?

Mr. SWIRE. Well, we have a couple of statements or conclusions in our report that I think are relevant to that. One is we found no evidence that there was in these surveillance activities any political targeting of Americans. So this is not where they are picking phone

numbers based on politics or faith groups or whatever, and that includes people with a lot of experience in the intelligence community who are on our group.

And the second thing is we found a very substantial compliance effort, much of which has been built up over the last 4 or 5 years, and so, a very earnest effort to comply with these rules, and so, in both of those cases, not political targeting and following the rules. We were distinctly heartened by what we found as we went through our——

Mr. FORBES. Well, let me ask you this because it is also my understanding that your group did not conclude that the Section 215 Bulk Telephony Metadata Collection Program had been operating illegally with respect to these statutes or the Constitution. You further found no allegations in the report of abuse of this authority by members of the law enforcement and intelligence community. You further found that there was no allegation that the National Security Letter Program operated illegally, that no allegation of misuse or abuse by the law enforcement or intelligence community was made in the report. And yet you made substantial recommendations to change them.

So as to these groups who are very concerned about that, what would be your recommendations to protect the interests of those groups?

Mr. SWIRE. Congressman, we were interested in traditional American checks and balances and having the different branches of government doing their jobs, and going forward having within the executive branch bulk collection held in secret without judicial or congressional participation in that. We thought that was not a good way to go. And so, for the bulk collection, we recommended being very skeptical of the bulk collection, and we recommended having judicial safeguards in instances where it went forward as a way to maintain these sorts of checks and balances.

Mr. FORBES. Good. Mr. Chairman, thank you, and I yield back the balance of my time.

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

Mr. COHEN. Thank you, Mr. Chairman. Would it be improper for me to recognize the Delta Sigma Thetas, who are here today?

Mr. GOODLATTE. I think it would be very proper.

Mr. COHEN. Well, welcome. They are here and a great sorority that does a lot of good for our country. Thank you, Mr. Chairman.

Mr. Cole, before we talk about the NSA, which is indeed the subject of this, I want to go to another subject and give you some praise. You recently spoke before the New York State Bar Association, and I was so encouraged by your speech. It was about criminal justice issues that relate to this Committee as well.

And you indicated that the President is open to using his commutation power in a much more manifest way than he has in the past. You called on attorneys to come forward and try to help people with clemency requests, and that notice will be given to individuals in prison maybe with mandatory minimums that are unjust, people who had no violence in their background, may be first-time offenders who were sentenced for long times who judges said, I

hate this, but I have to. And you give them notice. I thank you for that. And you and the President deserve praise for this effort.

It is my opinion that the President can leave a legacy for justice that could be unmatched if he used that power that you have discussed, and I am sure you have worked with him on, in a manifold way. There are thousands of people that need justice and should receive it, and this is probably the only way they can. I know he is waiting on the legislature, the Congress, to act. I think he should probably act on his own.

The FISA Court is appointed entirely by the Chief Justice, and I have great regard for the Chief Justice. He and I are friends. But I do not know that that makes for a good balance of power on the FISA Court. His appointments, and it may just folks he kind of knows, but 10 of the 11 judges who have been currently sitting were appointed by Republican presidents. And it may just be how that happened, you know, but it could be that there is a certain ideological link there, and it should be changed.

I would think that the FISA Court ought to have a wide expanse of ideology, and some people are more skeptical of the government's perspective and more inclined toward looking toward civil liberties. I do not know that we have that in that Court. Does it trouble you, Mr. Cole, that the Chief Justice names every single of those people?

Mr. JAMES COLE. Congressman, I do not think it particularly troubles me. I think we have seen judges throughout the Court, and everyone that I have dealt with at the Court has just been straight down on the facts and the law, and making sure that they honored civil liberties. We have seen released any number of opinions of judges when there were compliance problems, and the judges coming down hard on the Justice Department and on NSA to make sure that we fix them, and to make sure that we protected people's privacy and people's civil liberties.

So I think you have got a good group of judges that have been there over the years.

Mr. COHEN. Let me ask you this. You said the judges down the line. Do they not almost unanimously agree? How many times have you seen a split opinion?

Mr. JAMES COLE. Well, there is only one judge that looks at a FISA application, so you would not have the split. And what has been discussed any number of times is that we present these applications to the FISA Court. They go to the staff. They go to the judges. Sometimes the judges will kick them back, and they will say you need more information about this, or, I do not find you have met the standard on that. And sometimes we will provide more information, other times we will withdraw it.

So the statistics of how many have been granted that were submitted are a little bit misleading because it does not take into account some of the dialogue that goes on between the Justice Department and the Court that results in the applications being withdrawn.

Mr. COHEN. And they do not sit en banc?

Mr. JAMES COLE. No. There is a review group, an appellate group, which is 3 judges, and they will sit as 3 judges.

Mr. COHEN. How often are they split?

Mr. JAMES COLE. I would have to go back and look. I do not really know the statistics off the top of my head.

Mr. COHEN. Would "rare" be a good term to apply to their outcomes?

Mr. JAMES COLE. It might be, but I just do not know the statistics.

Mr. COHEN. Did the President not come out for some type of change and think that maybe each of the judges should rotate and pick somebody?

Mr. JAMES COLE. I think that is one of the things that has been proposed in some of the pieces of legislation. I think generally as long as we get good judges who are there and we do not inject politics into it, I think we are happy as long as we have got judges that are there, and that fully staff the——

Mr. COHEN. I understand not getting politics in it, but the Pope is politics. I mean, everything is politics. The justices are politics. Would it be wrong if the congressional leaders, equal Democrat and Republican, suggested some people to the judges and they pick from that group so there would be more of a check and balance on the choices?

Mr. JAMES COLE. I think there are any number of models that might be workable in this regard to try and find a way to staff that Court. We are more than happy to work with the Congress on trying to find good ways to do that.

Mr. COHEN. Thank you. Thank you. I appreciate it, and I thank the Chairman for his indulgence in recognizing the greatest group of ladies in red since the Biograph Theater.

Mr. GOODLATTE. That is an interesting comparison. [Laughter.]

The gentleman from Texas, Mr. Gohmert, is recognized for 5 minutes.

Mr. GOHMERT. Thank you, Mr. Chairman, and I appreciate the witnesses being here. Mr. Cole, if you had been testifying in front of this Committee back before Edward Snowden took the documents he did, and you were asked if it was possible that any contractor would be able to access and take the documents that we now know he did, based on your comment that nobody can access these documents without proper cause, back then you would have said nobody could access those documents without proper cause and authorization, would you not?

Mr. JAMES COLE. I think what I was saying, Congressman, is under the law and the court order nobody is allowed to do that without violating the——

Mr. GOHMERT. So you are making a distinction that it is possible that they could access those documents, just like Edward Snowden did, correct?

Mr. JAMES COLE. Things are possible. You know, this is something that we would like to nail down, but exactly what——

Mr. GOHMERT. Well, you answered my question on that. The answer, though, accurately would be that not only Members of Congress, but anybody is subject to having that data looked at or accessed by someone who may not follow the law.

But let me tell all of you witnesses, in my first term we went through the process of debating whether or not we were going to renew the PATRIOT Act, and 215 was of particular importance.

And I asked the question, for example, you know, under 215 where it says that you would only access these documents to protect against international terrorism or clandestine intelligence activities. I said what is "clandestine intelligence activities," and I was assured that since we are talking about international terrorism, our intelligence activities have to do with foreigners, and we were assured that was the case. And Chairman Sensenbrenner at the time assured that he had been assured that that was the case, and that is why he was initially totally opposed to any more sunsets that I fought so hard for and we did finally get in here. And now we find out those representations were not accurate.

And let me tell you something else that concerns me is, yes, I know the Constitution and the Fourth Amendment does say that we have the right to be secure in our persons, houses, papers, and effects against unreasonable searches and seizures. And that is not to be violated, and no warrants are to be issued but upon probable cause supported by oath or affirmation, particularly describing places, persons, or things to be seized.

And when we saw the copy of this order from the FISA Court, all those assurances from my terms as a freshman went out the window because you have a judge, based on this before the FISA Court, who just says give all call detail records, telephony metadata. And then it defines telephony metadata basically as everything that you would desire about information and calls being made.

I cannot find in that order any particularity or any specificity as at least appellate courts have always required. So this causes me great concerns without regard for discussion about Snowden, the fact that we had information provided to us that were misrepresentations of what was being done by this government.

So let me also ask, since we have been told repeatedly how critical this FISA ability under 215 is, we have been told that all of these different plots have been foiled. And when it comes right down to it, it appears it was basically a subway bombing, and there are articles that indicate that, well, gee, they intercepted some information, so they went back and got all the phone logs for communication. But you do not need FISA Court, you do not need 215 when you have probable cause from a terrorist, a known terrorist, calling an American citizen. You would be able to get a warrant for that, would you not? I ask all of you.

Mr. JAMES COLE. Well, I think there are a couple of issues there.

Mr. GOHMERT. Well, the question is, you would be able to get a warrant if you showed that a known foreign terrorist made calls to an American citizens. You could go in and get basically any court to grant a warrant to get those logs, could you not?

Mr. JAMES COLE. It depends on whether you get it under FISA, in which case you would have to show that it was an agent of a foreign power or a terrorist or an intelligence—

Mr. GOHMERT. That was part of my question, a known foreign terrorist.

Mr. JAMES COLE. Right. You may well be able to do that.

Mr. GOHMERT. Mr. Swire, do you think we could get that?

Mr. SWIRE. Congressman, to date the courts have not held that that was a search, so they say there is not a Fourth Amendment constitutional protection in the metadata. And we recommend——

Mr. GOHMERT. In other words, you do not need 215 to get that, do you?

Mr. SWIRE. Well, you need some statutory basis to require the companies to turn over the data, but it is not a constitutional protection. It is statutory right now.

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

Mr. GOHMERT. If I could get an answer from our last witness.

Mr. MEDINE. Again, we agree that under Supreme Court law there is not a constitutional Fourth Amendment issue, but we also do believe this information could be obtained through other authorities, a warrant, subpoena, or possibly national security——

Mr. GOHMERT. Without 215?

Mr. MEDINE. Yes.

Mr. GOHMERT. Okay. Thank you very much.

Mr. JAMES COLE [continuing]. Would only be required for the listening of the call, not for the data.

Mr. GOHMERT. Thank you. I yield back.

Mr. GOODLATTE. The Chair recognizes the gentleman from Georgia, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman. The revelation that U.S. intelligence agencies were collecting telephone and email metadata on foreign to domestic, domestic to foreign, as well as domestic to domestic communications caused an uproar. This disclosure has given rise to the suspicion that intel agencies have been spying on Americans. The intel community denies spying on Americans, and states that the purpose of the metadata collection is to protect Americans from terrorist attacks like 9/11.

Now, in the wake of the death of Osama bin Laden, who was one of the 5 top leaders of Al-Qaeda, and, in fact, 4 of the 5 top leaders of Al-Qaeda, including Osama bin Laden, are no longer living. And Al-Qaeda has, thus, decentralized with affiliates worldwide acting independently to establish an Islamic state through violence. These groups all share a Salafi jihadist ideology, which is that violence is the only pathway to achieving a world governed by what Al-Qaeda calls true Islam. Those groups are working toward that goal.

Given the nature of the Al-Qaeda threat, or actually the Salafi jihadist threat, given the nature of that threat, and also assuming that those organizations use cell phones, chat rooms, emails, Facebook, and Twitter to conduct their operations, do you believe that that the universal data collection by U.S. intel agencies has the potential to disrupt Al-Qaeda's operations throughout the world? And secondly, and I think we already have answers to this from two of you, is metadata actually private information, and, if so, who does the information belong to? Is it the customer or is the service provider? Starting with you, Mr. Cole.

Mr. JAMES COLE. Congressman Johnson, I think that the 215 program is a tool, and it is a tool that is helpful. It is not going to solve all the problems all on its own in finding terrorists. It is one piece of what we use as a number of tools to try and find terrorists before they attack the country. In and of itself, it has some utility, but I do not think we should overstate the utility of it, but

it is helpful, and I think it is something that we have determined that we do not want to give up that capability because it is helpful.

Mr. JOHNSON. All right. Let me go to——

Mr. SWIRE. Congressman, yes. One of the major themes of our reports is that we have to use our communication system for multiple goals. We have to use it to capture dangerous people and find them. It is the same communication system we used for commerce and we use for free speech and all these other things.

And so, our report tried to figure out ways to be really good at finding the threats and also protect these other goals. People are all struggling with how to build that, and it is a big challenge.

Mr. MEDINE. Congressman, you raised the question about whether Americans were improperly being spied on. We did not find any evidence of that, but the mere fact that people believe that could be affects their behavior, their association, their speech rights. And that is one of the major reasons we recommend, the majority of the board, to not continue the 215 bulk collection program because there are other methods that are more particularized to gather this information without storing everyone's phone records.

Mr. JOHNSON. How would that affect the ability of our intelligence agencies to protect Americans from a threat like 9/11?

Mr. MEDINE. The majority believes that the ability to collect this information could be transferred to the providers instead of maintained in a bulk collection and maintain the same level of efficiency.

Mr. JOHNSON. Okay. What would cause the private providers to have adequate security as to who in their operations had access to the, for lack of a better term, private information, the private metadata? What are the consequences? What are the ramifications of that?

Mr. MEDINE. Well, under current law, the Federal Communications Commission requires telephone providers to maintain those records for 18 months, and also maintain the security of that information. So that is current law, and that happens every day that the providers maintain that information. What we are saying is instead of having them dump all of their information into a government database, it should be kept with them and obtained from them on a case by case basis.

Mr. JOHNSON. Anyone else?

Mr. JAMES COLE. I think one important point, and it goes to a question Mr. Gohmert asked, is that there are lots of security protections in lots of different databases. You can get around them every now and again. You can get around them in a government database. You can get around them in a provider's database. People can hack in. We tried to put in protections and legal restrictions to prevent that from happening, but nothing is completely fool-proof.

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

Mr. JOHNSON. Thank you.

Mr. GOODLATTE. The gentleman from Ohio, Mr. Jordan, is recognized for 5 minutes.

Mr. JORDAN. Thank you, Mr. Chairman. Mr. Cole, are you familiar with the name Barbara Bosserman?

Mr. JAMES COLE. I have heard that name, yes.

Mr. JORDAN. Is she an attorney who works at the Justice Department?

Mr. JAMES COLE. She is.

Mr. JORDAN. And she is part of the team that is investigating the targeting of conservative groups by the Internal Revenue Service, is that correct?

Mr. JAMES COLE. She is a member of that team.

Mr. JORDAN. A member of that team. I would dispute that and say she is leading the team, but I will take your word for it. Now, in the last 5 days, Mr. Cole, you have sent me two letters, one January 30th, last week, one just yesterday, where we had invited Ms. Bosserman to come testify in front of the Oversight Committee, and you sent me two letters saying that she is not going to come. And I counted them up. In these two letters, I think it is 7 different times you say this is an ongoing investigation, and that is why Ms. Bosserman cannot come to our Committee and testify. Do you recall those two letters you sent me, Mr. Cole?

Mr. JAMES COLE. I do.

Mr. JORDAN. Yes, and you signed both of them?

Mr. JAMES COLE. I did.

Mr. JORDAN. And you referenced many times ongoing an investigation?

Mr. JAMES COLE. Yes, it is.

Mr. JORDAN. So here is my question. How can the President of the United States go on TV on Superbowl Sunday and say that there is not a smidgen of corruption in this investigation, not a smidgen of corruption in the IRS with how they targeted conservative groups? How can he be so sure when it is an ongoing investigation, something you told me 7 times in two letters in 5 days? How can the President make that statement?

Mr. JAMES COLE. Congressman, I think you should probably address that question to the White House.

Mr. JORDAN. Did you brief the President on the status of this investigation?

Mr. JAMES COLE. I have not.

Mr. JORDAN. Do you know if the Attorney General has briefed the President on the status of this investigation?

Mr. JAMES COLE. Not that I am aware of.

Mr. JORDAN. Do you know if Ms. Bosserman, part of this team, who is investigating the targeting of conservative groups, do you know if she has talked to the President?

Mr. JAMES COLE. Generally, the Justice Department does not brief the White House on—

Mr. JORDAN. So how is the President so sure?

Mr. JAMES COLE. Congressman, I am not in a position to answer—

Mr. JORDAN. He did not say I do not think there is, there probably is not, nothing seems to point that way. He said there is not a smidgen of corruption. He was emphatic. He was dogmatic. He knew for certain. And no one has briefed him?

Mr. JAMES COLE. No one I am aware of, Congressman.

Mr. JORDAN. So you know what I think, Mr. Cole? I mean, you know, just a country boy from Ohio. You know what I think? I think the President is so emphatic and he knows for certain be-

cause his person is running the investigation, because Ms. Bosserman gave \$6,750 to the Obama campaign and to the Democratic National Committee, and she is heading up the investigation. I think the President is so confident because he knows who is leading the investigation. And that is a concern not just for me, and Members of this Committee, and Members of the Oversight Committee, but, more importantly, the American people who have to deal with the IRS every single year. Does that raise any concerns with you, Mr. Cole?

Mr. JAMES COLE. Congressman, Ms. Bosserman is a member of the team. She is not leading this investigation.

Mr. JORDAN. How was the team picked?

Mr. JAMES COLE. The team was assigned in normal course by career prosecutors. It includes the FBI, the IG for the——

Mr. JORDAN. How many members are on the team? This is something the FBI has refused to answer for the last year because I have been asking the question. They have refused to meet with us. They initially said they were going to meet with us. Then they talked with lawyers of the Justice Department and they said, no, we are going to rescind that offer, Mr. Jordan. We are not going to come meet with you. So how was the team put together, and how many members are on the team?

Mr. JAMES COLE. Congressman, off the top of my head, I have no idea how many members are on that team. And generally, we do not brief elected officials on ongoing investigations. That is a standard——

Mr. JORDAN. But again, we are not asking for a full briefing. We understand it is ongoing. We would just like to know who is heading it up. How many agents have you assigned? How many lawyers have you assigned? Who is heading it up? If it is not Ms. Bosserman as I think it is, who actually does head it up?

Mr. JOHNSON. Mr. Chairman, parliamentary inquiry, please?

Mr. GOODLATTE. The gentleman will state his parliamentary inquiry.

Mr. JOHNSON. Is it proper for a Member of the Committee to question a witness about a matter that is not relevant to the matter that the hearing has been noted for?

Mr. GOODLATTE. It is proper, and it has been done many times before in this hearing, this Committee.

Mr. JORDAN. I would just point out——

Mr. GOODLATTE. The gentleman will continue.

Mr. JORDAN. Mr. Cole sent me two letters in the last 5 days. It is a pretty important issue. And when you appoint someone or you assign someone who gave \$6,750 to the very person who—the President could be a potential target in this investigation, and yet the person leading the investigation gave \$6,000 to his campaign? She has got a financial stake in an outcome, a specific outcome. And Mr. Cole says “normal course of duty.” We have got 10,000 lawyers at the Justice Department, and, oh, it just happened to work out that Ms. Bosserman heads up the team. Really?

Mr. JAMES COLE. She is not heading up the team, Congressman. There are many people——

Mr. JORDAN. It is not what the witnesses we have talked to have said. Mr. Cole said she asked all the questions when they have been interviewed.

Mr. JAMES COLE. She is not the head of the team, and there are many people who will be making the decision as to what to do with this case based on the evidence, the facts, and the law, just like every single investigation the Department of Justice does.

Mr. JORDAN. Okay. All I know is the President said——

Mr. JAMES COLE. And including FBI agents——

Mr. JORDAN. All I know is the President said there is not a smidgen of corruption.

Mr. JAMES COLE [continuing]. Including eight——

Mr. JORDAN. The President has already reached a decision.

Mr. JAMES COLE [continuing]. And the Inspector General's office.

Mr. JORDAN. Mr. Chairman, if I could real quickly. I sent my letters to Ms. Bosserman. She did not write me back. You did, Mr. James Cole. Did you talk to her about coming to testify? Did you tell her not to come testify?

Mr. JAMES COLE. I did not tell her not to testify.

Mr. JORDAN. Did you have any conversation with Ms. Bosserman about the request I gave her to come testify in front of our Committee?

Mr. JAMES COLE. Congressman, there is a standard——

Mr. JORDAN. No, no, I did not ask that. I said did you talk to Ms. Bosserman about that specific request I sent to her. My letter was to her, and I got responses back from you.

Mr. JAMES COLE. And I am answering your question, Congressman. There is a very long-held policy in the Department of Justice that line attorneys are not subjected to the questioning by Members of Congress.

Mr. JORDAN. Did you ask her if she wanted to testify?

Mr. JAMES COLE. If I may finish, Congressman, they are not subjected to questioning——

Mr. JOHNSON. Regular order, Mr. Chairman.

Mr. JAMES COLE [continuing]. By Members of Congress, and we do not send people up here to talk about ongoing investigations. We have done that in every Administration.

Mr. JORDAN. But you are not answering my question. Answer my question.

Mr. GOODLATTE. The time of the gentleman has expired. The gentleman may answer the question.

Mr. JAMES COLE. I think I have answered it.

Mr. JORDAN. I do not think you have.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from California, Ms. Chu, for 5 minutes.

Ms. CHU. Mr. Medine, the PCLOB's report urges Congress to enact legislation that would allow the FISA Court to seek independent views from the special advocates. These advocates would step in where there are matters involving interpretation of the scope of surveillance authorities or when broad collection programs are involved.

The report stresses that the Court should have discretion as to when these advocates step in. But is it advisable for the Courts to have that discretion? Is it possible that the Courts may leave the

advocates out of the process when such important questions are before them?

Mr. MEDINE. First, we do think it is important for advocates to be involved in issues of new technology and new legal developments. In terms of how they get involved, our feeling was that there are cases where they should certainly, obviously, be involved such as in a novel program that is being proposed. But there may be other cases which may not seem as novel on its face, but the judge is aware of the facts and circumstances, and wants to bring them in as well.

So we felt it was appropriate to give the judge discretion as to when to involve the advocate, but we also called for reporting. And under the Court rules, Rule 11, the government is required to indicate to the Court if it is making an application that involves a new technology or a new legal issue. And so, what we have asked is that there be reporting of every Rule 11 case, and how many of those instances has a special advocate been appointed, and that way there can be oversight of the court process of appointment.

But we do, again, think that it is appropriate for the judges to maintain some discretion.

Ms. CHU. Would that report also include times when special advocates were not included, though?

Mr. MEDINE. Right. How many times has Rule 11 application been forwarded, and how many of those instances has an advocate been appointed or not appointed? So again, if it is a significant case, one would assume it is likely that they would be, but there will be accountability to the public by the Court as to when they make those appointments.

Ms. CHU. Now, you also advocate for the ability of the special advocates to request appellate review of court rulings. Why did you recommend this, and how would this strengthen privacy protections?

Mr. MEDINE. In our American judicial system, we have a process by which district judges get reviewed by appellate bodies and ultimately the Supreme Court. We think that works effectively to have a dispassionate review by 3 judges at the appellate level and the 9 justices at the Supreme Court. And we think that the FISA Court process would be improved by encouraging that development.

And so, we would like to empower the advocate to bring to the FISA Court of Review, which is their appellate body, adverse decisions to the advocate and in favor of the government so that there could be greater review. Again, much as there would be in any case in the District Court system.

Ms. CHU. Mr. Swire, many of us think that, of course, the language in the statute in which the Section 215 bulk collection of metadata is broad, but that the government's interpretation of the relevant standard is even broader. The review group proposed a standard that the Court may only issue a 215 order if the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation. And like a subpoena, the order has reasonable and focused scope and breadth.

Can you tell us how this standard would narrow the government's inquiry so we could protect the American public in terms of its privacy interests? And how is this standard an improvement?

Mr. SWIRE. Well, one change is that it would be a judge involved, and that is something that President Obama has recently said they are going to work with the FISA Court to do. A next change is to try to have these narrowing of scopes so that the bulk collection by the government prior to judicial looking at it would not occur. So it would be a narrowing in that respect as well.

Ms. CHU. Also, the review group recognizes that intelligence programs, some, should remain secret. But you are also proposing that a program should be kept secret from the American public only if the program serves a compelling governmental interest, and if the efficacy of the program would be substantially impaired if our enemies were to know of its existence.

If this proposed standard were in existence today, would the government have been compelled to disclose Section 215 bulk collection program? How is your standard an improvement over what we have today?

Mr. SWIRE. Right. Well, our recommendation 11 talks about a compelling government interest, and there would be a process within the government. When that process happens, we emphasized having not only intelligence perspectives, but, for instance, economic perspectives, civil liberties perspectives, as part of a sort of comprehensive review.

And I also note that on bulk collection, the President has asked John Podesta to lead a process for private and public sector bulk data which is supposed to come back with additional recommendations about bulk data within, I think, 60 days.

Ms. CHU. Thank you. I yield back.

Mr. GOODLATTE. The time of the gentlewoman has expired. The Chair recognizes the gentleman from Texas, Mr. Poe, for 5 minutes.

Mr. POE. Thank you, Mr. Chairman. I have great concerns about this whole process. This is reminiscent to me of the old-fashioned star chamber where courts met in secret, issued their verdicts and edicts in secret. No one knew what happened until the sentence was carried out.

I also spent some time in the Soviet Union when it was the Soviet Union. Everything I did and all the citizens did was spied on by the Soviets. And here we are in 2014 trying to justify what I think is spying on American citizens.

Mr. Cole, I have a question for you, but I want to quote Mr. Medine in his testimony. He said, "Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation." Mr. Cole, name one criminal case that has been filed based upon this vast surveillance and metadata collection.

Mr. JAMES COLE. Congressman, I think there was one which was a material support case that was filed based on the 215 metadata where we were able to identify someone. And again, as I have said, this is not—

Mr. POE. Reclaiming my time, as you know our time is limited. So how many criminal cases have been filed based upon this massive seizure?

Mr. JAMES COLE. Well, the criminal support statute is a criminal—

Mr. POE. I understand. My question is how many.

Mr. JAMES COLE. I do not know off the top of my head, Congressman.

Mr. POE. There is one.

Mr. JAMES COLE. There may be one.

Mr. POE. There may be one. So we have this vast metadata collection on Americans, and the reason is, oh, we have to seize this information or we are going to all die because of terrorists. And you are telling me as a former prosecutor—I am a former judge and prosecutor—all this information has collected one criminal case, is that what you are saying, that you know of?

Mr. JAMES COLE. Well, Congressman, the point of this is not necessarily to make criminal cases.

Mr. POE. I am not asking you—

Mr. JAMES COLE. The point of it is to gather intelligence.

Mr. POE. Reclaiming my time. My question is, one criminal case. That is all you can show for criminal cases being filed against individuals, right?

Mr. JAMES COLE. I think that is the correct number, but I would have to go back and check to be sure.

Mr. POE. It may not even be one.

Mr. JAMES COLE. The point of the statute is not to do criminal investigations. The point of the statute is to do foreign intelligence investigations.

Mr. POE. But the collection is on American citizens. When a warrant is signed—I signed a lot of warrants, Fourth Amendment. You know, I actually believe in the Fourth Amendment. A warrant is served. Police officers go out and investigate. They return the warrant, and it is filed as a public document in State courts and in Federal courts. But when collection on American citizens of their information, this is not made public to them. They never know that this information was seized from them, do they?

Mr. JAMES COLE. Well, as I think even the PCLOB and the President's review group have noted, the Fourth Amendment does not cover the collection of metadata under the current law. So it would not have those requirements.

Mr. POE. I know that is the current law, but that is not my question. My question is, the information is seized from them. They do not know that their personal information was seized by the Federal Government. They do not know that. They are not protected under our current statute under the PATRIOT Act. Is that correct or not?

Mr. JAMES COLE. The information does not come from them. It comes from the companies that they have phone service with. And, no, they are not informed directly that that metadata from those phone companies has been collected.

Mr. POE. Do you have a problem with that information being seized on Americans through a third party and Americans never know that that they are the subject to this metadata collection? I

mean, do you have a personal problem with that, or do you think that is okay, the government ought to do that?

Mr. JAMES COLE. These are the issues we grapple with every day, Congressman, as far as trying to do national security investigations and trying to protect people's civil liberties. And we take leads from the Court as to the scope of the Fourth Amendment and where people's reasonable expectations of privacy are. And these are difficult lines to deal with, and just what we are doing right now is trying to find where that right line is.

Mr. POE. Well, I think it is an invasion of personal privacy, and it is justified on the idea that we have got to capture these terrorists. And the evidence, based on what you have told me, is all of this collection has resulted in one bad guy having criminal charges filed him. I think that is a bit over reaching to justify this massive collection on individuals' personal privacy. That is just my opinion. I yield back to the Chair.

Mr. GOODLATTE. The Chair thanks the gentleman, and recognizes the gentleman from Florida, Mr. Deutch, for 5 minutes.

Mr. DEUTCH. Thank you, Mr. Chairman. General Cole, I am going to come at the judge's line of questioning from a slightly different angle, but I think trying to get at the same point. In a September letter to NSA employees, General Alexander wrote that "The Agency has contributed to keeping the U.S. and its allies safe from 54 terrorist plots," and that 54 terrorist plots has been repeated on several occasions.

Last week in testimony before the Senate, there were some officials from the Administration who suggested that terrorist plots thwarted is not the appropriate metric for evaluating the effectiveness of the program. And I would just like to understand has the argument changed, and if it has, why should we now apply a different metric to determine the success of this program if it is not criminal prosecutions and if it is not terrorist plots thwarted?

Mr. JAMES COLE. A couple of things, Congressman. The 54 number, as I recalled it, was both 702 and 215. And the bulk of it, frankly, was 702 coverage. And that is a very, very valuable program, and, frankly, probably more valuable than 215.

215 has a use, and it has a number of different uses. They are not as dramatic as 702, but they provide pieces of a puzzle. They provide tips and leads that allow us to then go and investigate and then gather other information. And that is really the value of 215.

Mr. DEUTCH. But even if that 54 number that had been used does not apply primarily to the 215 program, you are telling me that the notion of terrorist plots thwarted even as it applies to this program is not the metric we should be using.

Mr. JAMES COLE. It is not the only metric. Certainly it is a great metric, but I do not think it is the only metric we should be using. I think if we are gaining evidence that is valuable to us in doing investigations that help keep the country safe, that is a valuable metric.

Mr. DEUTCH. Right. And Mr. Medine had told us earlier in his testimony, their first recommendation was to end the 215 program, and said that whatever successes you are referring to could have been replicated in other ways. Mr. Medine, is that right? And how could that have been accomplished?

Mr. MEDINE. Well, there are other authorities—grand jury subpoenas, search warrants, national security letters—that allow for access to the information without the need to collect bulk records.

Mr. DEUTCH. And would have accomplished all of the same things that the 215 program does successfully.

Mr. MEDINE. Substantially. Even the material support we talked about, but in many other cases. We looked at a lot of different metrics and based our recommendations on that.

Mr. DEUTCH. Right. And when we talked about the suggestions going forward, the idea of moving this information away from the government, Mr. Swire, you had said that when we are talking about metadata held by or the suggestion of metadata to be held by private providers or private third parties instead of by the government. And, Mr. Cole, I think you said people are thinking outside the box about how to store this information.

My question is this. The metadata that is being collected that you are comfortable moving to the private parties puts that metadata, does it not, and here is what I am concerned about. It puts the metadata that Mr. Medine and others believes is unnecessary to gather because it does not accomplish what is necessary. We can do it in other ways without intruding on people's civil liberties. But if it is stored by private contractors, private parties, it is at risk then, is it not, of being stored with all of the other data, dramatically more intrusive personal data, that we turn over to private parties regularly when we go on the internet, regularly.

It puts it in the same place with all of the information that we have been assured time and time again today this program does not do in terms of intruding on the specifics of our emails and the specifics of what we do on the internet, et cetera. It puts it all together. Why should that not be a concern of ours?

Mr. SWIRE. Congressman, I think part of the question is are we creating extra risk as we shift things around—

Mr. DEUTCH. Exactly right.

Mr. SWIRE [continuing]. And find ways to shift things around. When it comes to phone company telephone records, as has been mentioned earlier, the Federal Communications Commission already requires it to be there for 18 months. Phone companies have been holding phone company data for an awfully long time.

Mr. DEUTCH. Right, and, no, I understand, and that point has been made earlier. But there was another suggestion made. I think one of your suggestions was that we may need to have some other party. We may need to look outside of the box. My concern is that we are creating more risk than already exists in the program that we do not even need.

Mr. SWIRE. Right. And what we said, and our entire report is prefaced by a transmittal letter saying this is our best effort in the time we had to come up with things. And one of the suggestions we had was in addition to possibly the phone companies, maybe a private sector entity could hold this with the right sorts of safeguards, and that we should look for ways to transition.

We did not say we had the magic answer. Each one of these has downsized. But we thought getting it away from a huge government database was a better way to go.

Mr. DEUTCH. Right, to a private database where risks could be even greater than they already are. I appreciate it, and I appreciate all the witnesses being here. I yield back. Thank you.

Mr. GOODLATTE. The Chair thanks the gentleman, and recognizes the gentleman from Arizona, Mr. Franks, for 5 minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman, and thank all of you for being here. You know, it occurs to me that this Committee, the Judiciary Committee, has a unique role in Congress in the sense that it sort of epitomizes the entire purpose of government. Our job is to protect the lives and the constitutional rights of Americans. And sometimes it is difficult to make that balance work out right.

You know, everyone on this Committee, I believe, wants to try to do everything that we can to protect the national security, to protect the lives of American people. But we also want to protect their constitutional rights in that process, and that requires us to make a clear distinction on how we go about that to where we maximize both.

And I just have to suggest to you, without trying to sound argumentative, that this Administration has made it very difficult for us, because as Mr. Deutch has said and others, we feel that we have been blatantly deceived on what some of these programs have done and what they did. And consequently, it is hard for us sometimes to come up with the kind of architecture for any policy because we simply do not trust the Administration to be forthright with American people or us. And at the same time, I want to do the right thing here.

So let me just ask you this question, Deputy Attorney General Cole. The President has made several recommendations for changing these data collection programs, including ending outright the bulk collection program. And then the last time the authorities were up for renewal, then the Administration, after they had said this, came before us and asked us to renew them completely. Now, help me understand that. Help me understand the contradiction there.

Mr. JAMES COLE. I do not believe it is a contradiction, Congressman. I think it is just an evolution as people come to the debate and try to figure out the best way to do it, as we get the recommendations from the PCLOB and the President's review group, as we look at the value of what we get from these programs. And I think what the President has said is he does believe that the 215 program is valuable, but he is trying to find ways and has charged us with trying to find ways to accomplish as much and most of what that gives in other ways that will cause less concern for the American people, legitimate concern that they have about what is being done.

Despite all of the court restrictions that are put on, despite the fact that as both groups found, there has been no intentional abuse of any of this, it has been well regulated and well minded, and it has been reported to the courts and Congress and the executive branch. There is still a faith that we want to keep with the American people about making sure that they are satisfied we are doing everything we can do. So that is where we are. It is an evolution more than a contradiction.

Mr. FRANKS. Attorney General Cole, I appreciate that. I just would suggest to you that the American people are clearly at odds with that understanding. They feel that they have been deceived, and I certainly cannot possibly come back to them and tell them they have not.

But if I could shift gears and ask you, Mr. Medine, a question regarding 2315 that the Attorney General brought up. How can a bulk collection that potentially violates the First and Fourth Amendments be potentially unconstitutional, but individual collection is not? Help me understand the dichotomy there. I mean, if as, you know, the majority suggests here that the bulk collection of telephony metadata under Section 215 is constitutionally unsound, would the same not be true for individual 215 orders?

Mr. MEDINE. First, the board did not say that the bulk collection was unconstitutional. What we did say is that there is a Supreme Court precedent, *Smith v. Maryland*, that says that records held by third parties are not entitled to Fourth Amendment protection. But we have also looked at the Jones case involving GPS tracking and seen a potential trend, especially in the voices of five justices, suggesting that this type of information was entitled to constitutional protection because of the breadth of its collection.

So collecting information on hundreds of millions of Americans over an extended period of time is very different from collecting information on one person who may be a suspect for a short period of time. So we did not reach constitutional conclusion on that, but I think there is a distinction between those two scenarios.

Mr. FRANKS. All right. Well, quickly, Judge Bates, who formerly sat on the FISC, recently wrote a letter objecting to the creation of a public advocate position, like Mr. Obama has suggested. He wrote that, "Given the nature of FISA proceedings, the participation of an advocate would neither create a truly adversarial process nor constructively assist the courts in assessing the facts."

Attorney General Cole, I will ask you, do you agree with Judge Bates' conclusion and tell me why.

Mr. JAMES COLE. Well, I think the history of the Court has been that it has functioned quite well, and that the judges have been very earnest about trying to look at both sides. But I think, again, as we have started to think through this, there may be instances where the Court could benefit from another point of view, not in every instance. And the instances may be quite infrequent. But there are those where we think that another perspective may be helpful to the Court in reaching its conclusions.

Mr. FRANKS. Mr. Chairman, I am out of time. Thank you, sir.

Mr. GOODLATTE. The Chair thanks the gentleman, and recognizes the gentlewoman from Washington, Ms. DelBene, for 5 minutes.

Ms. DELBENE. Thank you, Mr. Chair, and thanks to all of you for being here today. Mr. Medine, I would like to talk about transparency and the impact of the Administration's step to allow technology companies to be able to provide greater disclosure about the number of government requests they receive.

Just yesterday many companies took advantage of the agreement reached with the DoJ and have provided new information to the public, which I think is a welcomed development. Do you think leg-

isolation that allows companies to provide more details to the public would be helpful? In particular, can you talk about the distinction between what the agreement last week allows and what you believe should happen? I am also a co-sponsor of the USA Freedom Act, and we also outline recommendations there. And I would love your opinion on that.

Mr. MEDINE. Our board's report recommends a number of areas where transparency could be greater so that there could be more public confidence in our intelligence programs, and so transparency with regard to the government's request to companies is certainly a part of that.

What our Board recommended is that companies be given an opportunity, in some cases a greater opportunity, to disclose government requests consistent with national security. And so, we have not had a chance to evaluate the arrangement that was struck with the Justice Department, but certainly it is a move in the right direction to allow the companies to make it clear what is collected and also to disabuse people, particularly overseas, and clarify that there is less collection going on than they think, which I think will actually help American businesses down the road. So we are very supportive in principle of doing this, but we have not examined the specifics of it.

In terms of whether there is a need for legislation, I think we could evaluate how well the government struck its balance. But there are important national security concerns in revealing information, and it is important to do it in the right way.

Ms. DELBENE. Okay. We would be interested in your opinion on that after you have had a chance to look at it in more detail.

Mr. Cole, you stated last week the Administration had determined that the public interest in disclosing this information now outweighs the national security concerns that required its classification. And, you know, my position is that even greater disclosure is warranted in order to restore the credibility and trust of the American in our government.

But I want to focus one particular element of the transparency agreement announced last week. In the letter you shared with companies' general counsels last week outlining the terms of the agreement, you state that the government is able to designate a service or designate a new capability order, and thereby delay reporting on that service for 2 years. And I wondered what the criteria was that you would be using in making the decision of what a new capability would encompass.

Mr. JAMES COLE. Well, I think the criteria is set out in the letter. It is a new platform or a service or a capability that we have not had before that would indeed be something new and that we would be, I think, going to the court and having it incorporated in the order. And so, it would be something where we have gained a new capability to intercept communications that we have not had before, so that if people are relying on our inability to be able to intercept that information—terrorists and people like that—that they will not all of a sudden see a spike if we come to adopt that view or that capability, and, no oh, I better get off this platform.

Ms. DELBENE. But given that that is a rather vague definition of what a new capability is, because of a new version of what you

are doing right now, how do we know that that is not going to be used in such a broad way that basically ends up preventing disclosure of a lot of information that otherwise is covered in the agreement?

Mr. JAMES COLE. I believe there is an avenue for the companies to go to the Court and challenge that, and certainly come to the Justice Department and challenge that, and say it, in fact, is not a new capability. And we can try and work that through, and the Court could find that it is not.

Ms. DELBENE. And why do you believe that there has to be such a caveat in the agreement at all?

Mr. JAMES COLE. From a national security standpoint so that people who are comfortable communicating over a certain type of capability do not all of a sudden realize that we can now intercept that capability.

Ms. DELBENE. But do have a specific example in mind from what—

Mr. JAMES COLE. Nothing that I would want to talk about in an open hearing.

Ms. DELBENE. Thank you, and I will yield back, Mr. Chair.

Mr. GOODLATTE. The Chair thanks the gentlewoman, and recognizes the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman. Mr. Chairman, I was going to pursue a line of questioning related to the balancing of constitutional principles, and two of them are at play here, national security and privacy. And then I was going to pursue a line of questioning related to the expectation of privacy and whether or not it can change with culture and technology. But two things happened, Mr. Chairman, on the long, arduous walk from your chair to mine.

One was something my friend from Tennessee said, suggesting a link between appointing judges and how they rule. In fact, Mr. Chairman, our colleague from Tennessee said everything is politics, justices are politics. So I want to ask Mr. Swire, I am going to read you a list of names, and everybody on this list has at least two things in common, and I want you to see if you can guess what those two things are, okay?

Mr. SWIRE. It is arduous for us, too, Congressman, but go ahead.

Mr. GOWDY. David Souter, John Paul Stevens, Harry Blackmun, William Brennan, Earl Warren, and Anthony Kennedy. What do all of those justices have in common?

Mr. SWIRE. I suspect you are pointing to the fact that they are Supreme Court justices nominated by Republican presidents.

Mr. GOWDY. That is exactly what I am referring to. And what would be the second thing they have in common? Would you agree that they wildly underperformed if they were put there to pursue a conservative agenda?

Mr. SWIRE. I am hesitant to say all these justices wildly underperformed on any criteria.

Mr. GOWDY. You do not think Brennan wildly underperformed if we put him there to pursue a conservative agenda?

Mr. SWIRE. I am sorry, which—

Mr. GOWDY. Blackmun, Brennan. They cannot get you in trouble anymore. [Laughter.]

Judges cannot take up for themselves, Mr. Chairman. They either cannot or will not. I just do not think it is appropriate to try to make links between who put somebody on the bench and how they are going to turn out because I just pointed to a half dozen that did not turn out the way we thought they were going to turn out.

The second thing that happened, Mr. Chairman, was Mr. Jordan's line of questions. Mr. Cole, I am not going to ask you about the IRS targeting scandal for two reasons. Number one, you cannot comment on it, and I know you cannot comment on it, so I am not going to put you in a position of having to repeatedly say you cannot comment on it. The second thing you cannot do is explain to us why the President said what he said Sunday. So because you cannot explain it any more than anyone can explain it, I am not going to ask you about it.

I am going to ask you to do one thing, and you do not have to comment on it. I am just going to ask you to do one thing, prosecutor to prosecutor. I am going to ask you to consider, in my judgment, how seriously the President undermined the integrity of that investigation by what he said, "not a smidgen." Lay aside that is not a legal term, "not a smidgen" or scintilla of evidence to support corruption or criminality.

This investigation is ongoing. I assume no conclusions have been reached, hence the word "ongoing." And for him to conclude that there is no evidence of criminality whatsoever in the midst of an investigation I think undermines the hard work that the men and woman of your Department do. And I do not expect you to comment. I do not want you to comment, other than I would ask you to consider anew appointing special counsel under the regulations. The special counsel of regulation say it is appropriate in extraordinary circumstances.

What we have been discussing all day today is the extraordinary circumstance of whether can you target under the Fourth Amendment. The IRS case is whether government has targeted people for the exercise of their First Amendment rights. So I do not think anyone would argue it is not extraordinary if there is an allegation that government is targeting someone.

And the second part of the regulation speaks to the public interest. So I would just ask you to please respectfully reconsider in light of what was said Sunday night, which was there is nothing here, not a smidgen of criminality in the midst of an investigation that matters greatly to lots of people. The Chief Executive said move on. For no other reason than to protect the integrity of the justice system, which I know you care about and I care about, I would ask you respectfully to consider appointing someone as special counsel in light of what the President said Sunday night, because he seriously undermined the integrity, in my judgment, of what is an ongoing investigation. And with that, I will yield, Mr. Chair.

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

Mr. JEFFRIES. I thank the Chair as well as the witnesses for your participation in today's hearing.

Mr. Cole, I want to go over a few questions related to the relevancy standard. I recognize this may have been ground covered earlier in the hearing, but if you would just indulge me. They will be pretty brief.

Since the passage of the PATRIOT Act, which I believe was done in late 2001, how many actual terrorist plots have been thwarted connected to the new tools made available to law enforcement pursuant to this act?

Mr. JAMES COLE. Well, I do not think that 215 was around in the original version of the PATRIOT Act. That came some time later. I do not know the exact number.

Mr. JEFFRIES. Right. I am asking about the overall PATRIOT Act.

Mr. JAMES COLE. I do not know the exact number.

Mr. JEFFRIES. Okay. Now, as it relates to the bulk collection of metadata allegedly authorized by 216 that came subsequent to the initial creation of the PATRIOT Act, how many terrorist plots can be directly linked to this bulk collection? Am I correct that the answer is zero?

Mr. JAMES COLE. I think the question is directly linked. There are tips and there are leads that come from the 215 metadata as I have said a number of—

Mr. JEFFRIES. Can you provide us with one example where a tip or a link actually led to the thwarting of a terrorist plot connected to this bulk collection?

Mr. JAMES COLE. Well, alleged charges. It does not mean that there were not other tips and leads that led to further investigations that were valuable and helpful to the government.

Mr. JEFFRIES. But it is fair to say there is no substantial connection between this bulk collection and the resolution or thwarting of any terrorist plot related to this particular authorization under 215, correct?

Mr. JAMES COLE. I think that may be correct, but I think that that is not always the only standard that is used.

Mr. JEFFRIES. Right. Now, you referenced that earlier in your testimony. Can you give an example to the American people to justify this bulk collection outside of its alleged relevance, given that there has been no evidence, not a scintilla of evidence, presented that it has been relevant to any terrorist investigation?

Mr. JAMES COLE. Well, I think it is relevant in a couple of ways. One is to be able to rule out that there are connections within the United States from terrorist plots that may be starting outside the United States. So it is very valuable to be able to know that so we can direct our resources very much at the core of what we are trying to look for.

Mr. JEFFRIES. Now, do you think that the current relevance standard is a robust one?

Mr. JAMES COLE. I think the current relevance standard is one that is used in both criminal and civil law, and it is a very broad standard.

Mr. JEFFRIES. It is a very permissive standard in terms of what the government has been able to get access to, correct?

Mr. JAMES COLE. It is not unfettered. It has to be done in a way that is necessary. We cannot just take whatever we want any time we want for any purpose. We have to go to a court and justify the fact that we need this volume of records in order to find the specific things we are looking for under very restricted circumstances. And then the court has to say you have permission to do this.

Mr. JEFFRIES. Right, but what is very troubling, and I would like to talk to Mr. Swire about this, it is my understanding that once that bulk collection has been obtained, that the standard of reasonable articulable suspicion as it currently exists is a decision made by a NSA supervisor, not by an independent member of the judiciary, correct?

Mr. SWIRE. In the first instance, it is made by the analyst, and it is reviewed by a supervisor.

Mr. JEFFRIES. Now, how is the Review Board proposing to change the absence of judicial consideration?

Mr. SWIRE. As was true in 2009 when there were some difficulties with compliance, we recommended that it go to the FISA Court in individual instances for a judge to review.

Mr. JEFFRIES. Are you saying in the first instance in terms of the authorization of bulk collection or subsequent collection to search the data there must be a judicial determination made?

Mr. SWIRE. In this case, there is collection, and then there is reasonable articulable suspicion about some phone number. And at that point you would go to the judge and say, judge, here is our RAS, and here is why we think we should look at it.

Mr. JEFFRIES. Okay. Now, as it relates to collection, there has been discussion and debate about which entity would be most appropriate, putting aside the question as to whether it is even proper for this information to be collected, and I think the jury is still out on that, and the balance of facts suggest that it is not. But assuming that this information is collected, I guess the proposals have included the private sector, telephone companies, and an independent third party yet to be identified. Has there been any consideration given to the judicial branch as a separate, but coequal, branch of government independent from the executive creating the mechanism to retain this data given the fact that a judicial determination at some point is going to be made as to whether it should be searched?

Mr. SWIRE. Yes. I am not aware of the judicial branch holding databases and running those except for their own court records. So that would be quite a different function than I think what we have seen previously.

Mr. JEFFRIES. Okay, thank you. I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman, and recognizes the gentleman from Texas, Mr. Farenthold, for 5 minutes.

Mr. FARENTHOLD. Thank you, Mr. Chairman. Mr. Medine, you talked a little bit earlier in response to some questions about limited Fourth Amendment protections for information held by third parties. I think a lot of that is what Section 215 kind of bootstraps on. It gives the government broad authority to get a hold of that information.

Just so the folks watching this and everybody understands, there is a difference between, like, if I have a file on my computer or if

I have a file on something on a cloud storage. I have more privacy, correct, in what is on my computer, more protection.

Mr. MEDINE. Under current Supreme Court law, that is right.

Mr. FARENTHOLD. And the same would be true for something sent by postal mail. I would have more privacy than something sent by email. That is kind of more traditional. And I would assume that, you know, a canceled check that I have in my drawer is more protected than the bank record. Is that something you think most Americans understand the difference in this day and age about information that is held electronically or held by third parties? Do you think most Americans understand that it is basically fair game?

Mr. MEDINE. I suspect that they do not, but I think the key thing here is that, as you say, technology has changed dramatically since the Supreme Court's decision in *Smith v. Maryland*, which was collecting a limited amount of information for one person over a short period of time as opposed to—

Mr. FARENTHOLD. Our ability to gather information has changed. So the courts could revisit this, but is it also not appropriate that Congress could revisit this and say you actually do have a reasonable expectation of privacy in certain things?

Mr. MEDINE. That is exactly what the majority of our board has recommended is that based upon our legal analysis of Section 215, our constitutional analysis, which we say is heading in the direction of adding protections, and also our balancing national security with privacy and civil liberties, we saw a great impact of this program on—

Mr. FARENTHOLD. So let me just ask Mr. Cole, and I suspect I know the answer to this question. So if any of my information is held by a third party, do you see any substantial limitation on what Section 215 allows you guys to get?

Mr. JAMES COLE. Yes, I see very significant limitations on what we could get being held by a third party.

Mr. FARENTHOLD. All right. Let us just talk about some things that are probably held in bulk. We talked a lot about the metadata on telephone calls. Could geolocation data that is routinely reported back from cell phones be gathered?

Mr. JAMES COLE. If there is a need, it may or it may not.

Mr. FARENTHOLD. Bank records, credit card transactions, things like that?

Mr. JAMES COLE. They may not be. It depends on whether there would be a need to show the connections where you would need the whole group—

Mr. FARENTHOLD. But under the rationale that you get all telephone records, could that not be extended to say, all right, we need all credit card transaction records, or all geolocation data so we can go back and mine it after the fact, from what we hear from the folks to your left, is a very limitedly effective program.

Mr. JAMES COLE. Well, we are not mining the data, Congressman. That is not something—

Mr. FARENTHOLD. Or go back and searching it, I guess.

Mr. JAMES COLE. Well, and we are searching only in a very limited way.

Mr. FARENTHOLD. Right, but the same argument that says you can collect all the phone data, could the exact same argument not be used for any other sorts of data that are collected by businesses in bulk?

Mr. JAMES COLE. Not necessarily because the phone data connects two different people, and you have to look at those two different sets of information.

Mr. FARENTHOLD. Right. So the geolocation data does the same thing. I go—

Mr. JAMES COLE. Not necessarily because it only focuses on one person and not—

Mr. FARENTHOLD. Right. But if you got the geolocation data, you could get everybody who is within 150 feet of me by rather than searching the person's phone, you could search the law and where they are, and you could tell everybody who's in this room right now.

Mr. JAMES COLE. But there may be other ways to go about that without collecting all of the data for every single cell tower in the United States.

Mr. FARENTHOLD. Okay. But do you believe that it would be legal for you all to do that?

Mr. JAMES COLE. Only if there was a need. The Court's rulings have really focused on the fact that there is a need under the facts and circumstances—

Mr. FARENTHOLD. All right. I see I am almost out of time, and I wanted to follow up on something that came up in the Oversight and Government Reform Committee last week. Can you tell us whether the NSA is playing any role in identifying, assessing, or classifying information about security threats or vulnerabilities associated with the healthcare.gov website? Are you aware of anything?

Mr. JAMES COLE. I am not aware of anything, Congressman. Nothing that I am aware of.

Mr. FARENTHOLD. Thank you very much. I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Rhode Island, Mr. Cicilline, for 5 minutes.

Mr. CICILLINE. Thank you, Mr. Chairman. I thank you and the Ranking Member for the warm welcome, and I look forward to the work of this Committee. Thank the witnesses for being here and for your testimony.

I am, too, a proud sponsor of the USA Freedom Act and really associate myself with the remarks of my colleague, Mr. Sensenbrenner, and hope the urgency of action is clear to all of the witnesses and hopefully to our colleagues in the Congress.

I share the view of many people that it is very difficult for me to understand how the existing statute authorizes this massive data collection of all Americans, and I am struggling to understand how that authorization is provided in the statute. But I want to ask a couple of very specific questions.

One is I think there has been testimony from all three witnesses that there is not a lot of evidence, if any, that this action, this metadata data collection, has led to the interruption of a terrorist attack, but it has been useful in a variety of different ways. And since the private industry holds these records for 18 months, has

anyone looked at in the instances it has been useful what the time period has been? Has it been beyond the 18 months? If we were to change that to 24 months, would we cover all of the useful moments and not have to have the government collecting any of this data? Does anyone know the answer to that?

Mr. JAMES COLE. I think that is one of the factors that we are trying to look at to see how long you need the data for. This was one of the issues when the President said, and we talked about cutting it down to 3 years instead of 5 years for holding it, is one step. And we may look further to see what the right amount of time is.

Mr. CICILLINE. So with respect to the information we have currently, the benefits of in these instances where it has been useful, we do not know what that time period has been.

Mr. JAMES COLE. We are looking into that.

Mr. CICILLINE. Okay. The second thing I want to ask is, you know, we have this very deeply held belief in this country that the key parts to our justice system or two of the key parts are an independent neutral magistrate or judge. The current system allows the queries to be made by decisions made by someone other than a judge. And one of those reforms that has been recommended is that a FISA Court judge make that determination as a result of hopefully some adversarial process so that arguments can be made on both sides. That seems a very common sense reform.

I would like to ask your thoughts about the national security letters because it seems to me the same kind of information can be collected through the national security letters that do not require a judicial determination. And it would seem to me that that would be a fairly easy reform to implement that says these letters can broadly collect lots of information without any judicial determination that it is necessary or appropriate. Why not impose the same requirement? And I know, you know, the argument always is, oh, it is too much, you know. It will require lots of extra hours.

Setting aside the fact that it will be a lot of work for some folks and that we are prepared to fund that, does it not make sense that we ensure that there is a judicial determination as to the propriety of the information sought that can be quite broad? And I would like all three of you to comment on that.

Mr. JAMES COLE. First of all, you have to understand national security letters are not as broad as other things, other kinds of subpoenas, grand jury subpoenas, even administrative subpoenas under the Controlled Substances Act or 215 authorities. It is more limited. That being said, it is much like an administrative subpoena or a grand jury subpoena, which does not involve any prior judicial approval before they are issued. Any judicial involvement comes on the back end if people do not comply with it.

And they are very routine. They are used—

Mr. CICILLINE. But those grand juries—excuse me for interrupting—those grand jury subpoenas require the participation of grand jurors, of citizens, to make a determination—

Mr. JAMES COLE. They do not issue them themselves. There usually can be just a blanket authority from the grand jury to go issue—

Mr. CICILLINE. But it requires action of citizens to authorize it. In this case, the national security letters, there is no participation

of citizens. It can be a NSA official that makes that determination with no either citizen participation or judicial participation.

Mr. JAMES COLE. Actually grand jurors usually do not participate in the decision to issue a subpoena. They receive the evidence that comes as a result of it and consider it, but they do not usually get involved in the issuance of the subpoena. That is usually done by the prosecutor.

Mr. CICILLINE. So is it your position that having a judicial determination of the national security letter request is not appropriate? Would that not provide additional protection against an intrusion into the privacy rights of citizens with a de minimis kind of intervention by a judicial officer?

Mr. JAMES COLE. I do not think it would provide any significant protection against privacy invasions for citizens. There are still administrative subpoenas, grand jury subpoenas, lots of things like that that go well beyond what a national security letter can do. I do not see the point of it.

Mr. CICILLINE. Mr. Swire?

Mr. SWIRE. Our report came out in a different place, and we did recommend a judge. And in terms of the comparison with a grand jury subpoena, here are two differences that are not always stressed. One is that the NSLs stay secret under current law probably for 50 years, and that is very different. And the second way from what happens in a criminal investigation where if there is a problem with the investigation, the criminal defendant and his or her lawyer find out about it quickly, and that is a check on over reach.

With NSLs, the person who is being looked at does not get that kind of notice, so you do not have a built in check against using it too much.

Mr. MEDINE. Our board unanimously recommended that the RAS determinations, reasonable articulable suspicion, immediately go to the Court, after the fact, for judicial oversight of that program.

Going forward, the only thing I would say is, because we have not studied national security letters on our Board as yet, to consider that we not make it a higher standard to collect counterterrorism information than we do in ordinary criminal cases, to look more broadly overall at how are these programs operating.

Mr. CICILLINE. Thank you. I thank you, and I yield back.

Mr. GOODLATTE. The Chair recognizes the gentleman from North Carolina, Mr. Holding, for 5 minutes.

Mr. HOLDING. Thank you, Mr. Chairman. Mr. Swire, with private parties holding metadata, what kind of liability do those private parties have for any misuse of the metadata?

Mr. SWIRE. So a phone company today, if it is hacked into or if they turn it over when they are not supposed to turn it over?

Mr. HOLDING. First, you know, if they are hacked into, I guess there would be some determination as to whether they have taken adequate steps to protect the data. So what liability do they have there? What liability do they have if they turn it over to the government, and for some reason the government misuses it? Are there any immunities that these third parties have?

Mr. SWIRE. So there is not an immunity if they lack reasonable security. Most of them have privacy policies where they said they are going to use reasonable security measures. The Federal Trade Commission or the Federal Communications Commission could bring a case against it. Private tort suits have not succeeded mostly, but the government could come in.

When it comes to the second part, I think that comes up with the scope of the immunity that Congress included in the law the last time around. I do not know all the contours of that, but it is quite immunity is my understanding.

Mr. HOLDING. And, of course, if we set it up so these third parties are retaining this information for a longer period of time, I assume that they would want additional assurances of immunities.

Mr. SWIRE. I predict they would want that, yes.

Mr. HOLDING. Mr. Cole, you would certainly agree that we live in a dangerous world.

Mr. JAMES COLE. I am sorry?

Mr. HOLDING. We live in a dangerous world.

Mr. JAMES COLE. Yes, we do.

Mr. HOLDING. And the dangers are overseas, and they are at home.

Mr. JAMES COLE. That is correct.

Mr. HOLDING. There are plenty of people who wish us great harm. And in the years subsequent to 9/11, the danger may have changed, but I do not think the danger has diminished.

Mr. JAMES COLE. That is correct.

Mr. HOLDING. In fact, it may have increased.

Mr. JAMES COLE. It has become different, and it has become a lot more difficult to detect.

Mr. HOLDING. And you have mentioned several times and the other Members have mentioned several times about the use of the metadata in 215. And, you know, some people pointed out that, you know, no criminal case has been brought, you know, on the basis of metadata queries. But you pointed out that it is a part of a fabric of an investigation. I would like to think of it as a mosaic when you are putting together an investigation, whether it is public corruption, or a sophisticated drug conspiracy, or indeed, you know, a terrorism investigation.

I want to give you a few minutes to spin a hypothetical based on your experience as a prosecutor and as, you know, someone who oversees a lot of investigations, a hypothetical where the Section 215 metadata is used as a piece of that mosaic. And to give some context to the conversations, you know, that we have had back and forth, and kind of what that mosaic looks like.

Mr. JAMES COLE. Well, obviously there is any number of different ways it could play out. But one possible scenario is you have reasonable articulable suspicion that a certain phone number is connected with a certain terrorist group, and you then inquire about it, and you see calls to and—

Mr. HOLDING. Now let us back up a little bit. And how would you come about one of these telephone numbers?

Mr. JAMES COLE. Well, that could be from any number of other sources of intelligence, and without going into too much detail, there is a lot of information that feeds in that helps inform how

we come to those conclusions if there is, in fact, reasonable articulable suspicions. But it has to be documented. It is not just something that is floating in the air. It has to actually be written down so somebody can read it, look at. A supervisor can determine that, in fact, it is reasonable articulable suspicion, and authorize the inquiry to be made.

At that point, we just have the phone number. We then look at who that phone number has called, and we may see that there are a number of calls to another number. At that point, we do not know who that is, but we may then give that information to the FBI. They may then through a national security letter or something else determine who that number belongs to. They may then be able to look at other holdings that they have and other information they have that indicates that that other number is, in fact, somebody that they have been investigating for terrorism. And then they start putting that together, and the investigation starts to blossom from there. That is one of the ways that this could play out.

Mr. HOLDING. So the metadata may not be the smoking gun, but it certainly puts not only a piece of the mosaic, but it might be like the cement that kind of puts the mosaic together, hooks it to another part.

Mr. JAMES COLE. It is tip or a lead. It starts the process going.

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

Mr. GOODLATTE. I thank the gentleman, and the Chair recognizes the gentleman from Georgia, Mr. Collins, for 5 minutes.

Mr. COLLINS. Thank you, Mr. Chairman. I appreciate the time. And I am probably not going to spend the whole time because one of the things that I want to focus on here is probably the question, is I think from the sense—Mr. Cole, you have been here many times, and we have had these conversations. Others have been here as well. Today the Committee, especially Judiciary, reminds me more of a P90X workout. One side you are going hard for 5 minutes, and then the next time, whew, I rest for 5 minutes. [Laughter.]

Hard for 5 minutes, rest for 5 minutes. And what happens here is you see a unilateral sort of discussion and understanding that what we have that nobody is comfortable with. They are not. They do not want to put our national security at risk. Nobody on this panel, nobody in this Congress, and many people in the country, they do not want to put—but they are also very uncomfortable with the collection. They are very uncomfortable with the way it has been dripped out of this is what is happening now, this is what is happening now, 2 weeks later here is what is happening. By the way, we are now angry birds, you know. Whatever it is, it is just dripping out.

And so, every time we begin to maybe put a hold on it, it becomes a deeper problem with another revelation, and some of that was definitely not intended. Some of that was leaked maliciously, and I recognize all that. And from my part of Georgia, people understand national security. They understand patriotism. That is not the problem. What they do not understand is a loss of trust in the government, frankly a loss of trust in this Administration, a loss of trust.

So what I really would like to focus on just for a moment, and if you have a lot you want to say, great. If you do not, then that is okay. But I think we have discussed a lot of specific recommendations. We have talked about have you found out, have you showed it. The mosaic, as my dear friend from North Carolina talked about, about investigations. But mine goes back to an essential question that this Congress will have to ask, and I believe it is the only reason that the President came out and said we need to change this, we need to look at this, is because, frankly, the poll numbers are bad. You have been looking at this for 5 years. You knew it for 5 years. And now it is, well, this is getting bad, we need to get ahead of this, let us show leadership, the whole crowd is up there, let me run in front and lead. The problem is trust.

So my question as we look at this, no matter what recommendations may come here, and I have associated with many on both sides of the aisle of the problems that we have, is in my district and in many others, NSA has become not a three-letter word, but a four-letter word. It has become something that they just do not understand and they do not trust anymore.

So my question is, no matter what recommendations we give—any of you want to talk about it—for just a moment, how do we restore that? And that is the basic question here. How do we restore trust?

Mr. JAMES COLE. Congressman, I think you raise a very, very important point, which is trust. We come to this through years of both Republican and Democratic Administrations where the intelligence community has determined that it is appropriate to classify a lot of things information that we are now talking about in open hearings. And they had a good faith determination at the time that it should be classified for the national security and safety of our country.

It is out, and we are talking about it. And the American people deserve to have answers, and they deserve to have a level of transparency that makes them comfortable about these things. And I think that this Administration, quite frankly, has taken the bull by the horns, and these are not easy issues. These are not easy resolutions. These are not easy balances to find. But this Administration has gone very far in trying to be transparent, in trying to bring these programs back into line, in trying to balance how far we can go, how transparent we can be, how many civil liberties and privacy interests we have to respect, and how much of the national security side we have to respect, and where that balance is. And these are tough balances.

You are not going to do it overnight. You are not going to sit there and say, oh, that is easy. Let us just go over and disclose all of this, or let us just not collect this information. These are things that if you do not collect it and something blows up, people are going to be very angry. But these are also things that if you do over collect, and you do over classify, and you do inhibit people's civil liberties, they are going to be upset about that, too. So we have to find that balance, and I wish it were easier, but it is not.

Mr. COLLINS. And, look, I respect that, and you have been up here, and you are an advocate of what the Administration is doing, and I get that. But I think the trust factor is the biggest issue, and

I think it was not grabbing the bull by the horns. I think it was grabbing a microphone and saying I will make you feel better, and I understand that. But at the same point, it does not go to the heart of the question. It does not go to that trust issue on how we in this Congress can explain that, and how the Administration can make it look more instead of a public appearance and we are going to PR, how we actually solve this.

Look, I respect everyone. Thank you for being here. But that goes back to the real issue. This is a trust issue. We can do the recommendations, but we have got to get back to trust, and we just do not have that trust right now.

Mr. Chairman, I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman, and the Chair thanks all of our witnesses on this first panel. You have taken a large number of questions, and we appreciate the input to the Committee.

I want to ask unanimous consent to place the following documents into the record: Annex A of the PCLOB report, separate statement of board member Rachel Brand; Annex B of the PCLOB report, separate statement of board member Elizabeth Collins Cook; comments of the judiciary on proposals regarding FISA; a letter written by the Honorable John D. Bates, director of the Administrative Office of the United States Courts on January 10, 2014;* Presidential Policy Directive Number 28, the President's directive regarding signals intelligence issued January 17, 2014.**

I want to thank all the members of the panel, and you are excused. And we will—

Mr. NADLER. Mr. Chairman?

Mr. GOODLATTE. Yes?

Mr. NADLER. May I ask unanimous consent that we admit into the record the entirety of the PCLOB report since the dissenting views are going be—

Mr. GOODLATTE. Without objection, that will be made a part of the record as well.***

Mr. NADLER. Thank you.

Mr. GOODLATTE. And we thank all of our panelists.

Mr. JAMES COLE. Thank you, Mr. Chairman.

Mr. GOODLATTE. And we will move onto to the next panel. We are expecting a vote soon, but we want to keep moving.

[Pause.]

Mr. GOODLATTE. We welcome our second panel today, and if all of you would please rise, we will begin by swearing you in.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you very much. Let the record reflect that all of the witnesses answered in the affirmative.

Our first witness of the second panel of witnesses 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

*The corrected date of the submitted letter is January 13, 2014.

**See Appendix for submitted material.

***The PCLOB report document submitted for the record is not reprinted here but can be accessed at: <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf>.

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 from Michigan Law School.

Our second witness is Mr. Dean C. Garfield, president and CEO of the Information Technology Industry Council, a global trade association that is a voice advocate and thought leader for the information and communications technology sector. Previously, Mr. Garfield served as executive vice president and chief strategic officer for the Motion Picture Association of America.

Mr. Garfield is a regular contributor to the Huffington Post and has been featured in several national and international publications representing the ICT industry. Mr. Garfield holds degrees from Princeton University and New York University School of Law.

Our third witness is Mr. David Cole, a professor of law at Georgetown University Law Center. He is also the legal affairs correspondent for The Nation and a regular contributor to the New York Review of Books. He is the author of seven books.

Mr. Cole previously worked as a staff attorney for the Center for Constitutional Rights from 1985 to 1990 and has continued to litigate as a professor. He has litigated many constitutional cases in the Supreme Court. Mr. Cole received his bachelor's degree and law degree from Yale University. Mr. Cole has also received two honorary degrees and numerous awards for his human rights work.

I want to thank you all for being here today. We ask that each of you summarize your testimony in 5 minutes or less, and to help you stay within that time, there is a timing light on your table. When the light turns from green to yellow, you will have 1 minute to conclude your testimony. When the light turns red, it signals the witness' 5 minutes have expired, but I think you all know that.

And I thank you all. And we begin with Mr. Bradbury. Welcome.

TESTIMONY OF STEVEN G. BRADBURY, DECHERT, LLP

Mr. BRADBURY. Thank you, Mr. Chairman.

The independent judges of the FISA court have repeatedly upheld the legality of the NSA programs, and the President has strongly affirmed that they remain necessary to protect the United States from foreign attack. While I welcomed the President's defense of the programs in his recent speech, I'm disappointed that he decided, evidently at the last minute, to pursue changes in the telephone metadata program recommended by his review group.

The President wants to move the metadata into private hands. I don't believe that's workable, not without seriously affecting the operation of the program and creating new data privacy concerns.

The current program allows NSA to combine data from multiple companies into a single, efficiently searchable database and preserve it for historical analysis. This database is among the most effective tools we have for detecting new connections with foreign terrorist organizations. Moving this database outside NSA would require ceding control to a private contractor, since no single phone company has the capacity to manage all the data.

Putting a private contractor between NSA and the data would compromise the utility and responsiveness of this asset. It would also reduce the security of the data. Today, the database is kept locked down at Fort Mead, with access strictly limited by court order and stringent oversight. If it were outsourced to a contractor, the data would likely reside in a suburban office park on much less secure servers.

It would be vulnerable to privacy breaches and cyber incursions from foreign governments and terrorist groups. It could be exposed to court-ordered discovery by litigants in civil lawsuits, and the contractor's employees would be much less subject to direct oversight by the executive branch, the FISA court, and Congress. Those are not desirable outcomes.

The President also intends to require FISA court approval of the reasonable suspicion determinations before NSA could query the database. This change moves us back toward the pre-9/11 approach. It will inevitably hamper the speed and flexibility of the program, particularly if it requires separate court approval of each query, and it will place a substantial new burden on the FISA court. Requiring the involvement of lawyers and court filings will impose a legalistic bureaucracy on a judgment call more appropriately made in real time by intelligence analysts.

Finally, the President ordered NSA not to analyze calling records out to the third hop from the seed number, something the NSA only does when there's a specific intelligence reason. Why should we needlessly forego these potentially important intelligence leads?

Beyond the changes endorsed by the President, I urge this Committee to reject most of the other major proposals for curtailing FISA. The most sweeping proposal would restrict the use of Section 215 to individual business records directly pertaining to a specific person.

A similar proposal would limit NSA to conducting queries of the telephone calling records only while the data is retained by the companies in the ordinary course of business. These restrictions would kill the metadata program by denying NSA the broad field of data needed to conduct the necessary analysis.

At the same time, denying NSA the ability to access metadata in bulk would preclude the historical analysis of terrorists' calling connections, which is among the most valuable capabilities of the 215 program. Any requirement to shorten the data retention period would degrade our ability to discover important historical connections.

One further proposal would attempt to convert FISA into an adversary process by establishing some form of public advocate. This proposal would raise significant constitutional concerns, both if the President is required to share sensitive national security secrets with an adversary and if the public advocate were given the power to oppose each FISA application and to appeal a decision of the FISA court.

Such an officer would lack the Article III standing necessary to initiate an appeal and would occupy a gray zone outside the three branch framework established in the Constitution.

Instead of creating a formal office of public advocate, the President wants to set up a panel of pre-cleared outside advocates who

could be called upon by the FISA judges to submit amicus briefs on significant questions. This proposal is less objectionable if it leaves to the FISA judges the decision to call for amicus input and preserves the President's discretion to decide whether the amicus gets access to classified information.

Of course, any requirement that an outsider be granted access to the intelligence information available to the court will chill the executive branch's willingness to disclose the most sensitive details relevant to FISA applications. As the FISA judges recently pointed out, this disincentive would threaten the relationship of trust between the Justice Department and the FISA court, something this Committee should strive to avoid.

Many of these reforms, Mr. Chairman, run the risk of re-creating the type of cumbersome, overlawyered FISA regime that proved so inadequate in the wake of 9/11. If our Nation were attacked again, I am concerned that a future President may feel the need to fall back on Article III authority to conduct the surveillance necessary to protect the country, and I don't think any of us would like that outcome.

Thank you very much.

[The prepared statement of Mr. Bradbury follows:]

TESTIMONY OF STEVEN G. BRADBURY
Before the
HOUSE COMMITTEE ON THE JUDICIARY
Hearing on
Examining Recommendations to Reform FISA Authorities
February 4, 2014

Thank you, Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the Committee.

I'm honored to appear before the Committee today to discuss the foreign intelligence programs of the National Security Agency ("NSA") and to offer views on the major reforms announced by the executive branch or currently under consideration in Congress or proposed by various boards and review groups for modifying or curtailing the NSA's programs and for amending key provisions of the Foreign Intelligence Surveillance Act, or "FISA."¹

Summary

Any debate over proposals to restrict the NSA activities revealed by Edward Snowden's leaks or to make significant amendments to FISA in response to those leaks should carefully consider whether the foreign intelligence programs that would be affected by the proposals are lawful and whether they continue to be necessary to defend the country.

In his speech on January 17, 2014, the President made it clear that after extensive review of the NSA programs, he has concluded (1) that the programs are lawful in all respects—authorized by statute and consistent with the Constitution, (2) that they remain necessary to protect the United States from foreign attack, and (3) that there have been no intentional abuses of the programs. If the NSA

¹ The author is an attorney in Washington, D.C., and the former head of the Office of Legal Counsel in the U.S. Department of Justice from 2005 to 2009, where he advised the executive branch on legal matters relating to national security, including surveillance authorities under FISA. The views presented are solely the personal views of the author and do not represent the views of his law firm or of any current or former client.

programs are lawful and consistent with the Constitution and if, in the estimation of the executive branch and the relevant committees of Congress, they remain necessary to protect the Nation from foreign threats, then the President and Congress should be very wary indeed about approving any changes in the programs that might undermine their effectiveness or that might diminish the ample existing security measures, privacy protections, and oversight protocols under which they operate.

For the reasons I explain in detail in part I of this testimony (pages 5-14 below), I agree with the President that there is no serious argument that the NSA programs as currently configured violate any applicable statutory or constitutional restrictions. The independent federal judges who sit on the FISA court have repeatedly scrutinized these programs over the past several years and ensured that they comply in all respects with the requirements of FISA and are fully consistent with the Fourth and First Amendments of the Constitution. The FISA court's decisions confirm that both the bulk telephone metadata acquisition and focused analysis currently occurring under the business records provision of FISA (commonly known as section 215 of the PATRIOT Act) and the broad foreign-targeted surveillance of international communications conducted under section 702 of FISA comply in all respects with the Constitution and the terms of the relevant statutes and are consistent with the intent of Congress.

With respect to the telephone metadata collection, in particular, this program has been approved on 37 occasions by at least 15 different federal judges on the FISA court and at least two other district court judges. No court has held that the telephone metadata program exceeds the statutory authority granted in section 215 to acquire business records that are "relevant to" an authorized counterterrorism investigation. The recent decision by Judge Richard Leon, which is currently stayed pending appeal to the D.C. Circuit, addressed the Fourth Amendment implications of the telephone metadata collection but did not address its compliance with section 215.

Moreover, a review of the FISA court opinions recently declassified and released to the public amply demonstrates that the FISA court is no rubber stamp for the surveillance policies of the executive branch. The judges of the FISA court, as well as the attorneys of the National Security Division of the Justice Department, the Inspectors General of the Intelligence Community and the Justice

Department, and the diligent oversight of the Intelligence Committees of Congress, have held the NSA to the highest standards in the operations of these programs, including by ordering the prompt correction of significant compliance issues identified to the court by the Agency and its overseers.

Indeed, I understand that all Members of Congress, specifically including the Judiciary Committees, were informed about the details of these two NSA programs or were at least given the opportunity to receive such briefings in connection with the reauthorizations of sections 215 and 702. The large majorities of both Houses that voted to reauthorize these statutes in 2011 and 2012 therefore represented, at least constructively, a clear approval and ratification of the legal interpretations supporting the NSA's collection and surveillance activities, including the bulk acquisition of telephone metadata.

As explained in part II of this testimony (pages 15-16 below), I also accept the judgment of the President, the Director of National Intelligence ("DNI"), and Gen. Alexander, the outgoing Director of the NSA, that the NSA programs revealed by Snowden are critically important to preserving the security of the United States and its allies and that these programs continue to make an essential contribution to our counterterrorism defenses. From everything I know, these programs are, as they were designed to be, among the most effective tools for detecting and identifying connections between foreign terrorist organizations and active cells within the United States and for discovering new leads, including new phone numbers, in furtherance of counterterrorism investigations. With respect to the telephone metadata program conducted under section 215, both the President and Michael Morrell, former Deputy Director of the CIA and a member of the President's Review Group, have stated that if this program had been in place before September 2001, it might have prevented the attacks of 9/11, and it has the potential to help prevent the next 9/11.

If that's true, it is the duty of the President to stand up and defend the programs before the American people and Congress. I'm pleased that the President finally spoke out in strong defense of these programs and the work of the dedicated officers of our intelligence agencies in his speech of January 17, though, as explained more fully below, it's disappointing that the President nevertheless felt the need to bow to political pressures and to propose changes in the operation

of the telephone metadata program that could significantly diminish the effectiveness of the program and could compromise the security of the database.

I'm also gratified that the leaders of the House and Senate Intelligence Committees have clearly and consistently defended the programs and the integrity of the NSA. I'm hopeful that through these hearings and debates, a majority of all Members of the House and the Senate will be convinced of the need to support and preserve these essential foreign intelligence capabilities in the face of popular reaction. The national interest must trump narrow political interests.

Finally, in part III of this testimony (pages 16-21), I explain the reasons for my conviction that all of the major proposals under consideration for curtailing, restricting, or modifying the NSA programs (most especially the section 215 telephone metadata program) and for reforming the scope and use of FISA authorities in reaction to the Snowden leaks should be rejected. These include the President's announced reforms to the section 215 telephone metadata program and the major reform recommendations of the President's Review Group and the Privacy and Civil Liberties Oversight Board.

As discussed in more detail below, certain of these reforms or reform proposals would expose the Nation to vulnerability by substantially weakening or even destroying outright the effectiveness of the 215 program. Other proposals would significantly diminish the ability of the government to ensure the security and oversight of the program. Still others would unnecessarily hamper foreign intelligence efforts by adding layers of lawyering or litigation-like process that would not actually achieve greater civil liberties protections for the public but that would, I fear, prove dangerously unworkable in the event of the next catastrophic attack on the United States.

I therefore strongly urge the Committee to avoid endorsing proposals for substantial modification of the NSA programs or FISA provisions. If reforms are adopted that would severely constrain the effectiveness and utility of the NSA programs, then Edward Snowden and his collaborators will have achieved their explicit objective of weakening the national security defenses and capabilities of the United States and diminishing the position of strength that America occupies in the world post-9/11. These harms to our national security would come with no significant corresponding enhancements to civil liberties.

I. The NSA Programs Satisfy All Statutory and Constitutional Requirements

I have previously explained in detail why both the section 215 bulk acquisition of telephone metadata and the section 702 foreign-targeted surveillance of international communications are authorized by statute, consistent with the Constitution and congressional intent, and appropriately protective of privacy and civil liberties.² I will not repeat the full analysis here, but I do offer the following points.

Section 215 Telephone Metadata Program.

The telephone metadata acquired by the NSA under the section 215 business records order consists only of tables of numbers indicating which phone numbers called which numbers and the time and duration of the calls. It does not reveal any other subscriber information, and it does not enable the government to listen to anyone's phone calls.

The Fourth Amendment does not require a search warrant or other individualized court order for the government to acquire this type of purely transactional metadata, as distinct from the content of communications. The acquisition of such call-detail information, either in bulk or for the communications of identified individuals, does not constitute a "search" for Fourth Amendment purposes with respect to the individuals whose calls are detailed in the records. The information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore consistently held that there is no reasonable expectation by the individuals making the calls that this information will remain private. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

In his recent decision granting a motion for a preliminary injunction of the metadata program, which is now stayed pending appeal, Judge Richard Leon of the federal district court in D.C. reasoned that the Supreme Court's decision in *Smith*

² See Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata under Section 215 and Foreign-Targeted Collection under Section 702*, 1 Lawfare Res. Paper Series No. 3 (Sept. 2013), available at <http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf>.

v. Maryland has become obsolete in the era of smartphones and fully functional wireless digital communications. But the calling-record data collected by the NSA is almost exactly the same data the police collected in *Smith*: the phone numbers dialed and the date and time of those calls. In *Smith*, the Court held that telephone customers have no reasonable expectation of privacy in these transactional records, and ever since the Court's 1967 decision in *Katz v. United States*, 389 U.S. 347 (1967), a reasonable expectation of privacy has been the measure for what constitutes a search under the Fourth Amendment. For that reason, the federal courts of appeals and all other district courts before Judge Leon have consistently followed *Smith* and applied its holding to other developing technologies, including the collection of e-mail metadata.³

Although Judge Leon's ruling emphasizes the "all-encompassing" and "indiscriminate" nature of the NSA's metadata collection, the breadth of the data collection does not alter anyone's reasonable expectations of privacy. If anything, the use of a pen register to target a single suspect's personal phone line, as occurred in the *Smith* case, is more intrusive than the NSA's metadata collection, given the vastness and anonymity of the data set and the minuscule chance that any particular person's calling records will be reviewed by an NSA analyst. In other words, the individual privacy interests of the tens of millions of telephone customers whose calling records are collected by the NSA are lessened even further, not increased, by the breadth of the database.

Judge Leon also cited the Supreme Court's 2012 decision in *United States v. Jones*, 132 S. Ct. 945 (2012), involving the GPS tracking of a criminal suspect, but that case is not germane. In *Jones*, the police trespassed on the suspect's property by installing a GPS device on his car and tracked his every move. The NSA's bulk collection, in contrast, entails no physical invasion of property and does not comprehensively track individual customers' movements and activities.

The NSA's acquisition of telephone metadata is also authorized under the terms of section 215, which 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 a link analysis of terrorist phone numbers, and this type of

³ *Accord Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-05 (9th Cir. 2008) (same analysis for email addressing information).

analysis is a critical building block in these investigations. Acquiring a comprehensive database is needed to enable effective 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 legal standard of relevance incorporated into section 215 is the same common standard that courts have long held governs the enforcement of administrative subpoenas, grand jury subpoenas, and document production orders in civil litigation, which, unlike section 215 business records orders, do not require the advance approval of a court.⁴

The Supreme Court has long held that courts must enforce administrative subpoenas so long as the agency can show that the subpoena was issued for a lawfully authorized purpose and seeks information relevant to the agency’s inquiry.⁵ This standard of relevance is exceedingly broad; it permits agencies to obtain “access to virtually any material that might cast light on” the matters under inquiry,⁶ and to subpoena records “of even *potential* relevance to an ongoing investigation.”⁷ Grand jury subpoenas are given equally broad scope and may only be quashed where “there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.”⁸ And in civil discovery, the concept of relevance is applied “broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case.”⁹

⁴ See 152 Cong. Rec. 2426 (2006) (Statement of Sen. Kyl) (explaining the “relevant to” language added to section 215 in 2006) (“Relevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders.”).

⁵ See *United States v. LaSalle Nat’l Bank*, 437 U.S. 298, 313 (1978); *United States v. Powell*, 379 U.S. 48, 57 (1964); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946).

⁶ *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984).

⁷ *United States v. Arthur Young & Co.*, 465 U.S. 805, 814 (1984) (emphasis in original).

⁸ *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

⁹ *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978).

The relevance standard does not require a separate showing that every individual record in a subpoenaed database is “relevant” to the investigation.¹⁰ The standard is satisfied if there is good reason to believe that the database contains information pertinent to the investigation and if, as here, the acquisition of the database is needed to preserve the data and to be able to conduct focused queries to find particular records useful to the investigation.¹¹ Similar subpoena authority is used by numerous different federal regulatory and law enforcement agencies, including the Securities and Exchange Commission, the Federal Trade Commission, the Consumer Financial Protection Bureau, and others, to conduct broad investigations of conduct within their statutory jurisdictions.

Of course, the NSA’s mission is far more important and essential than the mere regulatory missions of most other federal agencies because the NSA is charged with nothing less than the protection of our way of life from catastrophic foreign attack. The importance of the interest at stake informs any analysis of the reasonableness of the scope of data collected. The effective analysis of terrorist calling connections and the discovery through that analysis of new phone numbers being used by terrorist suspects, including previously undetected terrorist cells operating in the U.S., require the NSA to assemble and maintain the most comprehensive set of telephone metadata, and the section 215 order provides that unique capability.

¹⁰ See *In re Grand Jury Proceedings*, 616 F.3d 1186, 1202, 1205 (10th Cir. 2010) (confirming (1) that the categorical approach to relevance for grand jury subpoenas “contemplates that the district court will assess relevancy based on the broad types of material sought” and will not “engag[e] in a document-by-document” or “line-by-line assessment of relevancy,” and (2) that “[i]ncidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury’s broad investigative powers and the categorical approach to relevancy”).

¹¹ See, e.g., *In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000); *FTC v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987); *Associated Container Transp. (Aus.) Ltd. v. United States*, 705 F.2d 53, 58 (2d Cir. 1983). The same approach is sanctioned in the federal rules governing criminal search warrants. See Fed. R. Crim. P. 41(e)(2)(B) (“A warrant . . . may authorize the seizure of electronic storage media or . . . information” subject to “a later review of the media or information consistent with the warrant”); *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006) (sanctioning “blanket seizure” of computer system based on showing of need); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (sanctioning “seizure and subsequent off-premises search” of computer database).

While the metadata order is extraordinary in terms of the amount of data acquired, which is far greater than the amount of data involved in most other federal agency investigations, the metadata order is also extraordinarily narrow and focused because of the strict limitations placed on accessing the data. There's 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 cannot 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 five years are continually deleted from the system.

The order must be reviewed and reapproved every 90 days, and since 2006, this metadata order has been approved at least 37 times by at least 15 different federal judges. The telephone metadata program was also recently upheld as lawful in all respects in an independent decision by Judge William Pauley of the U.S. District Court for the Southern District of New York. The contrary analysis offered by three members of the Privacy and Civil Liberties Oversight Board in their recent report is entirely unconvincing.

In addition to court approval, the 215 program 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, the administration briefed the leaders of Congress and the members of these Committees on the details of this program. The administration also provided detailed written descriptions of the program to the chairs of the Intelligence Committees, and the administration requested that those descriptions be made available to all Members of Congress in connection with the renewal of section 215.

These briefing documents specifically included the disclosure that under this program, the NSA acquires the call-detail metadata for “substantially all of the telephone calls handled by the [phone] companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.”¹² Public reports indicate that the Intelligence Committees provided briefings on the details of the program to all interested Members of Congress, and the administration has conducted further detailed briefings on this program since the Snowden leaks became public.

Section 702 Collection.

The second NSA program revealed by the Snowden leaks—the foreign-targeted surveillance of international communications—is conducted under section 702 of FISA.

With court approval, section 702 authorizes a program of foreign-focused surveillance for periods of one year at a time. This authority may only be used if the surveillance does *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 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’s been disclosed about the foreign-targeted surveillance program, including the so-called PRISM Internet collection, it appears to be precisely what section 702 was designed to permit.

¹² Report on the National Security Agency’s Bulk Collection Programs for USA PATRIOT Act Reauthorization at 3, *enclosed with* Letters for Chairmen of House and Senate Intelligence Committees from Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, Department of Justice (Feb. 2, 2011). The identical disclosure was also made in a similar report enclosed with letters dated December 14, 2009.

The 702 program is also fully consistent with the Constitution. As a background principle, the Fourth Amendment does not require the government to obtain a court-approved warrant supported by probable cause before conducting foreign intelligence surveillance. The Supreme Court has reserved judgment on the question,¹³ but the courts of appeals have consistently held that the President has inherent constitutional authority to conduct warrantless searches and surveillance to obtain intelligence information about the activities of foreign powers, both inside and outside the United States and both in wartime and peacetime.¹⁴

The absence of a warrant requirement does not mean the Fourth Amendment has no application to foreign intelligence surveillance. Rather, searches and surveillance conducted in the United States by the executive branch for foreign intelligence purposes are subject to the general reasonableness standard of the Fourth Amendment. See *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995) (holding that the touchstone for government compliance with the Fourth Amendment is whether the search is “reasonable” and recognizing that the warrant requirement is inapplicable in situations involving “special needs” that go beyond routine law enforcement).

The reasonableness of foreign intelligence surveillance, like other “special needs” searches, is judged under a general balancing standard “by assessing, on the one hand, the degree to which [the search] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *United States v. Knights*, 534 U.S. 112, 118-19 (2001)

¹³ See *United States v. United States District Court* (the “*Keith*” case), 407 U.S. 297, 308 (1972) (explaining that the Court did not have occasion to judge “the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country”); *Katz v. United States*, 389 U.S. 347 (1967).

¹⁴ See, e.g., *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 914-15 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir.), *cert. denied sub nom. Ivanov v. United States*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974). But see *Zweibon v. Mitchell*, 516 F.2d 594, 619-20 (D.C. Cir. 1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation), *cert. denied*, 425 U.S. 944 (1976).

(quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). In the context of authorized NSA surveillance directed at protecting against foreign threats to the United States, the governmental interest is of the highest order. See *Haig v. Agee*, 453 U.S. 280, 307 (1981) (“It is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.”).

On that basis, prior to 1978, Presidents conducted surveillance of national security threats without court supervision. That practice led to the abuses that were documented by the Church and Pike Committees and eventually resulted in the passage of FISA.

FISA was enacted as an accommodation between Congress and the executive branch. It was designed to ensure the reasonableness of surveillance by requiring the approval of a federal judge for certain defined types of clandestine foreign intelligence surveillance conducted in the United States, instituting oversight of the process by the Intelligence Committees of Congress, providing for procedures to “minimize” the retention and dissemination of information about U.S. persons collected as part of foreign intelligence investigations, and regularizing procedures for the use of evidence obtained in such investigations in criminal proceedings.

Under FISA, electronic surveillance of persons in the United States for foreign intelligence purposes requires an order approved by a judge and supported by individualized probable cause to believe the target is an agent of a foreign power or engaged in international terrorism.

Ever since FISA was enacted, it’s been recognized that FISA raises significant constitutional issues to the extent it might impinge on the President’s ability to carry out his constitutional duty to protect the United States from foreign attack.

Importantly, in its original conception, FISA was not intended to govern the conduct of communications intelligence anywhere overseas or the NSA’s collection and surveillance of international communications into and out of the United States. FISA’s definition of “electronic surveillance” focuses on the interception of wire communications on facilities in the United States and on the interception of certain categories of domestic radio communications. See 50

U.S.C. § 1801(f). In 1978, most international calls were carried by satellite, and thus the statute's definition of "electronic surveillance" was carefully designed at the time to exclude from the jurisdiction of the FISA court not only all surveillance conducted outside the United States, but also the surveillance of nearly all international communications.¹⁵

FISA also exempted from statutory regulation the acquisition of intelligence information from "international or foreign communications" not involving "electronic surveillance" as defined in FISA,¹⁶ and this change, too, was "designed to make clear that the legislation does not deal with the international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."¹⁷ Congress specifically understood that the NSA surveillance that these carve-outs would categorically exclude from FISA included the monitoring of international communications into and out of the United States of U.S. citizens.¹⁸

In the years following the passage of FISA, however, communications technologies evolved in ways that Congress had not anticipated. International lines of communications that once were transmitted largely by satellite migrated to undersea fiber optic cables. This evolution increased greatly with the advent of the Internet. In the new world of packet-switched Internet communications and international fiber optic cables, FISA's original regime of individualized court orders for foreign intelligence surveillance conducted on facilities in the United States became cumbersome, because it now required case-by-case court approvals for the surveillance of international communications that were previously exempt from FISA coverage. Nevertheless, prior to 9/11, the executive branch found the FISA system to be adequate and workable for most national security purposes.

¹⁵ See S. Rep. No. 95-604, at 33-34, reprinted in 1978 U.S.C.C.A.N. 3904, 3934-36.

¹⁶ See Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), *codified at* 18 U.S.C. § 2511(2)(f) (1982).

¹⁷ S. Rep. No. 95-604, at 64, 1978 U.S.C.C.A.N. at 3965.

¹⁸ See *id.* at 64 n.63 (describing the excluded NSA activities by reference to a Church Committee report, S. Rep. No. 94-755, at Book II, 308 (1976), which stated: "[T]he NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans . . .").

All of that changed with the attacks of 9/11. In the estimation of the President and the NSA, the imperative of conducting fast, flexible, and broad-scale signals intelligence of international communications in order to detect and prevent further terrorist attacks on the U.S. homeland proved to be incompatible with the traditional FISA procedures for individualized court orders and the cumbersome approval process then in place. As the Justice Department later explained in a public white paper addressing the legal basis for the NSA's warrantless surveillance of international communications involving suspected terrorists that was authorized by special order of the President following 9/11, "[t]he President ha[d] determined that the speed and agility required to carry out the[se] NSA activities successfully could not have been achieved under FISA."¹⁹

The public disclosures in 2005 and 2006 concerning the President's authorization of warrantless surveillance by the NSA precipitated extensive debates and hearings in Congress. Ultimately, these debates culminated in passage of the FISA Amendments Act of 2008 and the addition of section 702 to FISA. Section 702 was designed to return to a model of foreign surveillance regulation similar to the original conception of FISA by greatly streamlining the court review and approval of a program of surveillance of international communications targeted at foreign persons believed to be outside the United States. Under section 702, such foreign-targeted surveillance may be authorized by the Attorney General and DNI without individualized court orders for periods of up to one year at a time upon the approval by the FISA court of the required targeting protocols and minimization procedures. *See* 50 U.S.C. § 1881a.

By establishing procedures for court approval (albeit more streamlined and "programmatic" approval than required for traditional individualized FISA surveillance orders) and by strengthening congressional oversight of the resulting program, section 702 continues to provide a system of foreign intelligence surveillance, including for international communications and surveillance targeted at foreign persons outside the U.S., that is more restrictive and protective than the Constitution would otherwise require.

¹⁹ U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* 34 (Jan. 19, 2006).

As publicly described, the NSA's section 702 program of foreign-targeted Internet surveillance easily meets the reasonableness requirements of the Fourth Amendment. The surveillance is conducted for foreign intelligence purposes, which carry great weight in the Fourth Amendment balance, and the retention and use of information collected in the program about U.S. persons are subject to extensive and detailed minimization procedures designed to protect the reasonable privacy interests of Americans, and these minimization procedures have been reviewed and approved by a federal court.

II. There Is Every Reason to Believe that the NSA Programs Remain Necessary to Protect the National Security of the United States and Its Allies

Both of the NSA programs discussed above are intended to provide quick and efficient detection and identification of contacts between suspected agents of foreign terrorist organizations and unknown operatives that may be hiding out within the United States. For my part, I believe that the need for such detection is just as acute today as it was in the immediate wake of 9/11. The President and both the Republican and Democratic leaders of the House and Senate Intelligence Committees firmly agree; otherwise, I'm confident that they would not support the continuation of these programs, in light of the public controversy the programs have generated following the Snowden leaks.

More specifically with regard to the 215 order, from all that I know, I have every confidence that the bulk acquisition of the telephone metadata is necessary to preserve the data for use in the FBI's counterterrorism investigations and to combine the call-detail records generated by multiple telephone companies into a single searchable database. Furthermore, the use of the entire integrated database is essential to conduct focused link analysis and contact chaining of terrorist phone numbers and thereby discover new terrorist phone numbers that we did not know about before.

It is necessary to retain the data for a sufficient period, such as five years, to be able to conduct historical analysis to find connections between newly discovered phone numbers and the numbers of previously identified terrorist agents that may have been the subjects of past investigations.

I believe that the 215 program provides a frequent and important input for ongoing investigations of terrorist activities. I don't believe the proper test of the program's necessity is whether it has provided the one primary piece of information required to thwart a specific terrorist plot just before an attack has been carried out. Any such narrow focus on the interdiction of particular mature plots is unrealistic because it does not take account of how these investigations are conducted and the fact that nearly all counterterrorism efforts involve numerous inputs from diverse sources over an extended period of time. A counterterrorism investigation is like assembling a jigsaw puzzle; every input is important, and it is rare that any one input can be identified as singularly critical.

A more suitable and relevant high-level metric of the program's utility might be to ask to following: For how many of the particular threat items reported to the President by the DNI in the President's Daily Intelligence Briefing ("PDB") has the section 215 telephone metadata program been used in developing the underlying investigation that resulted in that PDB item?

III. The Major Proposals for Curtailing or Modifying the NSA Programs and for Amending the FISA Authorities Should Be Rejected

I offer the following thoughts on why the President's reforms to the section 215 telephone metadata program and the other principal reform proposals, including legislative proposals, for modifying the authorities of the NSA under FISA should not be approved.

The most sweeping change under consideration, as I understand it, would restrict the government's authority under section 215 to acquiring on an item-by-item basis only those individual business records, including telephone call-detail records, that directly pertain to the person who is the subject of the counterterrorism investigation. A variation on this proposal would limit the NSA to conducting one-by-one queries of the call-detail databases of the phone companies only while the data is retained by the companies in the ordinary course of business.

Such requirements would kill the NSA's telephone metadata program, because they would, by design, deny the NSA the broad field of data needed to conduct in an efficient and workable manner the link analysis and contact chaining that is enabled by the current program.

At the same time, denying the NSA the authority to acquire the metadata in bulk and to retain it for a period of years would preclude any historical analysis of connections between a terrorist phone number and other, yet undiscovered numbers, and the ability to examine historical connections and patterns is among the most valuable capabilities of the 215 metadata program. Indeed, any proposal to limit the length of metadata retention to a period of less than the current five years should be approached with great care, because it would by definition diminish the capacity of the NSA to conduct this important historical contact analysis. I'm encouraged that the President has not proposed to limit the NSA's retention of the data to less than five years.

A less sweeping but still very significant restriction would prohibit the NSA from taking possession of the call-detail records obtained under the 215 order and would instead require that the data be maintained for an extended period under the control of the telephone companies, presumably at the expense of the federal government. This alternative was recommended by the President's Review Group, and the President indicated in his January 17 speech that he wishes to move the database to private hands and has tasked the Attorney General and DNI to study how that might be accomplished. At the same time, the President acknowledged the difficulties of doing so and the fact that this option may affect the speed and flexibility of the program and could exacerbate privacy concerns.

The current program enables the NSA to acquire all of the telephone metadata on an ongoing basis from several companies in order to preserve the data in a segregated and secure manner and combine it together in a form that is efficiently usable and searchable. Ceding control of the combined database to the phone companies would presumably require the involvement of a private, third-party contractor to house and manage the data, since no single phone company has the ability or inclination to maintain and aggregate all of the data of the several companies and host the data on servers for a sufficient period of years in a searchable form.

Today the database is locked down and kept secure and segregated by the NSA in the basement of Fort Meade. If the database were outsourced to a private contractor, it would in all likelihood be housed off-site, probably in some suburban office park, and it would certainly be kept on less secure servers. In that event, the

database would be far more vulnerable to privacy breaches and cyber incursions from foreign governments, terrorist groups, criminal organizations, and sophisticated hackers. Furthermore, unless Congress provided otherwise by statute, the data would be exposed to court-ordered discovery by private litigants in all manner of civil lawsuits. The private contractors with access to the database would also be much less subject to effective oversight by the executive branch, the FISA court, and Congress.

Any such arrangement involving a third-party contractor, therefore, would be distinctly less efficient, less secure, and less subject to effective oversight than the current program. That result cannot be a desirable one, both in terms of national security and in terms of the privacy of the data and the potential for its abuse.

Another proposal recommended by the Review Group and reflected in some bills pending in Congress would require prior FISA court approval for querying the telephone metadata—in other words, a prior court determination that there is reasonable articulable suspicion that the phone number to be queried against the database is associated with one of the specified foreign terrorist organizations. The President has ordered the NSA to put in place some version of this proposal, subject to the Attorney General’s working out acceptable procedures in consultation with the FISA judges. Depending on how it’s implemented, such a requirement would place a significant and potentially unwieldy restraint on the speed and flexibility of the program, particularly if it requires one-by-one court approval of each query, and will likely place a substantial new burden on the operations of the FISA court. If applied to the “hops” from the original seed number, for example, this requirement of prior court approval would throttle the utility of the program entirely.

The President has also ordered that the NSA not analyze calling records out to the third “hop” from the seed number. This change, too, poses a significant risk of diminishing the speed, flexibility, and utility of the program, since, as I understand it, the NSA currently analyzes third-hop data only where the Agency identifies a specific intelligence reason for doing so. Why needlessly prevent the NSA from pursuing valid and potentially important intelligence leads or interpose a new requirement of court approval before the NSA may do so?

Moreover, requiring court approval of each reasonable articulable suspicion determination before the NSA may access the database would impose a legalistic judicial overlay on a judgment that is designed to be made by and is far more appropriately made by seasoned intelligence analysts. Insisting on prior court approval will inevitably require the involvement of more and more lawyers as intermediaries between the intelligence officers and the judges of the court and will inevitably involve the translation of reasonable suspicion determinations into more and more paper in order to communicate the real-time intelligence judgments of NSA professionals into the language understood by the judges and their legal advisers. The alternative included in some legislative proposals of requiring approval by the lawyers of the National Security Division of the Justice Department would suffer from the same defect: It would interpose a lawyer's sensibility in place of the practical judgment of intelligence professionals.

One further proposal often raised is to attempt to graft onto the traditionally *ex parte* procedures of the FISA court a litigation-like adversary process—for example, by creating the position of a “Public Advocate” for the FISA court. Under certain of these proposals, the Public Advocate would be charged with representing the “public interest” or the “privacy interests” of the targets of the surveillance and would be expected to oppose the government’s applications, at least in cases raising novel interpretations of FISA or asking to extend the law beyond how it has previously been applied. One such proposal would require that the Public Advocate receive a copy of each application for a FISA order and would give the Public Advocate the independent right to decide when to intervene and even the right to appeal any FISA order approved by the court.

This concept of introducing a Public Advocate with independent authority and appeal powers into the FISA process raises serious constitutional concerns. Because the review of FISA applications requires access to the most sensitive national security information, including both current threat assessments and descriptions of the proposed intelligence operations, any appointed advocate would have to be a permanent, trusted officer of the executive branch or of the FISA court with the necessary security clearances. Constitutional issues would arise in any statutory mandate that the President invariably permit the Public Advocate to have access to such sensitive classified information. The protection of national security secrets is a duty the Constitution assigns exclusively to the President; Congress may not direct the exercise of this duty by statute. Constitutional issues would also

follow if the Public Advocate were given the power to appeal a decision of the FISA court over the objections of the executive branch.

Moreover, introducing such an advocate position would not likely achieve the meaningful benefits that proponents hope for. The judges assigned to the FISA court are already assisted by permanent legal advisers who are steeped in the precedents of the court and whose job is to second guess the arguments and analyses of the executive branch. If a particular FISA application raises significant questions, the legal advisers are already asked to prepare separate, in-depth analyses for the judges. The recently disclosed opinions of the FISA court convincingly show that the judges of the court and their legal advisers are not shy about applying a thoroughly independent review of the issues that is in no way beholden to the executive branch. If a Public Advocate were part of the executive branch, the advocate would always ultimately be answerable to the President. If employed by the court, the advocate would be little different from the existing legal advisers. Either way, the Public Advocate could never actually be a true independent adversary representing the interests of those under surveillance.

The President evidently disapproves the idea of a more formal Public Advocate, as described above. Instead, he has announced his support for the formation of a “panel” of pre-cleared advocates who could be called upon by the FISA judges to submit briefs—presumably only in the form of amicus briefs—on significant issues facing the court. This proposal may be unobjectionable, if it leaves to the FISA judges the decision to call for amicus input from a member of the panel where the judges believe a particular application merits such independent input and if leaves to the President and the executive branch the authority to grant security clearances to the panel members and to decide what sensitive intelligence information is appropriate for sharing with the amicus in a particular case.

Furthermore, it must be recognized that any requirement that the panel of outside amici be granted access to classified information will have the potential to chill the executive branch’s willingness to share the sensitive details of national security operations and intelligence information relevant to particular FISA applications. As Judge John Bates recently pointed out in his letter on behalf of all current and former judges of the FISA court, such a disincentive would threaten to hamper the important relationship of trust and confidence that currently exists

between the National Security Division of the Justice Department and the FISA court. It should be a top priority of this Committee to avoid that result.

One final observation that I believe is important to keep in mind: Many of the reform proposals discussed above, including those that would attempt to convert the FISA process into an adversary proceeding and those that would impose more frequent judicial approvals or bureaucratic processing of decisions heretofore made in real time by intelligence analysts, would run the risk of recreating the type of cumbersome, over-lawyered foreign intelligence regime that proved so inadequate in the face of 9/11.

Those currently in positions of responsibility in the Intelligence Community and the Members of this Committee and the Intelligence Committees who are briefed on the latest threat reporting know far better than I how likely it is (or rather how inevitable) that America will suffer another catastrophic terrorist attack at some point in the years ahead. In the event of such an attack, I fear that the constrained and lawyerly process for conducting signals intelligence required under the most intrusive reform proposals would prove inadequate, and the President, any President, would be forced once again to fall back on his Article II authority to conduct the effective surveillance he determines necessary to protect the country from follow-on attacks. Indeed, I believe the American people would demand no less.

That cannot be a result this Congress would prefer. But it is, unfortunately, a very real possibility if several of the proposals currently under consideration were to be adopted.

Mr. GOODLATTE. Thank you, Mr. Bradbury.
Mr. Cole, welcome.

**TESTIMONY OF DAVID COLE,
GEORGETOWN UNIVERSITY LAW CENTER**

Mr. DAVID COLE. Thank you, Mr. Chairman, Ranking Member, for inviting me here to testify.

I want to make three brief points in my opening remarks. First, that technological advances employed by the NSA raise substantial privacy and liberty concerns and demand new legal responses if we are not going to forfeit our privacy by technological default. Second, that Congress is particularly well situated to adopt rules to protect Americans' privacy in the digital age. And third, that the USA FREEDOM Act, sponsored by Representative Sensenbrenner and Senator Leahy, is an excellent start toward restoring the privacy and the accountability that has been infringed by NSA practices.

First, the NSA metadata program illustrates the profound threat to our privacy and to our associational freedoms brought on by the capabilities of the digital age. At the time of the framing or even 50 years ago, if the Government wanted to know what we read, what we listened to, who we spoke and associated with in the privacy of our home, they would have to get a warrant based upon probable cause.

Today, virtually everything we do in the home and out, including what we read, with whom we associate, where we go, and even what we are thinking about leaves a digital trace that reveals the most personal details of our lives.

According to the Administration's interpretation of Section 215, there is no limit on the Government getting these digital details of our lives, whether they be phone records or email records or Internet browsing data records or business or bank records. There is no limit on their ability to get them because they might at some point be useful to search through for a connection to terrorism.

According to the Government's reading of the Fourth Amendment, the Fourth Amendment provides no constitutional limit on the Government's ability to get all of this data about all of us because, by sharing it with Google or AT&T or Verizon, we have forfeited our—any interest in privacy that we might have.

But many people who have looked at this problem, including President Obama, including the President's review group, including the Privacy and Civil Liberties Oversight Board, including Justice Alito, including Justice Sotomayor, and including Justice Scalia, have said and acknowledged that when technology advances in this way, it is critical that we adapt our laws to ensure that we retain the privacy that we had at the time of the framing.

We're in a brave new world. And unless we adapt our laws to reflect that fact, we will effectively forfeit the privacy that is so critical to our own human relations and to a free and open democracy.

Second, Congress is well situated to act. As Justice Alito said in the Jones case, a legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way. When it comes to adjusting law to deal with advances in technology, Congress has historically done so, and it has historically done so where the Supreme Court

has either declined to protect Americans' privacy or failed to address sufficiently Americans' privacy.

So when the Supreme Court said the Fourth Amendment does not protect the privacy rights of people vis-a-vis pen registers, Congress responded by enacted statutory limits on the Government's use of pen registers. When the Supreme Court said we have no privacy rights in our bank records, Congress responded by enacting the Right to Financial Privacy Act. FISA itself imposes restrictions on the Government's ability to gather information that the court has not yet said is constitutionally protected.

That intervention is necessary here because the Administration has essentially interpreted Congress' prior law to give it *carte blanche*. I was around when we debated the changes on the PATRIOT Act, and I am absolutely certain that had the Administration come to Congress and said we'd like to amend the business records law, which at that time allowed the Government to get records on specific targets, and we'd like to amend it by giving us the authority to get records, phone records and other business records on literally every American and amass them in a single database and keep them for 5 years, there is no way that this Committee would have approved of that. There is no way that this Congress would have approved of that.

And yet that's the interpretation that the Administration has put on this law in secret. And therefore, I think it's critical that Congress respond, and I think the USA FREEDOM Act, by ending dragnet collection and requiring a nexus between business records sought and terrorism investigations, is the best way to go.

Thank you very much.

[The prepared statement of Mr. David Cole follows:]

Testimony of Professor David Cole
Georgetown University Law Center
Before the Judiciary Committee of the United States House of Representatives
“Recommendations to Reform Foreign Intelligence Programs”

February 4, 2014

INTRODUCTION

Chairman Goodlatte, Ranking Member Conyers, and members of the Committee, I appreciate the opportunity to testify today on proposals to reform foreign intelligence gathering.¹ Since June 2013, the American public, and the world at large, have learned of a dizzying array of previously secret surveillance activities carried out by the National Security Agency (NSA) – some of them authorized by Congress, many of them apparently carried out exclusively under Executive Order 12333. Whatever one thinks of Edward Snowden’s acts in revealing these programs, one thing is beyond dispute: the disclosures have touched off the most significant debate on the appropriate limits of surveillance this country – and possibly the world at large – has ever before undertaken.

While these programs remained secret, they were maintained by the executive branch, approved by the judiciary, and reauthorized (albeit in most cases, unknowingly) by Congress. Now that the programs have become public, all three branches of government have begun to reassess what they previously tolerated as long as they remained secret. President Obama appointed an expert Review Group to study the issue, and that Review Group, which featured the former counterterrorism adviser to the National Security Council and the former acting director of the CIA, recommended 46 reforms to rein in the NSA and increase transparency, accountability, and ultimately, trust among the American people and the world at large.² The President himself delivered a national speech last month on the subject, and adopted some of his Review Group’s recommendations.

The Privacy and Civil Liberties Oversight Board has issued its own substantial report, focused on the Section 215 telephone records program and the Foreign Intelligence Surveillance Court, and has urged termination of the bulk collection of metadata.³ Notably, the Privacy Board examined classified evidence and held classified briefings on the effectiveness of the program,

¹ I am a professor at Georgetown University Law Center, but appear before you today in my personal capacity.

² Liberty and Security in a Changing World, Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies (hereinafter “Review Group Report”), Dec. 12, 2013, available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

³ Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (hereinafter “Privacy Board Report”), Jan. 23, 2014, available at <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf>.

and concluded that its security benefits have been, in seven years, marginal at best. It found that the program has not led to the disruption of any act or attempted act of terrorism. The only instance in which the Section 215 phone records program has led to the discovery of a single otherwise unknown person charged with a terrorist crime involved an attempt to send money to Al Shabaab, a Somali organization, in violation of prohibitions on material support to that group. The Privacy Board recommends termination of the bulk phone records collection, because it finds that it was not authorized by statute in the first place, and because the risks it poses to privacy outweigh the benefits to security that it has provided.⁴

The courts have also begun to question the program. Judge Richard Leon of the U.S. District Court for the District of Columbia, has ruled that the program is likely unconstitutional.⁵ Judge William Pauley of the Southern District of New York has reached an opposite conclusion.⁶ Both cases are pending on appeal. Remarkably, the Foreign Intelligence Surveillance Court (FISC) itself issued no opinion on the lawfulness of the program when it initially authorized the program in May 2006. Nor did the FISC address the legality of the bulk metadata program on any of the subsequent occasions when, every 90 days, it reauthorized the program. In fact, the FISC did not write an opinion explaining its rationale until August 2013, many years after it had approved the program, and not coincidentally, two months after Edward Snowden disclosed the existence of the program.

Congress, meanwhile, is considering multiple bills proposing to rein in aspects of the NSA program. I support the bill introduced by Representative Jim Sensenbrenner and Senator Pat Leahy, the USA Freedom Act. It would make many changes, but among the most important is an amendment of Section 215 of the USA Patriot Act to require that the government show some nexus between the business records it seeks and a person or persons properly targeted for a foreign intelligence investigation. This would permit the NSA to obtain data related to suspects, but would not permit it to engage in bulk collection of every American's business records. The bill would restore an approach to privacy that has governed in this country since its founding – namely, the notion that the government should only invade privacy where it has some individualized objective basis for suspicion. It would end the dragnet collection of records about ordinary, law-abiding Americans who have no connection to terrorism, while retaining the ability of the government to gather information on those it has reason to believe are so connected.

The above activity by the three branches of government is in turn a reflection of the widespread public concern that has been expressed about the NSA's activities, both at home and abroad. For the first time since many of these programs' secret inception, the American people, and indeed the world at large, have had the opportunity to consider whether the NSA's activities accord with our most fundamental values of privacy, liberty, and equality. The last seven months of revelations have demonstrated that technology has advanced far beyond the law,

⁴ Two members of the Privacy Board dissented from this recommendation.

⁵ *Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925 (D.D.C. Dec. 16, 2013).

⁶ *ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863 (S.D.N.Y. Dec. 27, 2013).

affording the government the ability to construct detailed portraits of the most intimate associations, beliefs, and desires of any of us. Perhaps understandably, the NSA has sought to exploit these capabilities as aggressively as possible. After all, its mandate is to gather intelligence, not to balance security and privacy.

But the revelations also demonstrate that unless the law is adapted to catch up to technological change, we are at risk of forfeiting our privacy by default. This truth has been recognized by President Obama in his NSA speech, by his expert Review Group, and by the Privacy and Civil Liberties Oversight Board. It's been recognized by scholars across the country. And it's been recognized, in different contexts, by most members of the Supreme Court. Just as privacy laws had to adapt to the invention of the automobile, the telephone, the beeper, the GPS, and the thermal imaging device, so, too, they need to adapt to the government's increasing ability to use computers to collect and analyze massive amounts of digital data about all of us.

Congress has a critical role to play in adjusting the law to reflect the challenges of technology. As Justice Samuel Alito noted in the Supreme Court's most recent foray into this area, *United States v. Jones*, 132 S. Ct. 945, 964 (2012), "a legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." Unlike a court, Congress can consider the problem from a broader perspective. Congress can respond more quickly than the courts. And Congress may have a better sense of the privacy demands of the American people. Thus, Congress has in the past often responded to Supreme Court decisions that did not extend Fourth Amendment protection to particular forms of investigation by imposing statutory limits that protect the American people's privacy.

My testimony will focus the NSA's telephone records program, and will consist of three parts. First, I will underscore the substantial privacy concerns raised by bulk collection of digital data, and show why current legal limits are insufficient to preserve privacy. Second, I will discuss the importance of a Congressional response. And third, I will state why I think the Sensenbrenner-Leahy bill is a fitting response to the current situation.

I. THE PRIVACY AND ASSOCIATIONAL ISSUES AT STAKE

As President Obama, his expert Review Group, and the Privacy and Civil Liberties Oversight Board all agreed, technology in the digital age poses significant risks to the privacy that all of us hold dear. The Constitution's framers, recognizing that privacy is the lifeblood of democracy, enacted the Fourth Amendment to prohibit general warrants and unreasonable searches and seizures. It is no less true today that privacy is essential to a functioning democracy and a healthy community. Now, as then, privacy is critical for the intimacy that is necessary to human flourishing. Now, as then, privacy affords the breathing room necessary for those who dissent

from the majority to gather together, express their views, and engage in political activity. As George Orwell and Ray Bradbury have shown, a society without privacy is associated with totalitarianism, and is not one in which any of us would want to live.

But if privacy is no less essential today than it was at the time of the Constitution's framing, it is much less secure. If, at the time of the framing, the government wanted to know what an individual in the privacy of his home read and wrote, and with whom he associated, it would have to obtain a warrant to search his home. Even with a warrant, the government generally had no way of knowing an individual's innermost beliefs or desires.

Today, by contrast, without a warrant or individualized suspicion, the government can learn what one reads, writes, with whom one associates, and even what one desires, simply by collecting "business records" – the records of internet service providers, phone companies, banks, credit card companies, libraries, and the like. In the modern age, nearly everything we do leaves a digital trace. As the President's expert Review Group noted, quoting the National Academy of Sciences, the "essence of the information age," is that everyone leaves "personal digital tracks ... whenever he or she makes a purchase, takes a trip, uses a bank account, makes a phone call, walks past a security camera, obtains a prescription, sends or receives a package, files income tax forms, applies for a loan, e-mails a friend, sends a fax, rents a video, or engages in just about any other activity."⁷

President Obama similarly noted the ability of computers to obtain such information, and the privacy concerns that capability raises. As he stated,

Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer or smartphone. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached.⁸

Yet according to the administration, it can collect all such data as "business records" under Section 215 of the Patriot Act -- without establishing *any* particularized connection between the individuals whose records are sought and a terrorist investigation. And according to the administration, the Fourth Amendment imposes *no limitation* whatsoever on its doing so, because in its view all of us have forfeited our privacy by sharing this information with "third parties" – the businesses that make these services available. The fact that one cannot live in modern America without using these services, the administration contends, is immaterial.

⁷ Expert Review Group Report at 110.

⁸ Remarks by the President on Review of Signals Intelligence, Jan. 17, 2014, available at <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>.

This is a very troubling development for those who believe, as the framers did, that privacy is essential to democracy. As Justice Alito recognized in *United States v. Jones*, which involved the use of much less sophisticated technology -- a GPS -- to monitor the public travel of an automobile for 28 days, our privacy has long rested as much on the practical difficulties of tracking us as on any legal protections:

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case--constant monitoring of the location of a vehicle for four weeks--would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.⁹

Just as the GPS makes it cheap to monitor citizens' public travel, so the proliferation of digital information about almost every interaction we have, coupled with advances in computer technology, make it possible to collect and aggregate massive amounts of personally revealing data about all of us. If privacy laws are not adapted to take these developments into account, privacy as we have long known and cherished it will not survive.

The NSA program's defenders invariably claim that the phone records program poses less of a danger to privacy because it collects only the metadata about our phone calls -- who we call, who calls us, when we talk, and for how long -- rather than the content of the calls themselves. But former NSA general counsel Stewart Baker has admitted that metadata can be at least as revealing as content itself. He stated:

Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.... [It's] sort of embarrassing how predictable we are as human beings.¹⁰

Justice Alito is not the only one to recognize this risk that new technologies pose to our privacy. In the same *Jones* case, Justice Sotomayor wrote that:

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its

⁹ *Jones*, 132 S. Ct. at 963-64 (Alito, J., concurring).

¹⁰ Alan Rusbridger, "The Snowden Leaks and the Public," *The New York Review of Books*, Nov. 21, 2013 (quoting Stewart Baker).

unfettered discretion, chooses to track--may "alter the relationship between citizen and government in a way that is inimical to democratic society."¹¹

And more than a decade earlier, in *Kyllo v. United States*,¹² Justice Scalia, writing for the Court majority, similarly recognized the need to adapt the law to preserve traditional expectations of privacy from advances in technology. In that case, the Court ruled that the use of a thermal imaging device to measure heat emanating from the exterior of a house constituted a search. Justice Scalia warned that "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."¹³ Extending the Fourth Amendment to such practices, he explained, "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."¹⁴

In sum, technology has made it possible for the government to know more about us than was even thinkable at the time of the framing. The erosion of practical limits on dragnet surveillance renders legal constraints all the more important. Yet according to the administration's interpretation of existing law, there are few if any legal limits on its ability to collect bulk data on Americans. The Constitution, it has argued, poses no impediment to gathering such information, because under the "third-party disclosure rule" we have all forfeited our expectations of privacy in this information. And there are no substantial statutory limits because, again according to the administration, Section 215 of the USA Patriot Act affirmatively empowers it to gather such data about all of us if it might be useful, at some future point, to search through it for ties to terrorists. The issue goes far beyond telephone data. The same argument would apply to cell phone location data, internet browsing histories, email addressing data, and financial and credit information, and library records. The administration's view of existing law recognizes virtually no limits on the administration's ability to collect and maintain a vast database on everyone.

II. THE NEED FOR CONGRESSIONAL ACTION

Congress can and should do something about this, by amending the statute that the NSA relies on for its expansive exercise of surveillance power. Congress has repeatedly acted in the past to protect citizens' privacy, while preserving the ability of law enforcement and intelligence agencies to do their jobs responsibly and effectively. It can and should do so again.

As noted above, Justice Alito has expressly noted that Congress is well situated to adjust privacy laws to respond to advances in technology. In fact, Congress has often enacted statutes to protect privacy when the Supreme Court has either not yet addressed the issue, or has ruled that the Constitution's Fourth Amendment itself does not provide protection. Thus, when the

¹¹ 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (CA7 2011) (Flaum, J., concurring)).

¹² 533 U.S. 27 (2001).

¹³ 533 U.S. at 34.

¹⁴ *Id.*

Supreme Court ruled in *Smith v. Maryland*, 442 U.S. 735 (1979), that “pen registers” did not invade Americans’ expectation of privacy, and therefore could be obtained without any Fourth Amendment limitations. Congress enacted statutory restrictions on the use of pen registers. Specifically, 18 U.S.C. § 3122 requires government officials to obtain a court order before installing a pen register, based on a showing that “information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.”

Similarly, when the Court ruled in *United States v. Miller*, 425 U.S. 435 (1976), that citizens had no constitutionally protected expectation of privacy in their bank and credit records, meaning that the government could get them without court approval or any showing of necessity or suspicion, Congress enacted the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq., which provided statutory protections for citizens when the government seeks to obtain their bank and credit card records.

Congress has protected the privacy of video rental records, requiring a warrant, subpoena, or court order for the disclosure, even though the Court’s “third-party disclosure” rule would likely deny constitutional protection to such records. 18 U.S.C. § 2710.

When the Supreme Court in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), declined to interpret the Fourth Amendment to impose any special restriction on the government’s ability to search innocent third parties or the press for evidence of crime, Congress enacted the Privacy Protection Act of 1980, 42 U.S.C. § 2000aa, which afforded both innocent third parties and the press protections as a statutory matter that the Supreme Court had refused to provide as a constitutional matter.

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., regulates the government’s ability to conduct wiretaps and searches for foreign intelligence gathering purposes, despite the fact that the Supreme Court left open whether foreign intelligence gathering is subject to Fourth Amendment restrictions.¹⁵

Section 215 of the USA Patriot Act itself imposes statutory restrictions on access to business records that might otherwise fall under the “third-party disclosure” rule, and therefore might not be subject to Fourth Amendment limitations.

And Section 702 of the FISA Amendments Act of 2008, 50 U.S.C. § 1881a, imposes statutory restrictions on surveillance directed at foreign nationals living abroad, even though the Supreme Court has ruled that at least in some circumstances, the Fourth Amendment does not limit the government’s ability to search foreign nationals outside the United States.¹⁶

Thus, Congress has a long record of affording more protection to Americans’ privacy than the Supreme Court has interpreted the Fourth Amendment to provide. In some scenarios,

¹⁵ *United States v. United States District Court*, 407 U.S. 297, 308 (1972).

¹⁶ *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

Congress acted in response to Supreme Court decisions that at least arguably were insufficiently attentive to privacy demands. In other settings, Congress acted to fill a gap where the Supreme Court had failed to clarify the extent of Fourth Amendment protection, if any. In any event, this history demonstrates that Congress plays an essential role in safeguarding the privacy of Americans, and that it plays a role that is distinct from that played by the Court.

There is a particular need for congressional action here, because the executive and the FISC have interpreted an existing statute, Section 215, in ways that few if any members of Congress would have supported. That statute authorizes the government to obtain a court order for the production of business records only where they are “relevant to an authorized [foreign intelligence] investigation.” As the Privacy and Civil Liberties Oversight Board has convincingly and exhaustively demonstrated, Section 215’s requirement that only records “relevant to an authorized investigation” does not support the collection of all telephone metadata on every American, as the NSA has been collecting.¹⁷

The government has argued – and the FISC has accepted¹⁸ -- that collecting all Americans’ phone records and maintaining them for five years is “relevant” to a terrorism investigation because at some future time the government might want to search those records for links to terror suspects. In other words, all of our phone numbers are “relevant” not because any of us has any connection to terrorism, but because the NSA might someday find it useful to search through them all for as yet unspecified links to terrorism.

On this theory, the Privacy Board noted, “virtually all information may be relevant to counterterrorism and therefore subject to collection by the government.” (60) Indeed, “while terrorists use telephone communications to facilitate their plans they also write emails, open bank accounts, use debit and credit cards, send money orders, rent vehicles book hotel rooms, sign leases, borrow library books, and visit websites.”¹⁹ On the administration’s view of Section 215, it could collect records on all American’s email, internet, banking, credit, and library activities, because at some point those records might be useful to a terrorism search. There is no limiting principle. Yet surely Congress intended to impose a limit of relevance when it authorized not the collection of all business records of all Americans, but only of records “relevant to an authorized investigation.” Yet the administration’s interpretation renders meaningless the restriction of obtainable documents to “relevant” records. As the Privacy Board put it, this interpretation

¹⁷ Privacy Board Report, at 57-102.

¹⁸ NSA defenders often claim that 15 federal judges of the FISC court have ruled that the Section 215 program is legally authorized. In a very technical sense, that may be true. But it is misleading, because all but one FISC judge never actually wrote an opinion assessing the legality of the program. Instead, as noted in the Introduction, the FISC approved of the telephone records program in May 2006 without offering any explanation for its rationale, and until August 2013, none of the many judges who routinely approved of the program’s extension at 90-day intervals offered any explanation for their rationale. The only FISC judge who has actually set forth a rationale for finding the program legal is Judge Claire Eagan, on August 29, 2013, two months after the program was revealed to the public. Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Agu. 29, 2013).

¹⁹ Privacy Board Report at 62.

“supplies a license for nearly unlimited government al acquisition of other kinds of transactional information.”²⁰

In addition, as the Privacy Board has demonstrated, the government’s novel construction of “relevant” finds no support in any of the analogous situations in which the government or private parties are authorized to obtain “relevant” documents. The government has cited to no grand jury subpoena or civil discovery order in the history of American litigation that has authorized the collection of records on every American.²¹

The administration’s interpretation of Section 215 also conflicts with other statutes that impose more stringent restrictions on collection of the very same data that the NSA has been gathering under Section 215. For example, another section of FISA, 50 U.S.C. §1842, authorizes the use of “pen registers” and “trap and trace” devices to collect the same phone data that the NSA is now gathering under Section 215. Yet §1842 restricts the use of pen registers and trap and trace devices to specified phone numbers.²² The administration’s interpretation of Section 215 effectively allows it to evade the requirements of the pen register provision and get the same information on every American without specifying anyone’s numbers as a target.

The administration’s reading of Section 215 also conflicts with the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 et seq., which expressly addresses phone and other electronic communication records and states that a provider “shall not knowingly divulge a record or other information pertaining to a subscriber to or to a customer of such service ... to any governmental entity” except pursuant to specifically enumerated circumstances.²³ The enumerated circumstances do *not* include a court order under Section 215 (but do include a court order under ECPA).

Thus, the administration’s interpretation of Section 215 is at odds with the plain language of the statute, with all precedent interpreting the term “relevant” in analogous settings, and with other parts of FISA and ECPA. Yet in defense of its counterintuitive interpretation, the administration has cited to no evidence that at the time Congress amended Section 215 even a single member of Congress thought that the statute was giving the NSA authority to collect business records on every American. To the contrary, Representative Sensenbrenner, one of the Patriot Act’s architects in the House, has stated that he never intended to authorize such dragnet collection when authorizing the FBI to obtain business records “relevant to an authorized investigation.”²⁴

²⁰ *Id.*

²¹ *Id.* at 63-81 (reviewing interpretation and application of “relevance” in civil discovery, grand jury subpoenas, and administrative subpoenas).

²² See 50 U.S.C. § 1842(d)(2)(A)(iii).

²³ 18 U.S.C. §§ 2702(c), 2703(c).

²⁴ See, e.g., Letter of Sensenbrenner to Attorney General Eric Holder, Sept. 6, 2013, available at http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

Congress should act now in order to make clear that it did not intend to give the government access to all Americans' phone records, and more fundamentally, to ensure that Americans do not forfeit their privacy by default simply through advances in technology and secret interpretations of law.

III. THE USA FREEDOM ACT

The USA Freedom Act would end the NSA's bulk collection of phone records, and ensure that the government cannot secretly collect other records of Americans' private activities in bulk. It would amend Section 215 to authorize collection of business records only where the government could show that they pertain to a foreign agent or foreign power, the activities of a suspected agent of a foreign power, or an individual in contact with or known to a suspected agent of a foreign power. Thus, it would allow the government to seek business records in order to confirm or deny potential connections between suspected terrorists and foreign agents, on the one hand, and Americans on the other. But it would require the government to do so through targeted inquiries, not dragnet collections and searches that amass records on the private activities of every American.

The USA Freedom Act would sensibly impose the same restriction on National Security Letters and pen registers and trap and trace orders, to ensure that these authorities do not become end runs around the limits on Section 215. As the President's Review Group noted, National Security Letters allow the FBI to obtain without any court review some of the same business records that, under Section 215, require a court order. Of even greater concern, however, is that the NSL statute uses the same "relevance" standard used in Section 215. If the administration reads that standard to permit unlimited collection of business records under Section 215, the NSL authority could also be used just as broadly. Accordingly, the USA Freedom Act would amend these statutes by adding the same nexus requirement that it would add to Section 215.

These amendments, which are consistent with the Privacy Board's recommendation to terminate bulk collection, are preferable to the approach taken by President Obama in his NSA speech. There, he proposed that Americans' phone records would continue to be collected in bulk, but held by some private entity, to be identified later. Leaving the data in the hands of a private entity, however, does not solve the problem presented by dragnet collection of private information. Under the President's proposal, dragnet collection would continue. The focus of reform should be on ending dragnet collection altogether, and requiring law enforcement and intelligence agencies to use the targeted approach that the Constitution requires, and that maintains respect for Americans' privacy while at the same time affording government the tools to keep us safe. That is the approach the USA Freedom Act takes.

The USA Freedom Act also contains several measures that would increase transparency and accountability with respect to foreign intelligence gathering. These are critically important

reforms. As the revelations of the last several months have made clear, when intelligence agencies and the FISC operate entirely in secret, they are prone to adopting expansive measures that would likely be unacceptable if subjected to public scrutiny. There is of course a legitimate place for secrecy with respect to intelligence gathering. The American public does not need to know the details of every wiretap or order authorizing the collection of specific business records. But when the government adopts surveillance practices that affect literally every one of its citizens, and does so entirely in secret, secrecy has gone too far. As long as the telephone metadata program was secret, neither the executive, the courts, nor Congress did anything to stop it. Now that it has been revealed to the public, the President has proposed reforms, one court has declared the program likely unconstitutional, and Congress is considering numerous bills to rein in the NSA. That course of events illustrates the problem with secrecy. The institutional checks and balances established by the Constitution are important safeguards of liberty, but as this episode has revealed, they are insufficient without the light of public scrutiny.

In order to focus on the Section 215 program, I have not addressed other reforms in the USA Freedom Act, including new limitations on Section 702 of the FISA Amendments Act, and reforms to the FISC. I support those reforms as well, but will leave to others more extended discussion of them.

CONCLUSION

Three principles should guide Congress as it confronts the challenge of regulating foreign intelligence surveillance. First, we should not let advances in technology deprive us of our privacy by default. We can enjoy the tremendous advantages and conveniences of the digital age and still preserve our privacy. But in order to do so, Congress must enact rules to limit the power of new technologies to impose dragnet surveillance on all of us through the bulk collection of data revealing personal information. Second, Congress is especially well suited to enact the rules necessary to preserve privacy in the digital age, as it can consider the issues in a more wide-ranging way than the courts, and historically has had a better sense of the privacy that Americans expect. And third, the principle that has long been used to balance privacy and security – that the government’s security interests permit intrusions on privacy when the government develops individualized suspicion – remains the appropriate guidepost as we go forward. The very fact that the government has so little to show in terms of security benefits from seven years of collecting every American’s phone records underscores that this sort of dragnet approach is not necessary to our security.

Privacy remains just as essential today as it was when the Fourth Amendment was adopted. But the challenges to maintaining privacy are much more substantial, because technology has given the government the tools to invade our privacy in ways that were inconceivable a generation ago. If we are to preserve the privacy that remains critical to a healthy democracy, Congress must act.

Mr. GOODLATTE. Thank you, Mr. Cole.

Mr. Garfield, I don't know how the introductions and the seating got reversed there. Our apologies to you, but you get the last word of the testimony. Then we are going to take a recess to go vote, and we will come back and ask questions of all members of the panel.

**TESTIMONY OF DEAN C. GARFIELD,
INFORMATION TECHNOLOGY INDUSTRY COUNCIL**

Mr. GARFIELD. Thank you, Chairman Goodlatte, Ranking Member Conyers.

On behalf of some of the most dynamic and innovative companies in the world, we thank you for hosting this hearing and for inviting us to testify.

My testimony today will be infused with a healthy dose of humility because we recognize that the phrase, "We don't know what we don't know," is particularly apt in the area of national security. That being said, given the multinational and multisectoral nature of the tech sector and our business, we know we have something important to contribute to this conversation.

As you instructed, rather than repeating my written testimony, which has been submitted for the record, I'll focus on the economic impact; second, the societal implications; and then, third, offer some solutions.

With regard to the first, the economic impact is significant and ongoing. We live in a world where innovations that were previously the province of your imagination or solely the movies are now found in technology that positively impact all of our everyday lives.

Those innovations are not just cool and potentially lifesaving. They have positive economic benefit, with the United States benefiting significantly.

By way of example, the data solutions industry, which is fast growing, is expected to create over 4 million new jobs in the next 3 years. Nearly a third of those jobs are expected to be created in the United States, which we all benefit from.

Unfortunately, because of the NSA disclosures, "made in the USA" is no longer a badge of honor, but a basis for questioning the integrity and the independence of U.S.-made technology. In fact, a number of industry experts have projected that the losses from the NSA disclosures in the cloud computing space alone will be in the tens of billions of dollars.

Second, with regard to the societal implications, the impact is significant there as well. Many countries are using the NSA's disclosures as a basis for accelerating their policies around force localization and protectionism. We've all read about what's happening in Brazil and their efforts to create a walled garden around their data.

Brazil is not alone. Some of our other allies, including Europe, are questioning the safe harbor that enables cross-border data flows. As well, many European countries are advocating the creation of country-specific clouds.

If that is able to proceed and turns into a contagion, we run the real risk of going down the path of a Smoot-Hawley like protectionist downward spiral that dramatically impacts U.S. businesses and actually impacts businesses all around the world and transfer

what is an open, global Internet instead into a closed, siloed Internet, which is not something that none of us would like to see.

Congress is in a great position to avoid that, and so I'll turn to solutions. I offer 3 sets of solutions that build on 8 principles that we released 2 weeks ago.

First, we think that additional transparency is critical. The previous panel spoke to some of the steps that have recently been taken by the Justice Department to enable greater disclosures. We view those steps as a positive step forward but still think that legislation is necessary to cement those gains and to build on them.

Second, we think greater oversight is also very important, and developing a framework that enables a civil liberty advocate to be a part of the FISC court process—I'm sorry, the FISA court process is also important.

The last round of questions for the first panel revolved around trust, and we think that rebuilding trust is also critically important. And there are a number of steps we can take in that regard.

One is around the standard-setting processes around encryption. The NSA disclosures have significantly undermined the encryption standard-setting process, and the President in his speech passed on the opportunity to affirm the integrity of those processes. We think that it's critically important that that occur.

Second, and finally, the issue that's been much debated in the first panel around Section 215. We think the work that you're doing today and, hopefully, will do in the future around examining and reexamining 215 is critically important. In addition to considering national security, we would advocate considering other factors, including economic security, civil liberties, cost, as well as the impact on our standing with U.S. citizens and around the world.

Those same factors are equally apt as we consider whether that data should be stored by a third party.

Again, I thank you for this opportunity and look forward to your questions.

[The prepared statement of Mr. Garfield follows:]



**Information Technology
Industry Council**

"Examining Recommendations to Reform FISA Authorities"

Testimony of

Dean C. Garfield

President & CEO, Information Technology Industry Council (ITI)

Before the

U.S. House of Representatives

Judiciary Committee

February 4, 2014



**"Examining Recommendations to Reform FISA Authorities"
 Testimony of ITI's Dean C. Garfield
 House Judiciary Committee
 February 4, 2014**

Mr. Chairman, Ranking Member Conyers, and members of the Committee, I am Dean Garfield, president and CEO of the Information Technology Industry Council, or ITI, a U.S.-based global trade association representing 55 of the world's most dynamic and innovative companies in the information and communications technology (ICT) sector. I want to thank you, Mr. Chairman, for scheduling this extremely important and timely hearing – important for the reasons that I will outline shortly and timely because bipartisan congressional action on surveillance reform this year is critical to the continued innovative and competitive success of our sector in global markets.

The ongoing revelations about data collection by the National Security Agency (NSA) are having a significant economic impact on our sector, aside from the substantial societal implications that have been so much in the news. I discuss below the economic impact, as well as the potential long-term implications on the global economy for innovation and Internet governance, and offer our thoughts on solutions.

We live in a world where reality is quickly outpacing even our imagination. Today consumers can purchase a watch that is also a phone and a biometric device that monitors your heart rate. We can purchase cars that can slow down on their own to avoid accidents and also alert you to avoid an accident. We have access to three-dimensional printers that one day will produce organs and limbs to expedite transplants. These innovations are not only cool—they are potentially both life-saving and world changing. Further, these inventions rely on an innovation ecosystem that is global in nature, largely because of an Internet governance model that is open, integrated, and borderless. The tech sector is committed to sustaining both because they have served this nation and our world well.

Business Impact

The United States has been a leader in, and major economic beneficiary of, practically every part of the technology sector. For example data analytics, according to information technology research and advisory firm Gartner, will generate more than 4.4 million jobs worldwide between 2012 and 2015, including more than 1.9 million new IT positions in the U.S. And, according to a study by the International Data Corporation, cloud computing will create almost 14 million jobs worldwide from 2011 to 2015, including nearly 1.2 million new positions in the U.S. and Canada. Public and government responses from around the world to the NSA disclosures put that job creating potential at risk. The NSA disclosures, by creating a misimpression of the U.S. technology sector, are eroding trust in U.S. companies and in the security of data they hold. It is well established that: (a) data security is not a question of server location but rather depends upon the mechanisms and controls in place to safeguard the data; and (b) the data held by U.S. companies are as secure as data held anywhere else in the world. U.S. tech companies, like tech companies globally, view data integrity and security as their first priority.

Nonetheless, damage is being done. "Made in America" is no longer viewed as positive for customers of U.S. online services. Indeed, almost every ITI member company is experiencing increased levels of concern about government access to data, specifically access by the U.S. government. Other governments, of course, engage in online surveillance, but the impression being fueled globally in response to the NSA disclosures is that the U.S. government is the source of the problem, with U.S. companies seen as either aiding government surveillance, or particularly vulnerable to it.



The potential losses are tangible, demonstrable, and widespread. In the short term, the resulting commercial losses will likely reach the tens of billions of dollars, translating into lost American jobs. One recent study from the Information Technology & Innovation Foundation anticipates the revelations could result in as much as a \$35 billion loss to the U.S. cloud computing industry over the course of three years. Other studies, including by Forrester, suggest the losses could be even higher over a longer period of time.

Broader Implications

The potential adverse economic impact here in the U.S. could be even more significant and lasting if other governments enact legislation to force localized data storage and production of technology. Let me take it one step further -- such forced localization measures would also disrupt the current Internet governance model that to date has ignited and sustained the incredible success of the Internet as a global platform for innovation and economic productivity. These problematic policy proposals are spreading across the globe and have the potential of pushing the now-open Internet into a Smoot-Hawley protectionist death spiral, with disruptive global impact on international trade and commerce. We are facing nothing short of a Balkanized Internet, and global innovation will certainly suffer. Brazil, for example, is considering a legislative proposal that could lead to the requirement that certain data be stored in Brazil, and has taken steps aimed at ensuring that all government communications, including email, are managed by local companies.

The revelations have also received significant attention in the European Union (EU), placing in jeopardy one of the most critical data transfer mechanisms that many U.S. companies in numerous sectors rely on to transfer data from the EU to our nation. Government officials at the European Commission and in EU Member States are now questioning whether this mechanism -- the U.S.-EU Safe Harbor Framework -- should continue to operate. Similarly, a number of European nations are proposing to establish country-specific clouds.

These types of proposal and requirements would be highly disruptive to business operations, create network architecture inefficiencies that would hinder the performance of ICT services, and Balkanize open platforms, including the Internet, that are key to continued transformative innovations and global commerce.

Solutions

It is critical the U.S. government take the lead to reverse the erosion of public trust and the acceleration of forced localization and other onerous policies that would Balkanize the Internet and other open platforms.

We need a public policy course correction, and it must begin here in Congress. In fact, Mr. Chairman, this hearing is particularly helpful in highlighting that economic and commercial interests must be part of the discussion around government surveillance, coequal to the factors governments globally now in the information age need to consider, including individual privacy, economic prosperity, and national security.

While Congress works to develop appropriate measures to improve surveillance policies, we also urge the Administration to actively engage on this issue globally, and at the highest levels. International government-to-government dialogue is critical to prevent harmful policies that will impact our economy.

Both the Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board have made recommendations relating to the nation's surveillance programs. And President Obama recently outlined policy measures he supports.

We are encouraged by the building momentum to reform our surveillance policies, which now must translate into congressional action.



The recommendations I outline below largely derive from a set of seven global principles that ITI has developed with the Software Information & Industry Association (SIIA). We believe these principles should guide government surveillance policies around the world. Among other imperatives, these principles highlight the need for greater transparency and oversight in connection with how intelligence-gathering programs operate. I also ask that our seven global principles be submitted for the record along with my testimony.

Our recommendations, as well as the principles, are guided by a recognition that we don't know what we don't know on national security, and by a realization that privacy and security do not sit on opposite ends of a spectrum. It is possible to advance both.

Transparency

The companies that make up the technology sector are committed to informing their users and the public about requests received from governments around the world for law enforcement and intelligence purposes. Companies should be able to provide more information about such orders.

The Administration's recent decision to allow companies to disclose certain information is certainly a step forward. Greater transparency, however, should be permitted and legislation enabling such disclosures is desirable.

Specifically, companies should be permitted to disclose the number of government orders for information made under specific legal authorities, including, but not limited to, separate disclosures for Section 215 of the USA Patriot Act, Section 702 of the FISA Amendments Act, and various National Security Letter statutes. Also, companies should be permitted to disclose the number of individuals or accounts, including accounts of business customers, impacted by the orders received as well as the type of information that is sought by such orders.

In addition, as appropriate, the U.S. government should supplement the annual reporting that is already required by law with information similar to what companies should be permitted to disclose: the total number of orders under specific authorities for specific types of data, and the number of individuals or accounts affected by each.

Basic information about how the government uses its various law enforcement related investigative authorities has been published for years without any apparent disruption to criminal investigations. Further, the provision of such data to the public on a time-delayed basis and in aggregate form should not compromise any ongoing investigation.

An additional transparency measure we would recommend relates to the legal decisions of the Foreign Intelligence Surveillance Court (FISC). The legal decisions of the FISC are not routinely disclosed to the public. These decisions, however, involve constitutional questions and interpretations of legal authorities pursuant to which the U.S. conducts its surveillance activities. These decisions should be released publicly, as appropriate, to enable an informed public discourse about the court's rulings, and to better guide future congressional oversight and policymaking. This type of transparency can also yield greater public trust in the government's surveillance programs, their oversight, and the process utilized by the government to gain access to user data.

Oversight

FISC proceedings operate in a non-public forum and the U.S. government is the sole party appearing before the judges. An additional party, whether it is referred to as a special advocate or a public advocate, should be appointed in appropriate cases to assist the FISC in evaluating the issues at hand. This additional party would be an advocate for the privacy and civil liberty considerations implicated in the court proceedings.



Rebuilding Trust: Cryptography

Steps should be taken, using a transparent, public process, to restore public trust in the central role that the National Institute of Standards and Technology (NIST) plays in developing standards and guidelines to protect federal information and information systems, and industry at large.

Recent news reports describe in general terms the efforts of the NSA to defeat cryptographic protections for surveillance purposes. The reports suggest this effort went beyond the use of specially designed high-speed computers to crack encryption codes and involved the NSA in an attempt to introduce weaknesses into the encryption standards followed by hardware and software developers worldwide.

For nearly 20 years, the technology and user communities have welcomed the involvement of the NSA, as one of many stakeholders, in the work of developing cryptographic standards because it brings one of the most knowledgeable and experienced code-writing institutions to the vital task of protecting information from unauthorized access. The public, the technology sector, and the government all have an interest in the creation and widespread use of the strongest possible cryptographic standards. Regardless of the accuracy of these reports, the mere suggestion that the NSA has used its participation in the cryptography development process to introduce weaknesses into cryptographic standards has created a crisis of trust in the technology community. Some security firms have issued advisories to their customers to avoid using algorithms that might contain weaknesses.

We further appreciate NIST's history of extensive collaboration with the world's cryptography experts to support robust encryption. NIST has reopened public comment on some specific standards and stated clearly: "If vulnerabilities are found in these or any other NIST standards, we will work with the cryptographic community to address them as quickly as possible." This initiative is an important step toward regaining trust in NIST's commitment to strong, robust, cryptographic, and other standards that have been vetted by experts globally.

The facts alleged in the news accounts should be investigated and the separate roles played by NIST and the NSA in cryptographic should be reaffirmed.

Rebuilding Trust: Section 215

In addition to the transparency and other measures outlined above that are designed to increase public trust, there is an additional step that would provide greater certainty about how the U.S. government designs and implements the surveillance programs it operates.

This step involves Section 215 of the Patriot Act. There is a great deal of uncertainty surrounding what type of surveillance is authorized by Section 215 of the Patriot Act. Uncertainty leads to distrust, as does indiscriminate collection of private sector data by the government. Any collection of private sector data by the government must have the appropriate legal basis. In addition, especially given the number of technology tools that exist today, the collection of private sector data need not be indiscriminate.

We urge Congress to re-examine Section 215 with a focus on the extent to which national security interests are actually being advanced under existing practices, and to consider, as part of that examination, domestic and international implications, the implications on the perception of independence of the U.S. tech sector, significant economic costs, and the impact on existing Internet governance models. These same considerations are also important in assessing whether the private sector should store meta-data, rather than the U.S. government.

**Conclusion**

Mr. Chairman, we need to restore "Made in America" as a positive description of U.S. cloud services. The first step forward begins here. We at ITI are ready to work with this Committee and your colleagues on both sides of Capitol Hill, as well as the Administration, to restore trust in the innovative products and services that ITI member companies provide, and to maintain the open and borderless Internet that has served to the benefit of so many individuals, companies, and countries around the world.

Thank you for this opportunity to appear before you today. I will be happy to answer any questions you may have.

-30-

SUPPLEMENT



Information Technology
Industry Council



**Global Principles for Governments
Collecting Private Sector Data from Commercial Entities**

Recognizing that governments around the world engage in surveillance activities; and

Recognizing that certain important considerations must be built into government access to private sector data in the course of surveillance activities;

The principles below are intended to apply to government collection of private sector data from commercial entities.

- I. **Lawful Basis and Necessity.** Any government collection of private sector data must be authorized by law, must not be indiscriminate, and must be limited to what is necessary to achieve a legitimate purpose. Laws that authorize government collection of such data should include: (a) appropriate procedural protections under certain circumstances; and (b) sunset provisions to ensure regular reviews to determine whether specific laws continue to be necessary, or need to be amended.
- II. **Access.** Access to private sector data collected by governments from commercial entities should be restricted to only those within government who need such access consistent with the intended purpose of such collection or as authorized by law.
- III. **Technology Neutrality.** The limitations on government data collection, and the procedural legal requirements that governments must adhere to in connection with such collection, should apply equally to all types of data, including both offline and online data, and across technologies and platforms.
- IV. **Transparency.** Governments should implement appropriate transparency measures about the programs and mechanisms utilized to collect private sector data. Commercial entities should be permitted to disclose certain appropriate information about the government requests they receive for private sector data.
- V. **Oversight.** Programs and mechanisms pursuant to which a government collects private sector data should be subject to meaningful oversight by an independent body established by the government. Such independent body should have sufficient powers to access relevant information to assess whether there is a legal basis for how the government conducts its private sector data collection activities and to make appropriate policy recommendations.
- VI. **Avoid Conflict of Laws.** Governments should: (a) recognize that global commercial entities may be subject to the laws of numerous jurisdictions with respect to the collection of private sector data by governments; and (b) endeavor to avoid conflicts among such laws.
- VII. **International Engagement.** Governments should recognize that the frameworks pursuant to which national governments collect private sector data have global impacts. Governments should engage in multilateral discussions with other governments to minimize adverse global impacts in connection with the collection of such data.

Mr. GOODLATTE. Thank you, Mr. Garfield.

The Committee will stand in recess, and we will return as soon as these votes are over to begin the questioning.

[Recess.]

Mr. GOODLATTE. The Committee will reconvene. We are missing one of our witnesses. We will go ahead and start with you, Mr. Bradbury, and I am sure we will be joined by Mr. Garfield shortly. There he is. You were safe. We were starting with Mr. Bradbury anyway.

Do you see any legitimacy in Justice Sotomayor's concern that there is a cumulative effect to the data collected? Does the evolution of technology necessitate a reevaluation of the concept of a legitimate expectation of privacy?

Mr. BRADBURY. Well, first, Justice Sotomayor in the Jones case was not addressing anything like the telephone metadata program. There was a criminal investigation targeted at a specific individual where they were tracking him around, and they put a device on his car, and they were collecting data about everywhere he went and everything he did. It was focused on a dragnet, if you will, on that particular individual. And there is nothing like that here. The only focus in this program in this program is on terrorist groups and their connections.

Number two—

Mr. GOODLATTE. Well, let me just interject there because I understand that concern, but I think the concern that a lot of Americans have is that while that is the purpose and intent of this, the collection of data, which as we know technology today allows us to do pretty incredible things, and not just the government, but it is certainly done in the private sector. It is done in presidential elections, for example, to mix data and come up with very, very informative facts from the advanced use of technology. And the long-term storage of that data at the same time is, I think, whether it is what she is concerned about or what many of us are concerned about.

Nonetheless, I know it is a concern of many of my constituents that when you put those two things together, there has to be a much greater degree of trust in what government is going to do with that data over an extended period of time.

Mr. BRADBURY. Certainly that is true, and I think it is important for Congress and an appropriate role for Congress to study if statutory changes are appropriate with regard to developments and the use of data and the creation of data and data records.

But the same concern, which I think is a hypothetical concern about the potential for abuse, would apply to broad data collections that are all done by all manner of Federal regulatory agencies under subpoena authorities, administrative subpoena powers, that are based on the exact same language of this statute, but that do not involve—

Mr. GOODLATTE. But let me point out one difference, and it really goes to my next question. And that is, do you believe it is possible that because the FISC operates in secrecy and all those other agencies you cite, and you are correct about that, they do not operate in secrecy. Is it possible for the evolution of the law in that court to become so ossified or to go off track because it does not get challenged in the same way that regular Federal courts, or Federal reg-

ulatory process for that matter, are challenged? And if so, what would be the damage in having a panel of experts, maybe like yourself, available to argue a counterpoint to make sure that the FISC has all points of view?

Mr. BRADBURY. Well, I do think that there is nothing wrong or objectionable, as I have indicated, with a panel of experts that could be called upon as amicus to provide views on a difficult question, provided the constitutional issues I identify could be addressed.

But the other agencies I mentioned do not have to go through a court, so there are no court decisions unless the subject of an administrative subpoena challenges it in court, which is rare because this standard is so generous to those agencies. So the Securities Exchange Commission, Federal Trade Commission, Consumer Financial Protection Bureau, they get vast amounts of data about transactions affecting private interests of Americans in vast quantities.

Now, I am not saying it is the same quantity as here, true. But here, the interests are very different. They are the protection of the Nation from foreign attack. That is the paramount mission of the National Security Agency. The reason for the secrecy in the FISA process is because it involves the most sensitive national security secrets and threats to the country. It simply cannot be exposed.

Mr. GOODLATTE. I understand that, but there is an element of trust here that will ultimately cause this to fail unless the American people believe that what the protections are available to them are actually being asserted and exercised in the judicial process. And they do not get to see that like they do in other proceedings. And your point is well taken about those other agencies. Maybe we should be looking at what they do with their data as well.

But finally, let me ask you, do you believe that the government acquisition of third party data should be permitted indefinitely, or should there be some limit on how much of this data should be permitted?

Mr. BRADBURY. Well, in terms of time limit, the government does impose a time limit if the court order includes a time limit that requires all this data to be deleted, purged, after 5 years. The reason they chose 5 years, it is a standard time in the NSA programs because it is an important period to look back and do historical analysis. We know there was a cell operating in a particular operation 3 years ago. We see a new number now. It is important to know if it—

Mr. GOODLATTE. There is always an example of, you know, if you saved it further. I think it declines, however, exponentially, for example, the example of the Boston bombing. The data that was used to determine whether he had phone contacts with people that might be engaged in a conspiracy that we are going to launch another attack, which is certainly a concern that law enforcement and the general public would have, would not need to have storage for 5 years.

But let me just also suggest that it is not just about the length of time. The gentlewoman from California asked the question of the first panel related to what is the limit on what kind of data can be gathered. It is not just telephone data. It is not just financial

services data. It could be almost anything. And, therefore, when you put together that wide array of data over an extended period of time, there becomes a great deal of mistrust about how this system could be abused.

Mr. BRADBURY. Yes, and I think once the disclosures were made and this became the subject of public debate—I think it is a healthy debate—I think it was incumbent on the President to come out early and often to explain to the American people the nature of the program, the limitations, the lack of abuse, and to defend the program. I was happy to see that he did that in his speech on the 17th. I think that came a little late in the day, and unfortunately it was combined with a decision to change the program in material respects.

So I think it is first the role of the President to defend these programs. And second, I think the Chairs and Ranking Members of the intelligence committees that oversee the programs have an important role in terms of explaining and defending the programs.

Mr. GOODLATTE. Thank you. I am going to ask one more question, and that is directed to you, Mr. Garfield. Can you list for us the problems that your member companies anticipate they will face if they are required to store all the data the NSA is currently storing?

Mr. GARFIELD. It would probably be a long list, but we have talked about many of them. Some of them include having to keep data that goes beyond the business purpose of that data, the time period for keeping it that extends beyond the time period, security concerns, cost concerns, as well as the broader concern around trust, which is a critical component of how we operate in the tech sector.

Mr. GOODLATTE. Thank you. The Chair recognizes the gentleman from Michigan, Mr. Conyers, for 5 minutes.

Mr. CONYERS. Thank you, Mr. Chair. In her concurrence in *U.S. v. Jones*, Justice Sotomayor wrote this: “It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” Well, here is where that leads us: your phone number, the website address, the email address, the correspondence with the internet service providers, the books, groceries, and medications that we purchase online retailers, and so forth and so on.

How should we, Professor David Cole, how we should we rethink the right to privacy in what Justice Sotomayor called the digital age?

Mr. DAVID COLE. Thank you, Representative Conyers. I think that Justice Sotomayor is onto something. I think Justice Alito said much the same thing. He did not speak specifically to the third party disclosure rule, but he did speak specifically to the risks to our privacy that are posed by the fact that the government has technology today that allows it to learn information about all of us without going through the steps that were required at the time that the Constitution was adopted. And historically, the Fourth Amendment has been adapted to deal with those kinds of technological advances, whether it is the phone, or the use of the beeper, or the use of a GPS, or the use of a thermal imaging device.

So I think the Supreme Court can and should recognize that in the modern era, there is a difference between my voluntarily sharing information with, say, Mr. Bradbury and, therefore, voluntarily assuming the risk that he will turn around and provide that information to the government. That is a voluntary risk that assume.

There is a difference between that and the fact that to live in the modern age today you necessarily have to share information with businesses. Every place you walk, you are sharing with the cell phone company where you are. Every time you make a search on the internet, you are sharing with Google what you are thinking about. Every time you send an email, you are sharing with Google or your internet service provider who your friends are, who you are addressing.

And the notion that we somehow as Americans have voluntarily surrendered our privacy and all that incredibly intimate detail is probably telling about what we think and what we do than anyone who knows us knows about us. I mean, I do not think my wife knows as much about me as my computer knows about me, and yet if you adopt a third party disclosure rule without any change to recognize the advance in technology, you have just forfeited privacy.

But that is for the Supreme Court. I think even if the Supreme Court does not change the rules, this Congress can recognize that Americans demand more privacy than that. And as I said in my opening and as I say in my written statement, Congress has frequently done that. And I think this is an appropriate time to do that yet again to protect the privacy that all Americans deserve.

Mr. CONYERS. What do you think of the USA Freedom Act that I worked with both our U.S. Senator Leahy and with our former Chairman, Jim Sensenbrenner? Do you think that—

Mr. DAVID COLE. I think that is precisely the type of response I think that is needed and that is justified because what it does is it says we are going to end the notion that the government, simply by calling something business records and claiming that at some point in the future they may want to look through those business records, the government can collect everybody's records. Instead, what the USA Freedom Act says is the NSA, the FBI, they can collect records if they demonstrate that those records have a nexus either to a target of an investigation—a suspected terrorist or a foreign agent—or to a person known to or associated with that target.

That seems to me a perfectly reasonable and tailored response. Indeed, I think that is how the Administration sold what they were asking Congress to do when Section 215 was amended with the PATRIOT Act. And again, as I said in the opening, I do not think anybody in Congress thought when they said we are going to allow you to get relevant records that are relevant to an authorized investigation. I do not think a single Member of Congress thought what we meant by that is there are no limits on the business records that you can get. You can get records on every American, every phone call without any showing of any connection to terrorism. That is clearly unacceptable in terms of protecting the privacy of Americans.

The USA Freedom Act protects that privacy. It ensures that security interests are balanced by giving the government the ability

to get those records where it has a basis for suspecting that a person has that nexus.

Mr. CONYERS. Thank you so much. I have got a question for Mr. Dean Garfield, but I am going to give it to him and ask him to submit it in writing so it will go in the record.

Thank you, Mr. Chairman.

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

Mr. BACHUS. Thank you. First, Professor Cole, I am a part of a bipartisan group that is looking at sentencing reform, which is a different area. We are not dealing with that today, but I know you have been very active in advocating for changes in our criminal justice system, and I applaud you for that.

Mr. DAVID COLE. Thank you.

Mr. BACHUS. And I will ask the first question to you. It is not just the technology that has changed over the last 30 or 40 years. It is really the amount of information out there. We share so much information on Facebook, Tweeter, or Twitter, InstaGram. You know, that information is there in the public realm. I think *Smith v. Maryland*, those cases that were decided in the 70's and 80's on privacy and our expectations on privacy. How does the fact that there is so much more information out there, and we are sharing so much more information, how does that affect our expectation of right to privacy or how should it?

Mr. DAVID COLE. Well, I think that is the key question, and I think the answer may lie in the decision of Justice Alito in the Jones case where he says that there is a difference between following a car from point A to point B in public. You do not have an expectation of privacy with respect to your going from point A to point B in a car in public. There is a difference between that and using a GPS to follow that car from point A to point B to point C to point D to point E to point F all the way to point Z, 24/7 for 28 days. You are still in public, but the notion that the government could have followed you 24/7 for 28 days without the technology, it just could not have. It would have cost remarkable resources they would not have. And Justice Alito says, therefore, people had a reasonable expectation of privacy with respect to that information because it was just onerous for the government to collect it.

The same thing is true with all this information. You know, we generate all this information, but what has changed is that now every time we make a decision and take an action, it generates a digital record. And now we have computers that have the ability to collect and amass all of that data and to examine it for connections and ties, which tells whoever is looking, whether it be the NSA, or the FBI, or the IRS, whoever is looking, tells them a whole lot more about an individual than they ever possibly could have known before the advent of this technology and before the blossoming of these digital traces.

And, you know, it seems to me that both the Constitution, the Fourth Amendment doctrine, and the statutory law of this Congress needs to be adapted to recognize that fact. Otherwise, as Justice Scalia said in the *Kyllo* case involving thermal imaging devices, we will simply forfeit our privacy to advances in technology.

We have a choice, and the choice is whether we want to preserve our privacy or not. It does not go automatically. It goes if we let it go. And Congress has the power to stop it.

Mr. BACHUS. Okay. Mr. Bradbury, would you like to comment?

Mr. BRADBURY. Well, I think there is a big difference between what has been referred to as the third party doctrine, records being held by a third party, and the notion that metadata, which is transactional data, simply data about communications, not the content of the communications, is not a search because there is not a reasonable expectation of privacy. That is data created by a company to conduct its business. And the people involved in the communications as subscribers know the company is creating that record, that data. It is not your personal record. It is not something that includes the content⁴ of the communication.

There may be a communication that is stored in a cloud some place and somebody might try to argue that is held by a third party and it is not subject to protections. But this Congress has given it protections under the Electronic Communications Privacy Act and the Stored Communications Act. And I think there is an argument that the Court would recognize it as protected because it still includes the substance and private communications. So I think there is a big difference between that pure transactional metadata and every other kind of third party stored data.

The last thing I would comment on, Congressman, is with respect to the Jones case and what has been called the mosaic theory is that at a certain point when you put enough information about an individual together in an investigation, voila, that becomes a search suddenly, I think that Court has not gone there yet. There is a lot of scholarship about it and discussion. But if the Court goes there, that could really seriously interfere with criminal investigations of all kinds.

I mean, think about organized crime investigations where the prosecutors who are investigating or the FBI puts up on the wall an organization chart with the pictures of the members of the organization and collects all kinds of public data about the goings-on of those particular members of the organization. Does that constitute a search that would require a warrant to put that kind of profile together from all manner of public available information? No, it cannot. If it does, then criminal investigations would come to a halt.

Mr. BACHUS. Thank you.

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

Mr. NADLER. I thank the Chairman. Let me first observe that because of the evolving technology, people may, in fact, if they think about it, realize that the metadata on their phones is in the possession of somebody, but still have an expectation of privacy when they are using the phone because you do not think about it in everyday terms. And if you did and you said, gee, I do not want this in the public domain because it might go into the public domain because the phone company is keeping it for billing records and maybe because of something else, you would have no privacy at all. So I think our law has to change. Maybe for 40 or 50 years the ex-

pectation of privacy theory was valid, you know, and was sufficient, but no longer as privacy becomes more invaded.

But let me ask you the following, Professor Cole. You wrote in your testimony, "The bill would"—the bill, that is to say, the USA Freedom Act—"would restore an approach to privacy that is governed in this country since its founding, namely the notion that the government should only invade privacy where it has some individualized objective basis for suspicion," which, of course, is not the bulk collection of information under Section 215.

But you are describing exactly what we always wanted to do to avoid the general warrant. The Fourth Amendment was written specifically to say no general warrants. You have to describe the thing to be searched. We do not want the king's officer to be able to come and say show me everything based on nothing except that you live in Boston.

What we have now, is this not the type of general warrant that Section 215, the way it has been interpreted, precisely the general warrant that the Fourth Amendment was enacted to prevent?

Mr. DAVID COLE. I think it is. I think that when you have an order that says go out and collect literally every American's every phone call record, how is that different from a general warrant? It is not targeted. It is not predicated on individualized suspicion. It is as expansive as a general warrant, and that is precisely the concern that was raised.

Now, Mr. Bradbury says, well, but it is only getting metadata, not content. I think that is a very evanescent—

Mr. NADLER. Because you can learn a lot from metadata.

Mr. DAVID COLE. Well, and here is what Stewart Baker, who is general counsel of the NSA, said about that. He said, "Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you do not really need content. It is sort of embarrassing how predictable we are as human beings."

Mr. NADLER. Okay. I thought the moment I heard about it, I thought it was precisely the general warrant. And we certainly had no intention of authorizing Section 215. And the FISA Court, if it were not the kind of kangaroo court it is because it only gets one side, and it is done in secret, probably would not have decided it that way.

But let me ask you a second question. The review board established by the President recommended, among other things, that we harmonize the standards for national security letters for Section 215 collection. This makes sense to me, particularly as many of the standards for NSL's minimization of initial approval process are less rigorous. What is your opinion? Should we harmonize the standards by requiring that NSL meet the same and presumably amended standards since it will fix the problem that now exists with the Administration and FISA Court's interpretation of what is relevant?

In other words, should we make the NSLs match 215, and, for that matter, if we do, why bother having NSLs at all anymore?

Mr. DAVID COLE. Right. Well, yes, I think they should be harmonized. The USA Freedom Act would harmonize them and would employ the same standard to define the nexus required to get business records generally and the nexus required to get NSLs.

Right now, NSLs in Section 215 have the same standards. It's just that it is this relevance standard which the government has read to be meaningless. So the USA Freedom Act would keep parity between——

Mr. NADLER. It would harmonize them?

Mr. DAVID COLE. Huh?

Mr. NADLER. It would harmonize them.

Mr. DAVID COLE. Right.

Mr. NADLER. Good.

Mr. DAVID COLE. It is harmonized, yes. But I think it needs to be harmonized and elevated to——

Mr. NADLER. Harmonized up, not down.

Mr. DAVID COLE. Yes.

Mr. NADLER. Mr. Garfield, in the few seconds I have, last week the government agreed to allow to Facebook, Microsoft, Google, Yahoo, Apple, and other tech companies to make information available to the public about the government's request for email and other internet data. Are these new disclosure rules sufficient? Should Congress take additional steps? And assuming that the NSA continues to collect telephone metadata under Section 215, will the government reach a similar deal with telephone companies for disclosures about call record requests?

Mr. GARFIELD. I will answer the first two questions, which I am in a good position to answer.

Mr. NADLER. That is why I asked you.

Mr. GARFIELD. The agreement last week I think is a positive step in allowing greater transparency, which is something we strongly believe in.

The answer to your second question as to whether legislation would be helpful is yes. It goes part way, but not far enough. For example, it is important that the private sector have transparency reports and disclosures, but it is also important that the public sector do as well. And so, in that respect, among others, I think having legislation would be very helpful.

Mr. NADLER. Thank you. My time has expired. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman, and thanks for this hearing. You know, Mr. Conyers read the exact quote from Justice Sotomayor's opinion that I had been looking at. And I have been thinking a lot about we have the role of writing the statutes, but behind that is, you know, what the Constitution requires. And I think that it is not just the Court that needs to examine that. I think the Congress has an obligation to do that as well.

And as I have been thinking about this, I have been thinking about two longstanding doctrines, one, the third party data, there is no expectation of privacy, as well the plain sight doctrine. And just as you have said, I mean, 30 years ago, if I walked out my front door, I knew that my neighbors could see me. I did not expect that my picture would be taken every place I walked and compiled, and using facial recognition technology someone could say where I was every moment of every day.

Yes, if I went in and checked into a hotel, I knew that that was not private information, but I did not expect that every email I

send, every website, that if I went on my Constitution document that somebody could track how often I read the Fourth Amendment. That was not part of the third party doctrine.

So I think Congress needs to not delegate this to the Court, but to head on take on these issues because I think if you look at where the Court is going, you know, I do not know how long it is going to take them to get there. You know, we cannot discuss what we are told in closed sessions, but I will just read the news reports that we had a few days ago, reports that that the NSA is spying using leaky mobile apps; a few days before that the NSA collected over 200 million text messages; that in late December that cookies were being used to track people; that there were 5 billion records of mobile phone location data collected daily; that there was collection of pornographic website visits used to blackmail potential so-called terrorists; that money transfers were being tracked. And it goes on and on.

So I guess, you know, one of the questions I have, Professor Cole, is if the Congress should step forward to interpret the Fourth Amendment in light of big data, how would we do that, statute by statute? And I am a co-sponsor of Mr. Sensenbrenner's bill, but that really relates to just a portion of this question. Do you have thoughts on that?

Mr. DAVID COLE. Well, I think it is a great question. I think it is the defining question of privacy for the next generation, which is how do we preserve privacy in the face of these advances in technology, which make it possible for the government to learn everything about us.

And I think, you know, it is absolutely critical that Congress play a role, that Congress has historically played a role, not waited for the Supreme Court to act, in some instances acting before the Supreme Court does so, FISA for example. In other areas when the Supreme Court has said there is no expectation of privacy, Congress has come on the heels of that and said, wait a minute, the American people disagree with you. We want our privacy. And so, I think that is what you did with respect to bank records, video rental records, PIN registers, and the like.

So there is a real history of Congress stepping up here and doing so. And I am not sure you can do it in a global way, but the USA Freedom Act, as I suggested earlier, is a useful start because it puts in place the principle of individualized suspicion, rejecting this general warrant notion.

Ms. LOFGREN. I am going to follow up with you and I am going to ask one additional question of Mr. Garfield. On the technology issues, one of the very distressing reports was that the government, rather than alert people to zero day events, simply exploited them. I am worried about the balkanization of the internet. We see what Brazil is doing, certain authoritarian regimes insisting that servers be placed in their country. I am worried about governance and whether ICON will be able to continue to be the governing body, or whether efforts to dismantle that will be enhanced by these revelations.

I am wondering if we should make obligations to the government to proactively take steps to preserve the global internet both

through mandates not to weaken encryption, mandates as to assisting in zero day events, and if you have thoughts on that.

Mr. GARFIELD. Yes, I absolutely do. We worry as well about the potential balkanization and what the NSA disclosures mean for internet governance. I think it is very important for Congress to act in this area. I think the President missed an opportunity by not speaking to the encryption standards issue and the need to bolster the integrity of encryption standards. And so, to the extent that Congress has the ability to do that, we would encourage it.

Ms. LOFGREN. My time has expired. Thank you, Mr. Chairman.

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

Mr. SCOTT. Thank you, Mr. Chairman. Mr. Garfield, can you just say another word about the effect of global competitiveness on this issue and how American companies are actually pretty much at a disadvantage if we do not get this straight?

Mr. GARFIELD. No, absolutely. So trust, integrity, security are key components of technology and doing well in technology and developing your business in that area. The United States has played a significant leadership role around the world. And to the point in my testimony, rather than continuing to be a badge of honor, today because of the NSA disclosures, countries and customers around the world are questioning the integrity and independence of U.S. technology companies, which puts us at a competitive disadvantage overseas, but also here where the American people also have those same trust concerns.

Mr. SCOTT. And do you have a choice in vendors in a lot of products, whether it is an American company or a foreign company?

Mr. GARFIELD. I am sorry?

Mr. SCOTT. Is there a choice in vendors in products?

Mr. GARFIELD. Almost always, I mean, but the tech sector is highly competitive. We represent both domestic and international companies. The impact, interestingly enough, is global because to the extent that innovations that are being led by the United States do not occur, the whole world is disadvantaged because we all benefit from those innovations. And so, it creates a global problem, but one that is particularly acute for U.S. companies.

Mr. SCOTT. Does your council have a position on where information should be stored if the decision is made to collect and store this data where it ought to be stored at NSA or some, say, department store or something like that?

Mr. GARFIELD. Yes. Our view is that the same considerations that we offer in evaluating 215 are apt in considering where that data is stored. For example, if the goal is to rebuild trust, it is not clear how having that data stored in a third party addresses the trust concern. If it is around data integrity and security, it is not clear how having it stored in a third party addresses that data integrity or security question.

And so, in the examination, we think it is important to come up with certain principles and have those principles guide the examination both of 215 as well as where the data is stored.

Mr. SCOTT. So are you suggesting it could be stored at the NSA as long as they separate it down the hall, across the street, but have NSA control it rather than the private sector?

Mr. GARFIELD. I am not suggesting that at all.

Mr. SCOTT. Well, where would it be?

Mr. GARFIELD. The beginning comment that I made, which is that there is a lot that I am not privy to for a whole host of reasoning, including security clearance. And so, I do not feel I am in a position to give advice to the U.S. government on national security. What I feel that I have the confidence to do is to make sure that certain important factors, in addition to national security, are considered. Economic security, privacy, civil liberties, as well as our standing in the world, are some of the factors that we think should be considered.

Mr. SCOTT. Thank you. Mr. Cole, the Administration has offered a lot of administrative changes. What would be the shortcomings if those changes are not codified?

Mr. DAVID COLE. If those changes are not codified?

Mr. SCOTT. Right.

Mr. DAVID COLE. Well, I think those changes are important ones, in particular the notion that the NSA cannot search through the bulk collection without first getting approval from a court. That seems to me an important modification. The notion that there would be an independent advocate in the FISC seems to be important. And one implication of not doing that, I think as we see, we see repeated instances of what we have now learned about, right?

So Mr. Bradbury said 15 judges of the FISA Court approved of the use of Section 215 to get all of our phone data. What he did not say is that when that program was first approved by the first judge in May 2006, he did not even write an opinion. He did not address the constitutional questions. He did not say why he thought the limitation on relevance was somehow met by giving the NSA access to everybody's information. No opinion.

Every 90 days thereafter, a different Federal judge, and this is how he gets to 15, signed an order that extended the program. No analysis of the constitutional question, no analysis of the statutory question. It was not until Edward Snowden disclosed it to the public that the FISC finally wrote an opinion 7 years after the program had been up and running explaining retroactively why they thought what they had been doing for 7 years was okay. And it is, as the privacy board has shown in its analysis, a very, very doubtful construction of the statute, one that, as Representative Sensenbrenner has, was not in anybody's mind who adopted the statute.

So I think the Administration's proposals are important, but I think they do not go far enough. And particularly the key way in which they do not go far enough is that they do not end bulk collection. They do not end dragnet collection. They just put it somewhere else. I think with the USA Freedom Act would do is end it, and that is a much better response.

Mr. SCOTT. You were not here when Mr. Cole answered the question about retroactive immunity. I asked the question that you keep hearing that the collection of the data was helpful. It was an illegal collection, finding that it was helpful does not give you immunity for the collection. Do you have a comment on what relevance it is that people keep saying we need because it is helpful as a justification for getting the data?

Mr. DAVID COLE. Yes, absolutely. I mean, it would be helpful if the police could, without a warrant, search every one of our homes on a daily basis without any basis for suspicion. That would be helpful because they might find some bad guys who are hiding behind the privacy that we all expect from our home. But that does not make it right.

But number two, I think when they say it is helpful, you have got to look behind that, as the privacy board did, met with them in classified sessions, looked at classified materials, looked at the "success stories," and found, and here I am quoting from them on page 146, "We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."

Mr. SCOTT. Well, to justify the program because it was helpful, it just adds insult to injury. It was not even helpful. But even if it had been helpful, it would not retroactively make the collection legal, would it?

Mr. DAVID COLE. That is right.

Mr. BACHUS [presiding]. Mr. Scott, your time has expired.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. BACHUS. Thank you. Mr. Chaffetz.

Mr. CHAFFETZ. Thank you. I appreciate the hearing. I know it has been a long one, and I appreciate your patience here.

Mr. Garfield, one of the terms that has been thrown out there is this so-called balkanization of the internet or internet balkanization. I would like you to expand on that. You have talked about bits and parts of it. You know, there have been some concerns about what is going on in Brazil, the European Union. They have announced some policies that would disadvantage the United States based companies. Can you kind of expand your thoughts on that?

Mr. GARFIELD. Yes. I know this is not just theoretical, it is actually real, so you point to Brazil where the government of Brazil is moving forward with policies that would essentially create a wall garden around data that is developed in Brazil. They have already said that the email systems being used by the government can only be stored or developed by Brazilian companies. So as a result, U.S. companies that have previously held a leadership position in the technology innovation in that space are being dispossessed.

It is an economic issue, but it also a broader internet governance issue. If it turns out that the open internet that we have all gotten used to becomes a balkanized series of walled gardens, then a lot of the innovation, a lot of the societal benefits that we have experienced will be limited.

Mr. CHAFFETZ. Thank you. In your written testimony you state the need to rebuild trust regarding the National Institute of Standards and Technologies, or NIST, and their commitment to cryptographic standards developed and vetted by experts globally. Could you explain the importance of this in your opinion?

Mr. GARFIELD. Yes. The reason why technologies work across geographic boundaries is you get off the plane and your phone will

work in Europe as well as the United States, is because of standards that are driven through consensus and multi stakeholder voluntary processes. Some of the disclosures have suggested that the United States has exploited vulnerabilities in cryptography, which erodes trust. And so, in order to ensure that our technology will work across borders, it is critical to rebuild that trust.

The President missed an opportunity in his speech to speak to this issue. We hope that he will, but Congress has the opportunity to correct that error.

Mr. CHAFFETZ. Thank you. I think you have touched on two of the concerns that globally the communication that we enjoy. These things are so important. So I appreciate all of your expertise being here today. I appreciate this Committee talking about such an important issue.

Mr. Chairman, I think you wanted me to yield you some time if that is correct? I will yield back or yield to you, whatever you choose.

Mr. BACHUS. Yes, yield to me, if you will.

Mr. CHAFFETZ. Yes.

Mr. BACHUS. And let me say this. I am going to pursue that same line. I had intended to. And, Mr. Garfield, are there other countries that are demanding information from your member companies about their citizens or foreign citizens?

Mr. GARFIELD. It happens in a number of countries. And so, as we think about internet governance and jurisdiction issues, we are always careful about the salutary impact. And so, the rules that we live by in one market set a precedent for how we operate globally, and that is in part why in our recommendations we strongly encourage more multilateral dialogue around these surveillance and security issues so we can get greater harmonization around the rules that are created.

Mr. BACHUS. Right. And are other countries tapping into your member company systems for spying purposes?

Mr. GARFIELD. The question presumes that that is happening anywhere, including here in the United States.

Mr. BACHUS. Well, say, in other countries.

Mr. GARFIELD. No. So our companies are always working hard to make sure that cryptography and security measures are robust.

Mr. BACHUS. But what I am talking about is, you know, they have databases, and they maintain those in other countries. Can they come and use that platform to access information for spying purposes?

Mr. GARFIELD. We work hard to make sure that is not, in fact, the case. I mean, the previous panel made the point that we live in a world in which cyber warfare and efforts on undermining cyber security are quite aggressive, including by companies as well as nations. We are always working because it is a first priority of ours to maintain the data integrity to fight against that.

Mr. BACHUS. Well, let me say this. If you are required to store some of this data, say, even the U.S. government, then it could be subject to requests in civil proceedings, divorce proceedings, once you maintain it. So you may want to consider to start maintaining that data.

Mr. GARFIELD. Exactly, and there are two issues. One is data stored by private companies at the request of the U.S. government, and then data stored at a third party. We are unequivocally opposed to data being stored by the private sector, us, beyond the need for business purposes for the very reason you highlight, which is the data integrity issue. It creates additional vulnerabilities. We are always fighting against that, but we do not want to create more targets.

Mr. BACHUS. Thank you. The gentlelady from Texas is recognized for 5 minutes.

Ms. JACKSON LEE. Let me thank you again, and let me take note that this is a long hearing, and we thank you very much for your participation here.

I was, Professor Cole, reading the old 215, and I guess I continue to be baffled, having been here when we crafted the PATRIOT Act in the waning hours, months, and days after 9/11. And everyone was in a perplexed state, and the idea was, of course, to protect our citizens. But I notice 215 in Section 501 particularly pointed out, they listed books, records, papers, documents, and other items. There goes the mega data. But they also said protect against international terrorism or clandestine intelligence activities. Further down, it goes onto again emphasize that we should specify that there is an effort to protect against international terrorism, clandestine intelligence.

And I only raise that because it looks to me that we have firewalls, but what resulted is this massive acknowledgement of the gathering of telephone records of every single American. And I want to find a way to politely push back on Justice Sotomayor's reflection, and I think it is a reflection, and I think it is one in the reality of today, which is maybe we can have privacy, and have you muse, if you will, on the new legislation that we have introduced where we enunciate a whole list of reasons. And I do not know if you have been able to look at that number 1 section that we have here that goes on to as relevant material, obtain foreign intelligence not concerning a United States person, protect against international terrorism. It sort of lays it out.

And I ask you, can we comfortably find a way to answer Justice Sotomayor and say, yes, we can? I might use that. And is there something else we should add in the legislation that I have co-sponsored enthusiastically, and we will be looking forward to it moving forward. Can we add something else because as I look at 215, Section 501, it looks as if we had all that we need to have to say, you know what? I do not think they wanted you to get the mega data. Are we where we need to be in this new legislation?

Mr. DAVID COLE. Thank you for that question. You know, I agree that Section 215, if you read it with its ordinary meaning, sought to put constraints on the types of records and the amounts of records that the government could obtain because it did not say you are hereby authorized to obtain all business records on all Americans. It said you are authorized to obtain business records that are relevant to an authorized investigation.

And as the privacy board's report shows in exhaustive detail, very powerful analysis, no court in any other setting has ever read a relevance limitation as expansively as saying you can pick up

every American's every record. No court, not in a grand jury context, not in a civil discovery context. So Congress did seek to put in limited language.

Ms. JACKSON LEE. We did.

Mr. DAVID COLE. But the Administration essentially took it out. So I think what Congress needs to do is to push precisely as Justice Sotomayor suggests, and I think that the key is to identify when it is obviously justified to sweep up the kinds of records that disclose so much about our intimate and personal lives. And I think the USA Freedom Act does a good job because it says you can do so when those records pertain to a foreign agent or a suspected terrorist, when they pertain to an individual in contact with or known to a suspected agent of a foreign power or a terrorist who is a subject of an investigation.

So that says you can get records on the target. You can get records on people connected to the target. But, no, you cannot get records on every single American because Americans want security, but they also want privacy, and they want to use their phones. And we should not have to give up any one of those three. I think the USA Freedom Act ensures that we have all three.

Ms. JACKSON LEE. And diligence is part of that. Mr. Gardner, let me ask you this. I know you may have been asked and answered over and over again. What will be the burden of the private sector hold onto this vast amount of data if it was to be crafted in that way? What would be the cost? What would be the problems?

Mr. GARFIELD. It is hard to put a precise number on it. I think it suffices to say the burden would be significant, not only in cost, but the impression that it creates. One of the challenges we face as a result of the NSA disclosures is there is a question around the integrity as well as the independence of U.S.-based companies. If we are to store that data, that would call into question whether we are, in fact, independent. And so, there are financial costs as well as broader costs as well.

Mr. BACHUS. Thank you.

Ms. JACKSON LEE. Mr. Chairman, if you would just indulge me for 30 seconds, a group question.

Mr. BACHUS. A brute question? But a very short response.

Mr. GARFIELD. Okay.

Ms. JACKSON LEE. Thank you very much. I will not follow up. I just want to get Mr. Bradbury and Mr. Cole in again, and I will group my question together. Mr. Gardner makes a valid point on the perception issue. Why is it not better that we have a monitored holding of the data of whatever it may be, and the fact that we have now laid out a framework by the Federal Government instead of the private sector.

And then just an aside with respect to how we do our intelligence. Do you think it is time that we haul in all of the outside contracting and do a better job of vetting and doing this in house dealing with our intelligence access? If I can get a quick answer. I think I put two questions in at once. Mr. Bradbury?

Mr. BRADBURY. Thank you, Congresswoman. I do think there are risks with outside contractors, and I think putting the data in private hands would raise those risks. I think it would increase privacy concerns and make the program less effective.

So I think it is monitored now while it is being held by the NSA, closely overseen. I do not think it is an excess or abuse of the relevant standard. I think if this Committee changes the relevance standard, it should not single out the NSA and the intelligence community. It should consider applying the same narrowing standard to all Federal regulatory agencies, which collect vast amounts of records and data for their own investigatory purposes. They do not just limit themselves to those narrow individual records that are directly pertaining to their investigation. They get databases so that they can search it for relevant queries.

And so, if the same standards applied across the board, I think it would really inhibit the functioning of government. I do not think the NSA should be singled out when its mission is the most important.

Ms. JACKSON LEE. Thank you. Mr. Cole, can you—

Mr. DAVID COLE. I think if you adopt the USA Freedom Act, which I think you should, then the problem of where to store the bulk collection is solved because there is no bulk collection, right? If you say the NSA can only collect data where it is actually connected to a terror suspect or someone who is connected to a terror suspect, there is no bulk collection, and there is not the problem of storage. The problem of storage arises only if you continue to permit bulk collection. I do not think that should continue to be permitted.

Ms. JACKSON LEE. I thank you, Mr. Chairman. I think we have got strong support for the H.R. 3361, and I look forward to moving forward on such legislation. With that, I yield back.

Mr. BACHUS. This concludes today's hearing. The Chairman thanks all of our witnesses for attending.

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 adjourned. Thank you.

[Whereupon, at 3:09 p.m., the Committee was adjourned.]

A P P E N D I X

MATERIAL SUBMITTED FOR THE HEARING RECORD

Material submitted by the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary

ANNEX A

Separate Statement by Board Member Rachel Brand

I commend the Board and our tiny staff for putting together this comprehensive Report while simultaneously struggling to establish our still-infant agency. Although I disagree with much of the Report's discussion and some of its recommendations, this may be the most thorough description and analysis of the Section 215 bulk telephony metadata collection program ("Section 215 program") that has been published to date.

I concur in most of the Board's recommendations, and I am pleased that we were able to achieve unanimity on so many of them. However, I write separately to briefly note several points on which I disagree with the Report. Most importantly, I dissent from the Board's recommendation to shut down the Section 215 program without establishing an adequate alternative.

Where I agree with the Board's Report

I join the Board's proposal to create a process for appointing an independent advocate to provide views to the Foreign Intelligence Surveillance Court ("FISC") in important or novel matters. (Recommendations 3-5.) Although I believe the FISC already operates with the same integrity and independence as other federal courts, I agree with the Board that some involvement by an independent third party will bolster public confidence in the FISC's integrity and strengthen its important role.

Of course, the devil is in the details. Meddling in a system that already works well is risky. Any proposal to change the FISC's operations must, among other things, ensure that the FISC can continue to operate very quickly; not jeopardize the security of the sensitive materials reviewed by the court; provide adequate resources to account for an increased burden on the court; and allow the FISC's judges to retain discretion and control over the participation of an independent advocate in any given case. I believe this Board's recommendations account for all of these considerations better than any of the other proposals that have been offered.

I also sign on to most of the Board's recommendations to provide greater transparency about the government's counterterrorism programs. (Recommendations 6-11.) I agree with the Board that additional transparency, where possible, promotes public confidence in our national security agencies. However, it is important to note that the Board recommends that transparency measures be adopted *to the extent consistent with national security*. It is this qualification that enables me to sign on to the core of those recommendations. I suspect I have a different view than some of my colleagues about how

to implement each of the recommendations, but those details will be worked out in the future.

I do not sign on to the Board's discussion concerning Recommendation 12, because I do not believe that an intelligence program or legal justification for it must necessarily be known to the public to be legitimate or lawful.

Finally, I join the Board's recommendations for immediately modifying the Section 215 program (Recommendation 2) because I believe these changes will ameliorate privacy concerns while preserving the operational value of the program.

Where I disagree with the Board's Report

I cannot sign on to the substance of much of the Board's analysis. I am concerned that the Report gives insufficient weight to the need for a proactive approach to combating terrorism, and I hope that the Report will not contribute to what has aptly been described as cycles of "timidity and aggression" in the government's approach to national security.⁶⁸⁹ After September 11, 2001, the public demanded to know why the government had not stopped those attacks. Fingers were pointed in every direction, and civil liberties and privacy considerations took a backseat in the public debate immediately following the attacks. Of course, the legal structure under which the agencies operated prior to 9/11 had been put into place in the 1970s as a reaction to the Church Committee's revelations of prior excesses and abuses by the Intelligence Community. Since the recent leaks of classified programs, the pendulum seems to be swinging sharply back in that direction. But I have no doubt that if there is another large-scale terrorist attack against the United States, the public will engage in recriminations against the Intelligence Community for failure to prevent it. These swings of the pendulum, though they may be an inevitable result of human nature, are an unfortunate way to craft national security policy, and they do a disservice to the men and women dedicated to keeping us safe from terrorism.

The primary value that this bipartisan, independent Board can provide is a reasoned, balanced approach, taking into account (as our statute requires) *both* civil liberties and national security interests. We should not overreact to the crisis or unauthorized disclosure du jour, but take a longer view.

With these background considerations in mind, I turn to my reasons for dissenting from the Board's recommendation to shut down the Section 215 program.

The Board concludes that the Section 215 program is not legally authorized. I cannot join the Board's analysis or conclusion on this point.

⁶⁸⁹ See, e.g., JACK GOLDSMITH, *THE TERROR PRESIDENCY, LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION* 163-64 (2007).

The statutory question—whether the language of Section 215 authorizes the telephony bulk metadata program—is a difficult one. But the government’s interpretation of the statute is at least a reasonable reading, made in good faith by numerous officials in two Administrations of different parties who take seriously their responsibility to protect the American people from terrorism consistent with the rule of law. Moreover, it has been upheld by many Article III judges, including over a dozen FISC judges and Judge Pauley in a thorough opinion in a regular, public proceeding in U.S. District Court.⁶⁹⁰

In light of this history, I do not believe this is a legal question on which the Board can meaningfully contribute. If we were addressing this as a matter of first impression, advising the government on whether to launch the program in the first place, we would need to grapple with this question of statutory construction. But we do not approach this question as a matter of first impression. It has been extensively briefed and considered by multiple courts over the course of several years. Some of those cases are ongoing. This *legal* question will be resolved by the courts, not by this Board, which does not have the benefit of traditional adversarial legal briefing and is not particularly well-suited to conducting *de novo* review of long-standing statutory interpretations. We are much better equipped to assess whether this program is sound as a *policy* matter and whether changes could be made to better protect Americans’ privacy and civil liberties while also protecting national security.

Because the Board also concludes that the program should be shut down as a policy matter, it seems to me unnecessary and gratuitous for the Board to effectively declare that government officials and others have been operating this program unlawfully for years. I am concerned about the detrimental effect this superfluous second-guessing can have on our national security agencies and their staff. It not only undermines national security by contributing to the unfortunate “cycles of timidity and aggression” that I mentioned earlier, but is also unfair, demoralizing, and potentially legally harmful to the individuals who carry out these programs.

Turning to the constitutionality of the Section 215 program, I agree with the Board’s ultimate conclusion that the program is constitutional under existing Supreme Court caselaw.⁶⁹¹ The Board appropriately states that government officials are entitled to rely on current law when taking action. But in speculating at great length about what might be the future trajectory of Fourth Amendment caselaw, it implicitly criticizes the government for not predicting those possible changes when deciding whether to operate the program.

⁶⁹⁰ See Memorandum & Order, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

⁶⁹¹ One federal judge recently reached the opposite conclusion, holding that the Section 215 program is likely unconstitutional. See Memorandum Opinion, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013). This demonstrates that these are difficult legal questions that ultimately will be resolved by the courts.

Perhaps the Supreme Court will amend its views on the third-party doctrine or other aspects of Fourth Amendment jurisprudence in future cases. But that is beside the point in a Report addressing whether the government's actions were legal at the time they were taken and now. Surely government officials should be able to rely on valid Supreme Court precedent without being second-guessed years later by a Board musing on what legal developments might happen in the future.

Of course, the government must seriously consider whether it *should* take actions that intrude on privacy even if it *can* take them as a legal matter. Whether the Section 215 program should continue as a matter of good policy is a question squarely within the Board's core mandate and one that courts have not addressed and cannot resolve. However, I do not agree with the Board's conclusion that the program should be shut down.

Whether the program should continue boils down to whether its potential intrusion on privacy interests is outweighed by its importance to protecting national security.

Starting with the privacy question, on the one hand, any collection program on this scale gives me pause. As the Board discusses, metadata can be revealing, especially in the aggregate (though I do not agree with the Board's statement that metadata may be even "more" revealing than contents). Whenever the government possesses large amounts of information, it could theoretically be used for dangerous purposes in the wrong hands without adequate oversight. Even if there is no actual privacy violation when information is collected but never viewed, accessed, analyzed, or disseminated in any way, as is true of the overwhelming majority of data collected under the Section 215 program, collection and retention of this much data about American citizens' communications creates at least a *risk* of a serious privacy intrusion.

This is why I join the Board's recommendations for immediate modifications to the program (Recommendation 2), including eliminating the third "hop" and reducing the length of time the data is held. Based in part on the Board's lengthy discussions with government officials, I believe these changes would increase privacy protections without sacrificing the operational value of the program.

On the other hand, the government does not collect the content of any communication under this program. It does not collect any personally identifying information associated with the calls. And it does not collect cell site information that could closely pinpoint the location from which a cell phone call was made. The program is literally a system of numbers with no names attached to any of them. As such, it does not sweep in the most sensitive and revealing information about telephone communications. This seems to have gotten lost in the public debate.

In addition, the program operates within strict safeguards and limitations. The Board's Report describes these procedures, but it bears repeating just how hard it is for the government to make any use of the data collected under this program. For example, before even looking at what the database holds on a particular phone number, an NSA analyst must first be able to produce some evidence—enough to establish “reasonable, articulable suspicion” or “RAS”—that that particular phone number is connected to a specific terrorist group listed in the FISC's order. Only a handful of trained analysts are authorized to do this. Before typing the phone number into a search field, the analyst must document the “RAS” determination in writing. And if the results of the query reveal a pattern of calls that seems worth investigating further, the analyst must jump through a series of additional hoops before gathering more information about the communications or distributing that information to other agencies. As a result, only an infinitesimal percentage of the records collected are ever viewed by any human being, much less used for any further purpose.⁶⁹²

With the safeguards already in place and the additional limitations this Board recommends, I believe the *actual* intrusion on privacy interests will be small.

On the other side of the equation is the national security value of the program. The Board concludes that the program has little, if any, benefit. I cannot join this conclusion.

There is no easy way to calculate the value of this program. But the test for whether the program's potential benefits justify its continuation cannot be simply whether it has already been the key factor in thwarting a previously unknown terrorist attack. Assessing the benefit of a preventive program such as this one requires a longer-term view.

The overwhelming majority of the data collected under this program remains untouched, unviewed, and unanalyzed until its destruction. But its immediate availability *if it is needed* is the program's primary benefit. Its usefulness may not be fully realized until we face another large-scale terrorist plot against the United States or our citizens abroad. But if that happens, analysts' ability to very quickly scan historical records from multiple service providers to establish connections (or avoid wasting precious time on futile leads) could be critical in thwarting the plot.

Evidence suggests that if the data from the Section 215 program had been available prior to the attacks of September 11, 2001, it could have been instrumental in preventing

⁶⁹² As the Board discusses, there have been lapses in compliance with the program's limitations. Most of these violations have been minor and technical. A few have been significant, though apparently unintentional. Compliance problems are always a matter of concern and demonstrate the need for robust oversight. But it is important to remember that the lapses the Board mentions came to light only because the government *self-reported* violations to the FISC. Those problems were then corrected, under the supervision of the FISC. And these corrective measures and self-reporting occurred *before* these programs were publicly disclosed. That is, they were identified and fixed not because of the scrutiny brought about by an unlawful leak of classified information, but because existing oversight mechanisms worked.

those attacks.⁶⁹³ The clear implication is that this data could help the government thwart a future attack. Considering this, I cannot recommend shutting down the program without an adequate alternative in place, especially in light of what I view to be the relatively small actual intrusion on privacy interests.

That said, if an adequate alternative that imposes less risk of privacy intrusions can be identified, the government should adopt it. The President appears to believe that the government can craft an alternative that retains the important intelligence capabilities of the program but reduces privacy concerns by storing the data outside the government. Although I expect this Board to have a role in crafting any such alternative and I look forward to those discussions, I doubt I could support a solution that transfers responsibility for the data to telephone service providers. This approach would make sense only if it both served as an effective alternative and assuaged privacy concerns, but I am skeptical it would do either. Because service providers are not required to retain all telephony metadata for any particular length of time, asking the service providers to hold the data could not be an effective alternative without legislatively mandating data retention. But data retention could increase privacy concerns by making the data available for a wide range of purposes other than national security, and would raise a host of questions about the legal status and handling of the data and the role and liabilities of the providers holding it. In my view, it would be wiser to leave the program as it is with the NSA than to transfer it to a third party.

Whatever happens to the Section 215 program in the short term, the government should frequently assess whether it continues to provide the potential benefits it is currently believed to have, including whether the incremental benefit provided by the program is eroded by the development of additional investigative tools. This process of re-evaluation should not consist merely of ad hoc conversations among individuals involved in the programs, but should be formalized, conducted at regular intervals with involvement by this Board, approved by officials at the highest levels of the Executive Branch, and briefed to the Intelligence and Judiciary Committees. I look forward to working with the intelligence agencies in conducting this analysis.

⁶⁹³ See, e.g., *Oversight of the Federal Bureau of Investigation: Hearing before the H. Comm. on the Judiciary*, 113th Cong. 25-26 (2013) (statement of Robert S. Mueller III, Director, Federal Bureau of Investigation) (testifying that if the data from the Section 215 program had been available to investigators before 9/11, it would have provided an “opportunity” to prevent those attacks); Decl. of Teresa H. Shea, Signals Intelligence Director, Nat’l Sec. Agency, ¶ 35, Dkt. 63, in *Am. Civil Liberties Union v. Clapper*, *supra* note 2; Michael Morell, *Correcting the Record on the NSA Review*, WASH. POST, Dec. 27, 2013 (had data from the Section 215 program been available at the time, “it would likely have prevented 9/11”).

ANNEX B**Separate Statement by Board Member Elisebeth Collins Cook**

I appreciate the thorough work of my colleagues, as well as the staff, and agree with almost all of the recommendations of the Report. I think it bodes well for the future effectiveness of the Board that we are virtually unanimous as to the policy-based recommendations reflected in the Report, and I urge that serious consideration be given to each of recommendations two through eleven. I agree that to date the Executive Branch has failed to demonstrate that the program, as currently designed, justifies its potential risks to privacy, and for that reason I join the recommendations to immediately modify its operation. I also agree with the Board that modifications to the operations of the Foreign Intelligence Surveillance Court ("FISC") and an increased emphasis on transparency are warranted—to the extent such changes are implemented in a way that would not harm our national security efforts.

I must part ways with the Report, however, as to several points. First, although I believe the Section 215 program should be modified, I do not believe it lacks statutory authorization or must be shut down. Second, I do not agree with the Board's constitutional analysis of the program, as it is concerned primarily with potential evolution in the law, and the potential risks from programs that do not exist. Third, I write separately to emphasize that our transparency and FISC recommendations must be implemented in a way that is fully cognizant of their potential impact on national security. Finally, I disagree with the Board's analysis of the efficacy of the program.

Fundamentally, I believe that the Board has erred in its approach to this program, which has been (a) authorized by no fewer than fifteen Article III judges, (b) subject to extensive Executive branch oversight, and (c) appropriately briefed to Congress. The Board has been unanimous that as a policy matter the Program can and should be modified prospectively, including by limiting the analysis the National Security Agency ("NSA") could do with the records and the amount of time NSA could keep the records. The Board has nonetheless engaged in a lengthy and time-consuming retrospective legal analysis of the Program prior to issuing those recommendations. I am concerned that this type of backward-looking analysis, undertaken years after the fact, will impact the willingness and ability of our Intelligence Community to take the proactive, preventative measures that today's threats require. And there is no doubt that should the Intelligence Community fail to take those proactive, preventative measures, it will be blamed in the event of an attack.⁶⁹⁴

⁶⁹⁴ By the same token, having undertaken this legal analysis, I do not understand the Board's apparent recommendation that the program it considers unauthorized continue for some interim period of time.

First, based on my own review of the statutory authorization, I conclude that the Section 215 program fits within a permissible reading of the Foreign Intelligence Surveillance Act business records provision.⁶⁹⁵ I am not persuaded that the reading of the statute advanced by the government and accepted by the Foreign Intelligence Surveillance Court⁶⁹⁶ and Judge Pauley of the United States District Court for the Southern District of New York⁶⁹⁷ is the only reading of Section 215, but I am persuaded that it is a reasonable and permissible one. Perhaps as important, I think the program itself represented a good faith effort to subject a potentially controversial program to both judicial and legislative oversight and should be commended. Moreover, the program has been conducted pursuant to extensive safeguards and oversight. When mistakes were discovered (and mistakes will occur at any organization the size of the National Security Agency), they were self-reported to the court and briefed to appropriate congressional committees; corrective measures were implemented, and the program reauthorized by the FISC.⁶⁹⁸

Second, the Board has engaged in an extensive discussion of emerging concepts of Fourth Amendment jurisprudence, none of which I join. Our conclusion that the program does not violate the Fourth Amendment is unanimous, as it should be: *Smith v. Maryland* is the law of the land.⁶⁹⁹ The government is entitled to rely on that decision, and the judges of the FISC (and our federal district and circuit courts) are required to do so, unless and until it is reversed. Analysis of whether, when, or how the Supreme Court may revisit that decision and its application is inherently speculative and unnecessary to the Board's report.

Nor do I join the Board's First Amendment analysis (which also informs the balancing/policy section). The First Amendment implications the Board finds compelling arise not from the Section 215 program but from perceived risks from a potential program that does not exist. Although the Board focuses on the "complete" pictures the NSA could paint of each and every American in concluding that it has a significant chilling effect, that is not an accurate description of the Section 215 program. The information the NSA receives *does not include the identity of the subscribers*. As the Board's Report acknowledges, a number is paired with its subscriber information (in other words,

⁶⁹⁵ See Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861).

⁶⁹⁶ See, e.g., Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006); Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

⁶⁹⁷ See Memorandum & Order, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

⁶⁹⁸ See, e.g., Primary Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 09-13 (FISA Ct. Sept. 3, 2009).

⁶⁹⁹ *Smith v. Maryland*, 442 U.S. 735 (1979).

information that would allow the NSA or other agency to identify the person associated with the number) only after a determination is made that there is a reasonable, articulable suspicion that a number queried through the database is associated with one of the terrorist organizations identified in the FISC's orders. For a telephone number reasonably believed to be used by a U.S. person, the reasonable articulable suspicion standard cannot be met solely on the basis of activities protected by the First Amendment. Any investigative steps related to that number can be taken only after a determination that the number associated with its subscriber information has potential counterterrorism value. There is no disagreement that this process is applied to only an extraordinarily small percentage of the numbers in the database, yet the Board Report's balancing/policy and First Amendment analyses proceed as if each and every number of every American is systematically paired with its subscriber information and analyzed in great detail.

In addition, the Board nowhere meaningfully grapples with two key questions. One, what is the *marginal* constitutional and policy impact of the Section 215 program, particularly in view of the Board's assertion that essentially everything the Section 215 program is designed to accomplish can be accomplished through other existing national security and law enforcement tools? Two, is there a difference as a policy and constitutional matter between an order or program that is designed by its very terms to force disclosure of each and every individual's protected activities (such as the disclosure requirement addressed in *NAACP v. Alabama*⁷⁰⁰), and a program such as the one under consideration today, in which information is *collected* about innumerable individuals, but human eyes are laid on less than .0001% of individuals' information? To the Board, there is no apparent constitutional or policy difference between mere collection of information and actually accessing and using that information. I do not agree.

Third, I agree with the Report's recommendations as to transparency (except recommendation twelve) and the operations of the FISC, both sets of which are designed to foster increased confidence in the government's national security efforts. I also understand that each of our recommendations is to be implemented with full consideration of the potential impact on our national security, and without hindering the operations of the FISC. As to transparency, we have always understood that not everything can be publicly discussed, *see, e.g.*, U.S. Const. Art. I § 5, cl. 3. ("Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy"), as we would like to avoid providing our adversaries with a roadmap to evade detection. The rational alternative, which occurred here, is to brief the relevant committees and members of Congress, seek judicial authorization, and subject a program to extensive executive branch oversight. In a representative democracy such as

⁷⁰⁰ *NAACP v. Alabama*, 357 U.S. 449 (1958).

ours, it is simply not the case that a particular use or related understanding of a statutory authorization is illegitimate unless it has been explicitly debated in an open forum.

Finally, I have a different view from the Board as to the efficacy and utility of the Section 215 program. Although the Report purports to consider whether the program might be valuable for reasons other than preventing a specific terrorist attack, the tone and focus of the Report make clear that the Board does believe that to be the most important (and possibly the only) metric. I consider this conclusion to be unduly narrow. Among other things, in today's world of multiple threats, a tool that allows investigators to triage and focus on those who are more likely to be doing harm to or in the United States is both good policy and potentially privacy-protective. Similarly, a tool that allows investigators to more fully understand our adversaries in a relatively nimble way, allows investigators to verify and reinforce intelligence gathered from other programs or tools, and provides "peace of mind," has value.

I would, however, recommend that the NSA and other members of the Intelligence Community develop metrics for assessing the efficacy and value of intelligence programs, particularly in relation to other tools and programs. The natural tendency is to focus on the operation of a given program, without periodic reevaluations of its value or whether it could be implemented in more privacy-protective ways. Moreover, the natural tendency of the government, the media, and the public is to ask whether a particular program has allowed officials to thwart terrorist attacks or save identifiable lives. Periodic assessments would not only encourage the Intelligence Community to continue to explore more privacy-protective alternatives, but also allow the government to explain the relative value of programs in more comprehensive terms. I hope that our Board will have the opportunity to work with the Intelligence Community on such an effort.

* * * * *

In many ways, the evaluation of this long-running program was the most difficult first test this Board could have faced. Unfortunately, rather than focusing on whether the program strikes the appropriate balance between the necessity for the program and its potential impacts on privacy and civil liberties, and moving immediately to recommend corrections to any imbalance, the Board has taken an extended period of time to analyze (a) statutory questions that are currently being litigated, and (b) somewhat academic questions of how the Fourth Amendment might be applied in the future and the First Amendment implications of programs that do not presently exist. I believe that with

respect to this longstanding program, the highest and best use of our very limited resources⁷⁰¹ is instead found in our unanimous recommendations.

The development of a modified approach to the very difficult questions raised by the government's non-particularized collection of data presents an ideal opportunity for the Board to fulfill its statutory advisory and oversight role. In this regard, I would note that some frequently mentioned alternatives pose numerous potential difficulties in their own right. For example, some have suggested that the NSA could essentially request that the telephone companies run the queries, rather than collecting and retaining records for querying. However, even assuming the companies currently keep the relevant records, there is no guarantee that those records will continue to be retained in the future. By the same token, if another terrorist attack happens, the pressure will be immense to impose data retention requirements on those companies, which would pose separate and perhaps greater privacy concerns. Finally, it is not at all clear how a third party entity to hold the data could be structured in a way that would (a) be an adequate substitute for the Section 215 program and (b) preserve the security of those records, while (c) ameliorating the perceived privacy concerns raised by that program.

There is much to consider in the near future, and I look forward to working with my colleagues on these important issues.

⁷⁰¹ Although many agencies claim to lack adequate resources, the situation of the PCLOB is particularly remarkable. The agency currently has a full-time Chairman, four part-time Members limited to 60 days of work per year, and two permanent staff members. The decision to engage in such an extended discussion of largely hypothetical legal issues was therefore not without practical consequences: the Board has delayed consideration of the 702 program, and has not addressed any of the other issues previously identified by the Board as meriting oversight. Moreover, the decision of three Members of the Board to allocate the entirety of the permanent staff's time to the drafting of the Board Report, while simultaneously drafting and refining that Report until it went to the printer, has made a comparably voluminous response impossible.

**Comments of the Judiciary on Proposals
Regarding the Foreign Intelligence Surveillance Act**

January 10, 2014

These comments on behalf of the Judiciary regarding proposals with respect to the Foreign Intelligence Surveillance Act of 1978 (FISA), codified as amended at 50 U.S.C. §§ 1801-1885c, were prepared by the Honorable John D. Bates, Director of the Administrative Office of the United States Courts, in consultation with the current Presiding Judges of the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (Court of Review), as well as with other judges who serve or have served on those courts.

It is the responsibility of the political branches to decide, within the bounds of the Constitution, what legal requirements and processes or substantive limitations should apply to intelligence gathering operations. For that reason, the focus of these comments is not to provide policy advice on issues of national security, foreign relations or privacy. Rather, the principal objective of these comments is to explain how certain proposals for substantive or procedural changes to FISA would significantly affect the operations of the FISC and the Court of Review (collectively, “the Courts”). These comments are presented in an effort to enhance the political branches’ ability to assess whether, on balance, it would be wise to adopt those proposals. This discussion also notes where we perceive that certain proposals may implicate serious constitutional concerns, although detailed analysis of the constitutional issues is precluded where those issues could foreseeably come before one of the Courts in the event that a proposal is adopted.

The following is a summary of our key comments:

- It is imperative that any significant increase in workload for the Courts be accompanied by a commensurate increase in resources.
- Some proposed changes would profoundly increase the Courts’ workload. Even if additional financial, personnel, and physical resources were provided, any substantial increase in workload could nonetheless prove disruptive to the Courts’ ability to perform their duties, including responsibilities under FISA and the Constitution to ensure that the privacy interests of United States citizens and others are adequately protected.
- The participation of a privacy advocate is unnecessary and could prove counterproductive in the vast majority of FISA matters, which involve the application of a probable cause or other factual standard to case-specific facts and typically implicate the privacy interests of few persons other than the specific target. Given the nature of FISA proceedings, the participation of an advocate would neither create a truly adversarial process nor constructively assist the Courts in assessing the facts, as the advocate would be unable to communicate with the target or conduct an independent investigation. Advocate involvement in run-of-the-mill FISA matters would substantially hamper the work of the Courts

without providing any commensurate benefit in terms of privacy protection or otherwise; indeed, such pervasive participation could actually undermine the Courts' ability to receive complete and accurate information on the matters before them.

- In those matters in which an outside voice could be helpful, it is critical that the participation of an advocate be structured in a manner that maximizes assistance to the Courts and minimizes disruption to their work. An advocate appointed at the discretion of the Courts is likely to be helpful, whereas a standing advocate with independent authority to intervene at will could actually be counterproductive.
- Drastically expanding the FISC's caseload by assigning to it in excess of 20,000 administrative subpoena-type cases per year -- even with a corresponding injection of resources and personnel -- would fundamentally transform the nature of the FISC to the detriment of its current responsibilities.
- It is important that the process for selection of FISC and Court of Review judges remain both expeditious and fully confidential; the Chief Justice is uniquely positioned to select qualified judges for those Courts.
- In many cases, public disclosure of Court decisions is not likely to enhance the public's understanding of FISA implementation if the discussion of classified information within those opinions is withheld. Releasing freestanding summaries of Court opinions is likely to promote confusion and misunderstanding.
- Care should be taken not to place the Courts in an "oversight" role that exceeds their constitutional responsibility to decide cases and controversies.

The adoption of many of the measures discussed herein would impose substantial new responsibilities on the FISC and ultimately the Court of Review. For the Courts to meet such new responsibilities effectively and with the dispatch often required by national security imperatives, they would need to receive commensurate augmentation of resources. Depending on what exactly is enacted, the augmentation may require increased legal or administrative staff, additional judges or devotion of more of the current judges' time to the work of the Courts, appointment of magistrate judges to work on the FISC, and enhanced secure spaces and communications facilities. The provision of some of these resources could well come at the expense of the work of judges in their home districts and circuits, thereby negatively affecting the operations of their respective federal courts.

We also wish to stress, however, that even significantly increasing resources will not guarantee that all proposed changes will be successful. Giving new responsibilities to the Courts, while also establishing more elaborate procedures for the Courts to follow, may actually detract from their ability to identify and resolve the issues that are most critical to national security and privacy interests. Thoughtful assessment of the advantages and disadvantages of proposed changes is therefore crucial.

In our view, some proposals that have been made – especially those that would create a full-time independent advocate to oppose a wide range of government applications before the Courts – present substantial difficulties that would not be resolved by simply increasing the Courts’ resources. We anticipate that this form of advocate participation would not only be cumbersome and resource-intensive, but also would impair the FISC’s ability to receive relevant information, thereby degrading the quality of its decisionmaking. We turn first to this question.

Proposals for a Special Advocate to Appear Before the Courts

The vast majority of FISC matters are *ex parte* requests by the government for search warrants, electronic surveillance orders, production of records or pen register/trap-and-trace orders. Every day, United States district courts receive dozens of such requests in criminal investigations and rule on them in an *ex parte* manner, with no party present except the government. The FISC process is very similar to the one employed by the district courts in these criminal matters.

Consistent with this well-established procedure for entertaining requests of this nature, FISA does not currently provide a means for the FISC to solicit the assistance of non-governmental entities in considering issues presented by such requests. Moreover, except in the rare situation where substantial information about an ongoing case has been declassified,¹ non-governmental individuals and entities now lack the information needed to seek leave to participate as *amici curiae* and to assist the FISC or Court of Review in resolving difficult legal or technological issues. An effort to address these narrow concerns would not be objectionable, as long as it does not burden Court operations in the large majority of cases where there is no need for a quasi-adversarial process.

Recent public debate has focused on matters such as NSA’s bulk collection of call detail records under Section 501 of FISA, codified at 50 U.S.C. § 1861, and the government’s acquisition of information pursuant to Section 702 of FISA, codified at 50 U.S.C. § 1881a. Such matters, however, comprise only a small portion of the FISC’s workload, measured either by number of cases or allocation of time. In all but a small number of matters, the FISC’s role is to apply a probable cause or other factual standard to target-specific sets of facts and to assess whether the government’s proposed minimization procedures are adequate under the particular circumstances. The authorizations sought in the large majority of cases do not implicate the privacy interests of many U.S. persons because the collections at issue are narrowly targeted at particular individuals or entities that have been found to satisfy the applicable legal standards. Nor, except in a small handful of cases, do such matters present novel or complex legal or technical issues. Accordingly, as the President’s Review Group on Intelligence and

¹ See *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Memorandum Opinion and Order, Docket No. BR 13-158 (FISA Ct. Dec. 18, 2013), where the FISC authorized a non-governmental advocacy group to file an *amicus* brief addressing the bulk telephony metadata collection program.

Communications Technologies (“Review Group”) has recognized,² most FISA cases are similar to law enforcement applications for search warrants and Title III wiretaps, which also are considered *ex parte*. Providing for an advocate in the large majority of cases, then, would be superfluous and would create the unusual situation in our judicial system of affording, at this stage of the proceedings, greater procedural protections for suspected foreign agents and international terrorists than for ordinary U.S. citizens in criminal investigations.

To be sure, genuinely adversarial processes, such as criminal or civil trials, provide an excellent means of testing a party’s factual contentions. But introducing an advocate into the FISA process would not produce that result. Advocates of the type put forward in various proposals to change FISA would not actually represent a proposed target of surveillance or any other particular client.³ For operational security reasons, such an advocate would not be able to conduct an independent factual investigation, *e.g.*, by interviewing the target or the target’s associates. An advocate therefore would be of little, if any, assistance in evaluating the facts of particular cases which, as noted above, is the heart of the FISC’s consideration in the large majority of cases.

Indeed, we are concerned that proposals to create a full-time advocate with the discretion to participate, or seek leave to participate, in any or all cases would impair rather than improve the FISC’s ability to receive information and rule on applications in an effective and timely manner. Enhanced resources would help the FISC overcome these impairments, but only to a limited extent. In order to explain the reasons for these concerns, it is helpful to summarize how the FISC operates.

² When the FISC was created, it was assumed that it would resolve routine and individualized questions of fact, akin to those involved when the government seeks a search warrant. It was not anticipated that the FISC would address the kinds of questions that benefit from, or require, an adversary presentation[.] . . . however, the FISC is *sometimes* presented with novel and complex issues of law. The resolution of *those issues* would benefit from an adversary proceeding.

Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies (Dec. 12, 2013) (“*Review Group Report*”) at 203 (emphasis added). The Review Group further acknowledged that “[b]ecause the number of FISA applications that raise novel or contentious issues is probably small, the Advocate might find herself with relatively little to do.” *Id.* at 204.

³ See, *e.g.*, *Review Group Report* at 200 (recommending creation of a “Public Interest Advocate to represent privacy and civil liberties interests” before the FISC).

Judges appointed to the FISC retain all their regular responsibilities for civil and criminal cases assigned to them in their respective districts. Each week, one of those judges is on duty for the FISC in Washington, D.C. Eight of the eleven judges do not reside in the Washington, D.C. area and must travel from their home districts in order to serve as the duty judge. The duty week assignment rotates among the judges, so that each judge takes one week every few months away from district court responsibilities to do FISC work. This rotation system avoids serious disruption to the work of any one district when a judge serves on the FISC.

Because much of the material reviewed by the FISC is highly classified, its work generally must be performed in a Sensitive Compartmented Information Facility (SCIF). FISC quarters in Washington, D.C., including office space and a court room (which are also shared by the Court of Review), are within such a SCIF. In contrast, a lack of secure communication and storage facilities makes it very difficult for eight of the eleven judges to review FISC pleadings or communicate about FISC matters when they are in their home districts. The large majority of FISC cases are handled by the duty judge within one week while in Washington (though preparatory work by Court staff often commences during the prior week). More complex or time-consuming matters are sometimes handled by judges outside of the duty-week rotation, at the discretion of the Presiding Judge.

FISC judges currently have substantial flexibility in deciding how best to receive from the government information they consider relevant to a particular case. Formal hearings are conducted when necessary. On the other hand, when deemed appropriate by a judge (for example, in a time-sensitive matter), the FISC may request or receive information from the applicant informally through its legal staff. This range of options enables the FISC duty judge to routinely entertain 40 or more applications in a typical week. In keeping with the *ex parte* nature of the proceedings, the government generally responds to these inquiries with a high degree of candor; indeed, the government routinely discloses in an application information that is detrimental to its case. This candor is also essential to the FISC's ability to discharge its responsibilities.

Introducing an advocate into a substantial number of FISC proceedings would likely slow down and complicate the Court's information-gathering and consideration of these fact-intensive cases. Under current FISC rules and practice, in non-emergency cases the government is required to submit proposed applications to the FISC within seven days of when it seeks to have the final application ruled upon. In order for an independent advocate to have a meaningful opportunity to review an application, decide whether he wishes to participate in its consideration, and prepare and submit views to the FISC, and for the FISC to consider the advocate's submission together with the application, the government would have to submit a proposed application substantially earlier than the present seven-day period. That requirement would likely conflict with the government's interest and the public's interest to obtain expedited consideration of an application or of successive applications when necessary to respond to a rapidly evolving threat. Moreover, even relatively routine national security investigations often involve changing facts, such that proposed applications would frequently require change or

supplementation. This process of keeping the FISC and the advocate apprised of changing circumstances over a longer period of time would be cumbersome and time-consuming.

This prolonged period of consideration in routine cases would also complicate the assignment of matters to FISC judges because such proceedings would likely extend beyond a judge's normal duty week. The more cases in which an advocate is involved, the more likely it would be that the Court would have to modify its current practice of having each FISC judge sit for one week at a time. A different approach, requiring a judge to engage with FISC matters for longer periods, is likely to require more time away from judges' home districts, to the detriment of their regular district court work.

The difficulties of such a process would be exacerbated by the need to interact on equal terms with the applicant and the advocate. In order for the FISC to abide by the procedural and ethical requirements that apply in adversarial proceedings, and for the advocate to appear on equal footing with the applicant, the FISC would have to ensure that the advocate was involved in all such interactions in any case in which the advocate may participate (or, if the advocate must seek leave to participate from the FISC, perhaps only in those cases where such a request is pending or has been granted). We expect that the logistical challenges of administering such a three-way process for more than a handful of cases would be considerable. And even if it were appropriate under the terms of a specific enactment to limit the involvement of the advocate in such interactions to cases where the advocate has sought or received leave to participate, the FISC may well need to ensure that the advocate, upon entering a matter, becomes fully apprised of any interactions that have already occurred.⁴

At an institutional level, there are difficult policy, and potentially constitutional,⁵ questions regarding how an advocate would fit within existing governmental structures. The Review Group recognized that where to house the advocate presents a "difficult issue" and came to no particular recommendation on this point. *See Review Group Report* at 204-05. Some proposals for an advocate may also compromise judicial independence.⁶

⁴ If the advocate and an applicant have a dispute about what information the advocate should receive, then the FISC may be required to resolve collateral, discovery-type issues, which would place new forms of demands on the resources of the Court and create the potential for delays that would impact national security.

⁵ *See* Congressional Research Service, *Introducing a Public Advocate into the Foreign Intelligence Surveillance Act's Courts: Select Legal Issues* (Oct. 25, 2013) at 8-14 (discussing issues under the Appointments Clause).

⁶ Some proposals would grant the advocate broad access, not only to government pleadings and Court decisions, but also to Court material relevant to those decisions. Such broad access could be understood to encompass draft decisions and memoranda from legal staff to a
(continued...)

In short, the burdens and complications arising from a full-time advocate who could elect to participate (or seek leave to participate) in fact-intensive, run-of-the-mill cases, weighed against the negligible benefits from involving an independent advocate in consideration of those cases, strongly counsel against creation of such a position.

Perhaps most troubling, however, is our concern that providing an institutional opponent to FISA applications would alter the process in other ways that would be detrimental to the FISC's timely receipt of full and accurate information. As noted above, the current process benefits from the government's taking on – and generally abiding by – a heightened duty of candor to the Court. Providing for an adversarial process in run-of-the-mill, fact-driven cases may erode this norm of governmental behavior, thereby impeding the Court's receipt of relevant facts. (As noted above, the advocate would rarely, if ever, serve as a separate source of factual information.) Instead, intelligence agencies may become reluctant to voluntarily provide to the Court highly sensitive information, or information detrimental to a case, because doing so would also disclose that information to a permanent bureaucratic adversary. This reluctance could diminish the Court's ability to receive relevant information, thereby undermining the quality of its decisions. In some cases, that reluctance could result in those agencies' opting not to pursue potentially valuable intelligence-gathering operations governed by FISA in order to protect extremely sensitive intelligence methods or targets from disclosure to that adversary.⁷

⁶(...continued)

judge. Such materials are privileged communications under both ethical canons and separation-of-powers principles and their disclosure to the advocate would seriously infringe on the independence of the judges' decisionmaking.

⁷ Some might suggest that an advocate who can engage across-the-board in FISA matters would enhance public perception that the process is fair and takes into account privacy, as well as national security, interests. Recent disclosures by the FISC and the Executive Branch have done much to dispel the misperception that the FISC "rubber stamps" government requests. *See, e.g., Review Group Report* at 202 ("As illustrated by the [recently declassified] section 215 and section 702 non-compliance incidents . . . , the FISC takes seriously its responsibility to hold the government responsible for its errors."); Letter of the Honorable Reggie B. Walton, FISC Presiding Judge, to the Honorable Patrick J. Leahy, Chairman, Senate Committee on the Judiciary (Oct. 11, 2013) ("During the three month period from July 1, 2013 through September 30, 2013, we have observed that 24.4% of matters submitted [to the FISC] ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action."). Moreover, public action such as enhancing transparency and modifying the substantive rules and standards governing intelligence collection (or reaffirming current rules and standards after public examination and debate) would be more likely to improve confidence in the FISA process than would introducing a new layer of secret bureaucracy.

A mechanism that facilitates the involvement of an advocate in those particular cases that, in the Court's judgment, would benefit from an advocate's participation would largely avoid these difficulties. Contrary to the suggestion of the Review Group, *see Review Group Report* at 204, we believe that judges are fully capable of determining which matters would benefit from such participation and how best to structure participation within a particular case.⁸ If an advocate's participation is at the discretion of the Court, however, placing statutory limitations on the types of cases in which that participation is available may prevent the Court from benefitting from the advocate's contributions in an appropriate case. For example, limiting an advocate's participation to cases presenting a novel or significant interpretation of the law could prevent the Court from taking advantage of an advocate's participation in a case that presented challenging technological, rather than legal, issues. Such limitations might also raise constitutional questions. *See* Congressional Research Service, *Requiring a Federal Court to Hear from an Amicus Curiae* (Dec. 9, 2013) at 4.

Proposals that would empower a permanent advocate to independently seek reconsideration of FISC decisions, or to appeal them to the Court of Review, would pose difficulties in addition to those summarized above. As others have noted, substantial standing and other constitutional issues would be presented if the advocate sought to challenge an authorization granted by the FISC. *See* Congressional Research Service, *Introducing a Public Advocate into the Foreign Intelligence Surveillance Act's Courts: Select Legal Issues* at 21-26 (Oct. 25, 2013).

As a practical matter, a full-time advocate empowered to seek reconsideration in the FISC and to appeal decisions to the Court of Review would significantly impact the operations of both Courts. An increased number of reconsideration requests would pose scheduling and logistical challenges in the FISC's current mode of operations. FISC judges frequently rule on cases toward the end of their duty week, so in many cases it is highly unlikely that an advocate's request for reconsideration would even be filed before a sitting judge from a district outside of the District of Columbia area returned to his or her district. As a result, judges would need to arrange their regular district court schedules to allow for an additional, return trip to Washington in the event a request for reconsideration were filed. If requests for reconsideration became sufficiently common, the FISC would likely need to reexamine its current one-week rotation schedule. Either approach would negatively affect judges' ability to perform their district court duties.

In the Court of Review, any meaningful increase in the number of appeals would transform the operations of that Court, which heretofore has not had a workload requiring full-time operation. Because Court of Review judges also serve full-time on district courts or courts of appeal, a significant increase in the number of FISA appeals might necessitate more judges being appointed to the Court of Review. And because the Court of Review currently relies on FISC staff and uses the FISC's secure space to conduct its work, a significant increase in its

⁸ An approach in which the FISC could appoint an advocate in a particular case where the advocate's participation would be helpful would also enable the Court to select an advocate who does not present recusal issues for the judge handling the case.

workload would likely require the Court to hire its own staff and construct or acquire its own secure space.

Effect of Certain Substantive Proposals on Court Operations

The following substantive proposals would impose significant new demands on the FISC and ultimately the Court of Review.

Changes to National Security Letter Practices: The Federal Bureau of Investigation (FBI) uses national security letters (NSLs), which are akin to administrative subpoenas, mainly to obtain subscriber information, *see Review Group Report* at 90, although other types of records may also be obtained, *see, e.g.,* 15 U.S.C. § 1681u (consumer report records).

An NSL-related recommendation of the Review Group could increase the FISC’s annual caseload severalfold. Under that recommendation, an NSL could be issued in non-emergency circumstances “only upon a judicial finding” of “reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect against international terrorism or clandestine intelligence activities.” *Review Group Report* at 89, 93 (internal quotations omitted). The Review Group did not reach a conclusion about whether to give jurisdiction over NSL requests to the FISC or other federal courts. *Id.* at 93. The Review Group recognized, however, that assigning such cases to the FISC “would pose a serious logistical challenge. The FISC has only a small number of judges and the FBI currently issues an average of nearly 60 NSLs per day.⁹ *It is not realistic to expect the FISC, as currently constituted, to handle that burden.*” *Id.* (emphasis added). We strongly agree. We are skeptical, however, that the suggestions put forward to revamp the FISC to take on such demands – “a significant expansion in the number of FISC judges” or “creation within the FISC of several federal magistrate judges to handle NSL requests,” *id.* – would be adequate.

Moreover, even if one assumes that adequate resources can be made available to the FISC to handle the sheer volume of new cases without compromising the district court work of FISC judges, jurisdiction over 21,000 NSL requests per year would transform the FISC from an institution that is primarily focused on a relatively small number of cases that involve the most intrusive or expansive forms of intelligence collection to one primarily engaged in processing a much larger number of more routine, subpoena-type cases. We fear that such a drastic shift of emphasis would diminish the FISC’s effectiveness in adjudicating and overseeing cases involving electronic surveillance, physical search or Section 702 acquisitions.

⁹ In annual terms, the FBI issued 21,000 NSLs in Fiscal Year 2012. *Review Group Report* at 90. By way of comparison, the FISC entertained 212 business records applications and 1,856 applications for electronic surveillance and/or physical search in calendar year 2012. Letter of Peter J. Kadzik, Principal Deputy Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Senate Majority Leader (Apr. 30, 2013).

Others have proposed changes to NSL requirements that would also have substantial, albeit less direct, effects on the FISC's caseload. For example, requiring an NSL to disclose to the receiving party the factual predicate for issuing the NSL would implicate investigative information that the FBI presumably would have good operational security reasons not to disclose in national security cases, regardless of how well-supported the NSL may be.¹⁰ These changes would likely result in the government's decreasing its reliance on NSLs for records subject to such a disclosure requirement and instead bringing to the FISC more applications under Section 501 for production of such records, in order to avoid disclosure of such information to private parties.

Section 501 – Bulk Call Detail Records: Some proposals call for elimination of bulk production to the government of call detail records under Section 501. *See, e.g., Review Group Report* at 86-89, 115-19. If the bulk production of such records were eliminated, we anticipate that the government would bring to the FISC many more particularized applications for productions of such records or, as envisioned by the Review Group, for authorization to query bulk metadata retained in private hands. *Id.* at 115, 118-119. Others have considered preserving the government's ability to obtain bulk production of call detail records, provided that the FISC would review the substantive basis for querying that information (either before or after the fact). Any of these variations would impose significant new burdens on the FISC.

Nondisclosure Provisions of FISC Orders: It is not apparent that recipients of FISC orders are generally interested in publicly disclosing those orders. For example, a recipient of an order to produce records under Section 501 may challenge a related nondisclosure order after one year from the date the latter order was issued. *See* § 501(f)(2)(A)(i), codified at 50 U.S.C. § 1861(f)(2)(A)(i). From 2005 through 2012, the FISC granted approximately 750 applications under Section 501. To date, no recipient of a Section 501 order has ever challenged its non-disclosure obligations pursuant to Section 501(f)(2)(A)(i).¹¹

Nevertheless, some have proposed substantial changes in this area. For example, the Review Group recommends that nondisclosure obligations should be placed on recipients of NSLs, Section 501 orders, pen register and trap-and-trace orders, Section 702 directives, and “similar orders directing individuals, businesses, or other institutions to turn over information to the government . . . only upon a judicial finding” – presumably by the FISC in matters within its purview – “that there are reasonable grounds to believe that disclosure would significantly threaten the national security” or another specified type of harm. *Review Group Report* at

¹⁰ We note that the President's Review Group recognizes that the factual predication for NSLs is likely to involve classified information. *See Review Group Report* at 93.

¹¹ In cases now pending before the FISC, several providers are seeking a declaratory judgment that they may lawfully release certain aggregate statistical information about various types of orders they have received, including Section 501 orders. Those cases, however, were not brought under Section 501(f)(2)(A)(i).

122-23. It further recommends that a nondisclosure order “remain in effect for no longer than 180 days without judicial re-approval.” *Id.* at 123.

Practically all FISC orders of various types identify the target, either directly or by disclosing target-specific information, such as a phone number the target uses. As we understand long-standing Executive Branch classification practices, the government typically regards the targets of counterintelligence or international terrorism investigations as classified while those investigations are ongoing and for at least several years thereafter. Under an approach such as the one recommended by the Review Group, we would anticipate that each application would be accompanied by a request for a nondisclosure order and that practically all applications would entail successive requests to extend those nondisclosure orders. This new form of request would require the government to present, and the FISC to assess, facts and considerations that are distinct from whether the proposed collection is warranted and U.S. person privacy interests are adequately protected. Without arriving at a policy conclusion, we are skeptical that this proposed new process would lead to greater public understanding of the implementation of FISA or other tangible benefits, and whether any such benefits are commensurate with the burdens imposed by entertaining a line of periodic requests to extend nondisclosure obligations for a large percentage of current and former FISA targets.

Querying Section 702 Information: Section 702 of FISA concerns certain acquisitions of foreign intelligence information targeting non-U.S. persons who are reasonably believed to be outside the United States. Currently, the government may not target U.S. persons for acquisition under Section 702, *see* § 702(b)(1), (3), but information about U.S. persons may still be obtained (*e.g.*, when a U.S. person communicates with a targeted non-U.S. person). Proposals have been made to generally prohibit querying data acquired under Section 702 for information about particular U.S. persons, with an exception for emergency circumstances and for U.S. persons for whom a probable cause showing has been made.¹² These proposals would engender a new set of applications to the FISC. Decisions about querying Section 702 information are now made within the Executive Branch. As a result, the Courts do not know how often the government performs queries of data previously acquired under Section 702 in order to retrieve information about a particular U.S. person. It seems likely to us, however, that the practice would be common for U.S. persons suspected of activities of foreign intelligence interest, *e.g.*, engaging in international terrorism, so that the burden on the FISC of entertaining this new kind of application could be substantial.¹³

¹² *See, e.g., Review Group Report* at 146 (recommending that such queries be allowed “when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism”).

¹³ For a variety of reasons, a U.S. person suspected of such activity may not otherwise be a FISA target. For example, there may be probable cause to believe that a U.S. person is engaged in international terrorism, but intelligence agencies may not have the ability to implement current forms of FISA collection against that person because of the person’s location or lack of

(continued...)

Selection of FISA Judges

Currently, the Chief Justice selects eleven district court judges to serve on the FISC for staggered terms not to exceed seven years. 50 U.S.C. § 1803(a)(1), (d). In order to ensure that judges bring to the FISC experiences and practices developed around the country, these judges must represent at least seven of the judicial circuits. § 1803(a)(1). At least three of the FISC judges must reside within 20 miles of Washington, D.C., so that a judge will be continuously available to entertain urgent matters. *Id.* The Chief Justice also selects three district court or circuit court judges to serve on the Court of Review for terms not to exceed seven years. § 1803(b), (d).

Various proposals have been made to alter the selection or composition of judges on these Courts,¹⁴ apparently reflecting a concern that their current membership is, or may be perceived to be, politically or ideologically slanted.¹⁵ We urge those considering these proposals to be mindful that a smoothly functioning selection process is necessary for the Courts to discharge their responsibilities.

For the Courts to operate effectively, prolonged vacancies must be avoided. Maintaining a full complement of judges will become even more imperative if other legislative changes result in a heavier workload for the Courts. We are concerned that a selection process that involves more persons – and especially one that is likely to introduce political factors – would result in vacancies detrimental to Court operations and possibly to national security.

It has also happened from time to time that a judge being considered for service on one of the Courts is not ultimately selected because of issues arising from the mandatory background investigation.¹⁶ Knowledge of a problematic background investigation would be more widespread if more persons were involved in the selection process. The prospect of potential

¹³(...continued)
information about particular facilities.

¹⁴ The Review Group recommends dispersing the authority to select FISC judges, such that “each member of the Supreme Court would have the authority to select one or two members of the FISC from within the Circuit(s) over which she or he has jurisdiction.” *Review Group Report* at 208. Various other proposals would involve the chief judges of the judicial circuits, the President or Congressional leadership in the selection of FISC or Court of Review judges.

¹⁵ See, e.g., *Review Group Report* at 207-08 (noting that ten out of the eleven current FISC judges were appointed to the district court bench by Republican presidents). The fact that both current Court of Review judges were appointed to the federal appellate bench by a Democratic president receives less attention.

¹⁶ This background investigation is required by the security measures adopted by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence, pursuant to 50 U.S.C. § 1803(c).

embarrassment – potentially for an individual who would continue to serve publicly for the remainder of her career as a sitting federal judge – might deter qualified judges from wanting to serve on the Courts.

With specific regard to FISC operations, it is also important to maintain the practice of having multiple judges based in Washington, D.C., or its immediate vicinity. In its current form, FISA explicitly relies on a pool of local judges to handle particular kinds of time-sensitive cases. 50 U.S.C. § 1803(e)(1). This approach is sensible, given the severe security-related limitations on the ability of non-local judges to work on FISC matters in their home districts. For the same reason, there is a further need for local judges to handle other types of emergency situations, as well as complex matters that require a judge's engagement for longer than a single week in the ordinary duty rotation. *See, e.g.*, Section 702(i)(1)(B) & (3)(C) (thirty-day period for FISC to review certifications and procedures for acquisitions targeting non-U.S. persons outside the United States and to provide a written statement of the reasons for its decision). Proposals that would make it more difficult to ensure that multiple FISC judges are based in the Washington area would negatively affect FISC operations.

Finally, proposals to disperse the selection authority among the associate justices of the Supreme Court or chief judges of the federal circuits ignore the Chief Justice's unique role in the Judicial Branch. The Chief Justice is the President of the Judicial Conference of the United States, which includes the responsibility to assign federal judges across the country to the various Conference committees and other tasks, including service on special courts such as the Judicial Panel on Multidistrict Litigation.¹⁷ The Chief Justice is therefore uniquely positioned, with the assistance of the Director of the Administrative Office of the United States Courts, to review the federal judiciary and select qualified judges for additional work on the FISC or the Court of Review.¹⁸

*Public Disclosure and Declassification of Court Opinions
and Other FISA-Related Information*

The Judicial Branch is committed to making court opinions available to the public unless there is a compelling need for secrecy. The FISC regularly makes publicly available those of its opinions that do not contain classified information.

A number of legislative proposals are aimed at making more information available to the public about FISA legal interpretations and other aspects of FISA implementation. Cases involving declassification and release of such information are pending before the Courts, so we are especially constrained from addressing the substantive merits of these proposals. We do,

¹⁷ The associate justices have no role in this process.

¹⁸ Although the selection of judges for the FISC and the Court of Review is often labelled as an "appointment," it is more accurately considered to be a designation to serve on the Court.

however, believe that the following points should be kept in mind as these proposals are assessed.

First, to the extent that the Courts may be assigned a new role in declassification and release of information, that role should accord with the constitutional allocation of functions in that sphere. Under the Constitution, classification of information in order to protect national security has been considered an Executive Branch responsibility. *See Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). When necessary to resolve a case before it (*e.g.*, under the Freedom of Information Act, 5 U.S.C. § 552), a federal court may review classification decisions made by the Executive Branch, typically under a deferential standard. *See, e.g., Krikorian v. Dep't of State*, 984 F.2d 461, 464 (D.C. Cir. 1993).

Second, while we support the highest degree of transparency consistent with protection of sensitive intelligence sources and methods and other properly classified information, we believe that there are practical limitations as to what can be achieved. Significant FISC opinions frequently involve the application of law to a complex set of facts, *e.g.*, how to apply FISA's four-part definition of "electronic surveillance," *see* 50 U.S.C. § 1801(f), to a proposed surveillance method for a new communications technology. The government may often believe it necessary to withhold from the public details about how a surveillance is conducted, so that valid intelligence targets are not given a lesson in how to evade it. But a redacted opinion that does not contain this factual information may merely recite statutory provisions or provide a partial discussion of how those provisions were applied, without the factual context necessary to understand the opinion's reasoning and result. In such cases, partial releases of opinions run the risk of distorting, rather than illuminating, the reasoning and result of Court opinions. That risk is probably even greater for summaries of opinions that are offered as public substitutes for withheld opinions, rather than as guides to opinions that are published.

We further suggest that, apart from the need to protect national security, legislative proposals for release of Court opinions should take into consideration appropriate protections for other categories of information, such as the names of government personnel or information implicating substantial privacy interests. Finally, any procedural framework for public disclosure should permit the Court a reasonable time to take any necessary action. Some proposals would impose severe time constraints.

FISC Role in Monitoring and Enforcing Executive Branch Compliance

A common objective of proposed changes to FISA is to enhance monitoring and oversight of intelligence gathering activities. Some particularly envision new roles for the FISC in this regard.

All three branches of government have responsibilities regarding FISA implementation. But it is important to recognize that the FISC does not have, and should not have, general auditing and oversight functions comparable to those performed by an Inspector General or a Congressional committee with jurisdiction over a particular Executive Branch agency. Judicial

involvement in the FISA process occurs within the context of Article III's cases or controversies requirement. FISA currently respects those Article III limitations by contemplating FISC involvement in the form of monitoring and enforcing compliance with FISC orders and authorizations, *i.e.*, within the context of FISC cases.¹⁹ To the extent that legislative proposals would enhance FISC review of Executive Branch compliance within the context of a particular FISC case, they are less likely to present constitutional difficulties. On the other hand, proposals that would assign to the FISC duties that are disassociated from any case before it would seriously risk exceeding constitutional limitations on the involvement of an Article III court in Executive Branch operations.²⁰

Finally, in line with the foregoing discussion of other matters, if the FISC were to be given a greater role in monitoring and enforcing Executive Branch compliance, it would require a commensurate increase of its current resources to discharge those responsibilities effectively.

¹⁹ See 50 U.S.C. §§ 1803(h) ("Nothing in this chapter shall be construed to reduce or contravene the inherent authority of the [FISC] to determine or enforce compliance with an order or rule of such court or with a procedure approved by such court."); 1805(d)(3) ("At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated."); 1824(d)(3) (same for physical search).

²⁰ See, *e.g.*, *Summers v. Earth Island Institute*, 555 U.S. 488, 492 (2009) (Article III limits the judicial power to deciding cases and controversies and, except "when necessary in the execution of that function, courts have no charter to review and revise legislative and executive action"); *In re Sealed Case*, 310 F.3d 717, 731 (FISA Ct. Rev. 2002) (FISC "may well have exceeded the constitutional bounds that restrict an Article III court" by asserting authority over "the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I)" (per curiam).



ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

HONORABLE JOHN D. BATES
Director

WASHINGTON, D.C. 20544

January 13, 2014

Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Chairman Goodlatte:

To better address the continuing interest from several Congressional committees in the views of the Judiciary regarding potential changes to foreign intelligence surveillance law and practice, I am writing to provide the following perspectives on certain proposals currently under consideration.

Traditionally, the views of the Judiciary on legislative matters are expressed through the Judicial Conference of the United States, for which I serve as Secretary. However, because the matters at issue here relate to special expertise and experience of only a small number of judges on two specialized courts, the Conference has not at this time been engaged to deliberate on them. In my capacity as Director of the Administrative Office of the United States Courts, I have responsibility for facilitating the administration of the federal courts and, furthermore, the Chief Justice of the United States has requested that I act as a liaison for the Judiciary on matters concerning the Foreign Intelligence Surveillance Act (FISA). In considering such matters, I benefit from having served as Presiding Judge of the Foreign Intelligence Surveillance Court (FISC).

Enclosed is a document setting forth the Judiciary's comments concerning certain potential changes to FISA and proceedings before the FISC and the Foreign Intelligence Surveillance Court of Review. In preparing this document, I have consulted with the current Presiding Judges of the FISC and the Court of Review, as well as with other judges who serve or have served on those courts. For the sake of convenience, throughout the enclosed document (and in the summary below) I use the terms "we" and "our" to describe the Judiciary's institutional perspectives.

Honorable Bob Goodlatte
Page 2

Our comments focus on the operational impact on the Courts from certain proposed changes, but we do not express views on the policy choices that the political branches are considering. We are hopeful, of course, that any changes will both enhance our national security and provide appropriate respect and protection for privacy and civil-liberties interests. Achieving that goal undoubtedly will require great attention to the details of any adjustments that are undertaken. For example, it may not be important whether an outside participant in certain matters before the Courts is labeled an *amicus curiae* or public advocate; what matters is the specific structure and role of such a participant.

The following is a summary of our key comments:

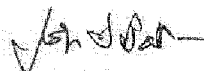
- It is imperative that any significant increase in workload for the Courts be accompanied by a commensurate increase in resources.
- Some proposed changes would profoundly increase the Courts' workload. Even if additional financial, personnel, and physical resources were provided, any substantial increase in workload could nonetheless prove disruptive to the Courts' ability to perform their duties, including responsibilities under FISA and the Constitution to ensure that the privacy interests of United States citizens and others are adequately protected.
- The participation of a privacy advocate is unnecessary—and could prove counterproductive—in the vast majority of FISA matters, which involve the application of a probable cause or other factual standard to case-specific facts and typically implicate the privacy interests of few persons other than the specified target. Given the nature of FISA proceedings, the participation of an advocate would neither create a truly adversarial process nor constructively assist the Courts in assessing the facts, as the advocate would be unable to communicate with the target or conduct an independent investigation. Advocate involvement in run-of-the-mill FISA matters would substantially hamper the work of the Courts without providing any countervailing benefit in terms of privacy protection or otherwise; indeed, such pervasive participation could actually undermine the Courts' ability to receive complete and accurate information on the matters before them.
- In those matters in which an outside voice could be helpful, it is critical that the participation of an advocate be structured in a manner that maximizes assistance to the Courts and minimizes disruption to their work. An advocate appointed at the discretion of the Courts is likely to be helpful, whereas a standing advocate with independent authority to intervene at will could actually be counterproductive.

Honorable Bob Goodlatte
Page 3

- Drastically expanding the FISC's caseload by assigning to it in excess of 20,000 administrative subpoena-type cases (i.e., NSI.s) per year – even with a corresponding injection of resources and personnel – would fundamentally transform the nature of the FISC to the detriment of its current responsibilities.
- It is important that the process for selection of FISC and Court of Review judges remain both expeditious and fully confidential; the Chief Justice is uniquely positioned to select qualified judges for those Courts.
- In many cases, public disclosure of Court decisions is not likely to enhance the public's understanding of FISA implementation if the discussion of classified information within those opinions is withheld. Releasing freestanding summaries of Court opinions is likely to promote confusion and misunderstanding.
- Care should be taken not to place the Courts in an "oversight" role that exceeds their constitutional responsibility to decide cases and controversies.

Thank you for your previously expressed interest in the perspectives of the Judiciary on these matters. Although these comments are not intended as expressions of support or opposition to particular introduced bills, I hope they are helpful to Congress in its deliberations on potential legislation. We have also provided these comments to the Administration. If we can be of further assistance to you, please do not hesitate to contact me at 202-502-3000 or our Office of Legislative Affairs at 202-502-1700.

Sincerely,



John D. Bates
Director

Enclosure

Identical letter sent to: Honorable John Conyers, Jr.
Honorable Patrick J. Leahy
Honorable Charles E. Grassley
Honorable Dianne Feinstein
Honorable Saxby Chambliss
Honorable Mike Rogers
Honorable C.A. Dutch Ruppersberger

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

January 17, 2014

January 17, 2014

PRESIDENTIAL POLICY DIRECTIVE/PPD-28

SUBJECT: Signals Intelligence Activities

The United States, like other nations, has gathered intelligence throughout its history to ensure that national security and foreign policy decisionmakers have access to timely, accurate, and insightful information.

The collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. At the same time, signals intelligence activities and the possibility that such activities may be improperly disclosed to the public pose multiple risks. These include risks to: our relationships with other nations, including the cooperation we receive from other nations on law enforcement, counterterrorism, and other issues; our commercial, economic, and financial interests, including a potential loss of international trust in U.S. firms and the decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes; the credibility of our commitment to an open, interoperable, and secure global Internet; and the protection of intelligence sources and methods.

In addition, our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

In determining why, whether, when, and how the United States conducts signals intelligence activities, we must weigh all of these considerations in a context in which information and communications technologies are constantly changing. The evolution of technology has created a world where communications important to our national security and the communications all of us make as part of our daily lives are transmitted through the same channels. This presents new and diverse opportunities for, and challenges with respect to, the collection of intelligence - and especially signals intelligence. The United States Intelligence Community (IC) has achieved remarkable success in developing enhanced capabilities to perform its signals intelligence mission in this rapidly changing world, and these enhanced capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment.¹ The

¹ For the purposes of this directive, the terms "Intelligence Community" and "elements of the Intelligence Community" shall have the same meaning as they do in Executive Order 12333 of December 4, 1981, as amended (Executive Order 12333).

United States must preserve and continue to develop a robust and technologically advanced signals intelligence capability to protect our security and that of our partners and allies. Our signals intelligence capabilities must also be agile enough to enable us to focus on fleeting opportunities or emerging crises and to address not only the issues of today, but also the issues of tomorrow, which we may not be able to foresee.

Advanced technologies can increase risks, as well as opportunities, however, and we must consider these risks when deploying our signals intelligence capabilities. The IC conducts signals intelligence activities with care and precision to ensure that its collection, retention, use, and dissemination of signals intelligence account for these risks. In light of the evolving technological and geopolitical environment, we must continue to ensure that our signals intelligence policies and practices appropriately take into account our alliances and other partnerships; the leadership role that the United States plays in upholding democratic principles and universal human rights; the increased globalization of trade, investment, and information flows; our commitment to an open, interoperable and secure global Internet; and the legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations.

Presidents have long directed the acquisition of foreign intelligence and counterintelligence² pursuant to their constitutional authority to conduct U.S. foreign relations and to fulfill their constitutional responsibilities as Commander in Chief and Chief Executive. They have also provided direction on the conduct of intelligence activities in furtherance of these authorities and responsibilities, as well as in execution of laws enacted by the Congress. Consistent with this historical practice, this directive articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes.³

Section 1. Principles Governing the Collection of Signals Intelligence.

Signals intelligence collection shall be authorized and conducted consistent with the following principles:

- (a) The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in

² For the purposes of this directive, the terms "foreign intelligence" and "counterintelligence" shall have the same meaning as they have in Executive Order 12333. Thus, "foreign intelligence" means "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists," and "counterintelligence" means "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." Executive Order 12333 further notes that "[i]ntelligence includes foreign intelligence and counterintelligence."

³ Unless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications or information about communications, except that it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities.

accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives.

- (b) Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.
- (c) The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage⁴ to U.S. companies and U.S. business sectors commercially.
- (d) Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.

Sec. 2. Limitations on the Use of Signals Intelligence Collected in Bulk.

Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern global communications. The United States must consequently collect signals intelligence in bulk⁵ in certain circumstances in order to identify these threats. Routine communications and communications of national security interest increasingly transit the same networks, however, and the collection of signals intelligence in bulk may consequently result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value. The United States will therefore impose new limits on its use of signals intelligence collected in bulk. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data

⁴ Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.

⁵ The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).

only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S. or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section.

The Assistant to the President and National Security Advisor (APNSA), in consultation with the Director of National Intelligence (DNI), shall coordinate, on at least an annual basis, a review of the permissible uses of signals intelligence collected in bulk through the National Security Council Principals and Deputies Committee system identified in PPD-1 or any successor document. At the end of this review, I will be presented with recommended additions to or removals from the list of the permissible uses of signals intelligence collected in bulk.

The DNI shall maintain a list of the permissible uses of signals intelligence collected in bulk. This list shall be updated as necessary and made publicly available to the maximum extent feasible, consistent with the national security.

Sec. 3. Refining the Process for Collecting Signals Intelligence.

U.S. intelligence collection activities present the potential for national security damage if improperly disclosed. Signals intelligence collection raises special concerns, given the opportunities and risks created by the constantly evolving technological and geopolitical environment; the unique nature of such collection and the inherent concerns raised when signals intelligence can only be collected in bulk; and the risk of damage to our national security interests and our law enforcement, intelligence-sharing, and diplomatic relationships should our capabilities or activities be compromised. It is, therefore, essential that national security policymakers consider carefully the value of signals intelligence activities in light of the risks entailed in conducting these activities.

To enable this judgment, the heads of departments and agencies that participate in the policy processes for establishing signals intelligence priorities and requirements shall, on an annual basis, review any priorities or requirements identified by their departments or agencies and advise the DNI whether each should be maintained, with a copy of the advice provided to the APNSA.

Additionally, the classified Annex to this directive, which supplements the existing policy process for reviewing signals intelligence activities, affirms that determinations about whether and how to conduct signals intelligence activities must

carefully evaluate the benefits to our national interests and the risks posed by those activities.⁵

Sec. 4. Safeguarding Personal Information Collected Through Signals Intelligence.

All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information.⁷ U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.⁶

- (a) *Policies and Procedures.* The DNI, in consultation with the Attorney General, shall ensure that all elements of the IC establish policies and procedures that apply the following principles for safeguarding personal information collected from signals intelligence activities. To the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality:⁹
 - i. *Minimization.* The sharing of intelligence that contains personal information is necessary to protect our national security and advance our foreign policy interests, as it enables the United States to coordinate activities across our government. At the same time, however, by setting appropriate limits on such sharing, the United States takes legitimate privacy concerns into account and decreases the risks that personal information will be misused or mishandled. Relatedly, the significance to our national security of intelligence is not always apparent upon an initial review of information: intelligence must be retained for a sufficient period of time for the IC to understand its relevance and use

⁵ Section 3 of this directive, and the directive's classified Annex, do not apply to (1) signals intelligence activities undertaken by or for the Federal Bureau of Investigation in support of predicated investigations other than those conducted solely for purposes of acquiring foreign intelligence; or (2) signals intelligence activities undertaken in support of military operations in an area of active hostilities, covert action, or human intelligence operations.

⁷ Departments and agencies shall apply the term "personal information" in a manner that is consistent for U.S. persons and non-U.S. persons. Accordingly, for the purposes of this directive, the term "personal information" shall cover the same types of information covered by "information concerning U.S. persons" under section 2.3 of Executive Order 12333.

⁶ The collection, retention, and dissemination of information concerning "United States persons" is governed by multiple legal and policy requirements, such as those required by the Foreign Intelligence Surveillance Act and Executive Order 12333. For the purposes of this directive, the term "United States person" shall have the same meaning as it does in Executive Order 12333.

⁹ The policies and procedures of affected elements of the IC shall also be consistent with any additional IC policies, standards, procedures, and guidance the DNI, in coordination with the Attorney General, the heads of IC elements, and the heads of any other departments containing such elements, may issue to implement these principles. This directive is not intended to alter the rules applicable to U.S. persons in Executive Order 12333, the Foreign Intelligence Surveillance Act, or other applicable law.

it to meet our national security needs. However, long-term storage of personal information unnecessary to protect our national security is inefficient, unnecessary, and raises legitimate privacy concerns. Accordingly, IC elements shall establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities.

- Dissemination: Personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333.
- Retention: Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.

Additionally, within 180 days of the date of this directive, the DNI, in coordination with the Attorney General, the heads of other elements of the IC, and the heads of departments and agencies containing other elements of the IC, shall prepare a report evaluating possible additional dissemination and retention safeguards for personal information collected through signals intelligence, consistent with technical capabilities and operational needs.

- ii. *Data Security and Access.* When our national security and foreign policy needs require us to retain certain intelligence, it is vital that the United States take appropriate steps to ensure that any personal information contained within that intelligence is secure. Accordingly, personal information shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, Presidential directives, IC directives, and associated policies. Access to such personal information shall be limited to authorized personnel with a need to know the information to perform their mission, consistent with the personnel security requirements of relevant Executive Orders, IC directives, and associated policies. Such personnel will be provided appropriate and adequate training in the principles set forth in this directive. These persons may access and use the information consistent with applicable laws and Executive Orders and the principles of this directive; personal information for which no determination has been made that it can be permissibly disseminated or retained under section 4(a)(i) of this directive shall be accessed only in order to make such determinations

(or to conduct authorized administrative, security, and oversight functions).

- iii. *Data Quality.* IC elements strive to provide national security policymakers with timely, accurate, and insightful intelligence, and inaccurate records and reporting can not only undermine our national security interests, but also can result in the collection or analysis of information relating to persons whose activities are not of foreign intelligence or counterintelligence value. Accordingly, personal information shall be included in intelligence products only as consistent with applicable IC standards for accuracy and objectivity, as set forth in relevant IC directives. Moreover, while IC elements should apply the IC Analytic Standards as a whole, particular care should be taken to apply standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.
- iv. *Oversight.* The IC has long recognized that effective oversight is necessary to ensure that we are protecting our national security in a manner consistent with our interests and values. Accordingly, the policies and procedures of IC elements, and departments and agencies containing IC elements, shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information, to include periodic auditing against the standards required by this section.

The policies and procedures shall also recognize and facilitate the performance of oversight by the Inspectors General of IC elements, and departments and agencies containing IC elements, and other relevant oversight entities, as appropriate and consistent with their responsibilities. When a significant compliance issue occurs involving personal information of any person, regardless of nationality, collected as a result of signals intelligence activities, the issue shall, in addition to any existing reporting requirements, be reported promptly to the DNI, who shall determine what, if any, corrective actions are necessary. If the issue involves a non-United States person, the DNI, in consultation with the Secretary of State and the head of the notifying department or agency, shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.

- (b) *Update and Publication.* Within 1 year of the date of this directive, IC elements shall update or issue new policies and procedures as necessary to implement section 4 of this directive, in coordination with the DNI. To enhance public understanding of, and promote public trust in, the safeguards in place to protect personal information, these updated or newly issued policies and procedures shall be publicly released to the maximum extent possible, consistent with classification requirements.

- (c) *Privacy and Civil Liberties Policy Official.* To help ensure that the legitimate privacy interests all people share related to the handling of their personal information are appropriately considered in light of the principles in this section, the APNSA, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy (OSTP) shall identify one or more senior officials who will be responsible for working with the DNI, the Attorney General, the heads of other elements of the IC, and the heads of departments and agencies containing other elements of the IC, as appropriate, as they develop the policies and procedures called for in this section.
- (d) *Coordinator for International Diplomacy.* The Secretary of State shall identify a senior official within the Department of State to coordinate with the responsible departments and agencies the United States Government's diplomatic and foreign policy efforts related to international information technology issues and to serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.

Sec. 5. Reports.

- (a) Within 180 days of the date of this directive, the DNI shall provide a status report that updates me on the progress of the IC's implementation of section 4 of this directive.
- (b) The Privacy and Civil Liberties Oversight Board is encouraged to provide me with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.
- (c) Within 120 days of the date of this directive, the President's Intelligence Advisory Board shall provide me with a report identifying options for assessing the distinction between metadata and other types of information, and for replacing the "need-to-share" or "need-to-know" models for classified information sharing with a Work-Related Access model.
- (d) Within 1 year of the date of this directive, the DNI, in coordination with the heads of relevant elements of the IC and OSTP, shall provide me with a report assessing the feasibility of creating software that would allow the IC more easily to conduct targeted information acquisition rather than bulk collection.

Sec. 6. General Provisions.

- (a) Nothing in this directive shall be construed to prevent me from exercising my constitutional authority, including as Commander in Chief, Chief Executive, and in the conduct of foreign affairs, as well as my statutory authority. Consistent with this principle, a recipient of this directive may at any time recommend to me, through the APNSA, a change to the policies and procedures contained in this directive.

- (b) Nothing in this directive shall be construed to impair or otherwise affect the authority or responsibility granted by law to a United States Government department or agency, or the head thereof, or the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals. This directive is intended to supplement existing processes or procedures for reviewing foreign intelligence or counterintelligence activities and should not be read to supersede such processes and procedures unless explicitly stated.
- (c) This directive shall be implemented consistent with applicable U.S. law and subject to the availability of appropriations.
- (d) This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

#