Agrast, Mark D. (OLA)

From:	Agrast, Mark D. (OLA)
Sent:	Friday, June 28, 2013 6:34 PM
To:	O'Neil, David (ODAG); Anderson, Trisha (ODAG)
Cc:	Kadzik, Peter J (OLA)
Subject:	FW:
Attachments:	Patriot Act letter 062813.pdf

FYI.

From (b)(3) per ODNI
Sent: Friday, June 28, 2013 6:26 PM
To (b)(3) per NSA; Carlin, John (NSD) (b)(3), (b)(6) per ODNI (b)(6) Caitlin Hayden; (b)(6) Greta Lundeberg (b)(6) Jill Robinson (b)(6) Bernadette Meehan; (b)(6) Avril Haines (b)(6) Christopher Fonzone (b)(3) per NSA; pjreyno@nsa.gov; Agrast, Mark D. (OLA); Gauhar, Tashina (NSD); Wiegmann, Brad (NSD)
Cc (b)(3), (b)(6) per ODNI
Subject:

NSA, DOJ, NSS colleagues –

As you probably all know the DNI has received the attached letter from 26 Senators was received today by the DNI. The DNI would like to sign out a response next week, because he is going on leave after that.

We will circulate a draft early next week for commen (b)(3), (b)(6) per ODNI doesn't know it yet but he will have the lead in drafting it). Our plan is t (b)(5) per ODNI). We'll say th (b)(5) per ODNI .

Here's what I'd ask this group:

(b)(5) per ODNI
(b)(5) per ODNI (b)(5) per NSC; (b)(5) per ODNI (b)(5) per
(b)(5) per ODNI .
(b)(5) per ODNI
.
(b)(5) per ODNI (b)(3), (b)(5) per NSA; (b)(5) per ODNI
(b)(3), (b)(5) per NSA; (b)(5) per NSC; (b)(5) per ODNI (b)(3), (b)(5) per NSA; (b)(5) per ODNI
.

In light of the DNI's desires and the holiday next week, please provide responses NLT Monday noon.

Thanks to all. What a cluster this whole thing is.

Bob

United States Senate

WASHINGTON, DC 20510

June 27, 2013

The Honorable James R. Clapper
Director of National Intelligence
Washington, D.C. 20511

Dear Director Clapper:

Earlier this month, the executive branch acknowledged for the first time that the "business records" provision of the USA PATRIOT Act has been secretly reinterpreted to allow the government to collect the private records of large numbers of ordinary Americans. We agree that it is regrettable that this fact was first revealed through an unauthorized disclosure rather than an official acknowledgment by the administration, but we appreciate the comments that the President has made welcoming debate on this topic.

In our view, the bulk collection and aggregation of Americans' phone records has a significant impact on Americans' privacy that exceeds the issues considered by the Supreme Court in *Smith v. Maryland.* That decision was based on the technology of the rotary-dial era and did not address the type of ongoing, broad surveillance of phone records that the government is now conducting. These records can reveal personal relationships, family medical issues, political and religious affiliations, and a variety of other private personal information. This is particularly true if these records are collected in a manner that includes cell phone locational data, effectively turning Americans' cell phones into tracking devices. We are concerned that officials have told the press that the collection of this location data is currently authorized.

Furthermore, we are troubled by the possibility of this bulk collection authority being applied to other categories of records. The PATRIOT Act's business records authority is very broad in its scope. It can be used to collect information on credit card purchases, pharmacy records, library records, firearm sales records, financial information, and a range of other sensitive subjects. And the bulk collection authority could potentially be used to supersede bans on maintaining gun owner databases, or laws protecting the privacy of medical records, financial records, and records of book and movie purchases. These other types of bulk collection could clearly have a significant impact on Americans' privacy and liberties as well.

Senior officials have noted that there are rules in place governing which government personnel are allowed to review the bulk phone records data and when. Rules of this sort, if they are effectively enforced, can mitigate the privacy impact of this large-scale data collection, but they do not erase it entirely. Furthermore, over its history the intelligence community has sometimes failed to keep sensitive information secure from those who would misuse it, and even if these rules are well-intentioned they will not eliminate all opportunities for abuse.

It has been suggested that the privacy impact of particular methods of domestic surveillance should be weighed against the degree to which the surveillance enhances our national security. With this in mind, we are interested in hearing more details about why you believe that the bulk phone records collection program provides any unique value. We have now heard about a few cases in which these bulk phone records provided some information that was relevant to

investigators, but we would like a full explanation of whether or not the records that were actually useful could have been obtained directly from the appropriate phone companies in an equally expeditious manner using either a regular court order or an emergency authorization.

Finally, we are concerned that by depending on secret interpretations of the PATRIOT Act that differed from an intuitive reading of the statute, this program essentially relied for years on a secret body of law. Statements from senior officials that the PATRIOT Act authority is "analogous to a grand jury subpoena" and that the NSA "[doesn't] hold data on US citizens" had the effect of misleading the public about how the law was being interpreted and implemented. This prevented our constituents from evaluating the decisions that their government was making, and will unfortunately undermine trust in government more broadly. The debate that the President has now welcomed is an important first step toward restoring that trust.

To ensure that an informed discussion on PATRIOT Act authorities can take place, we ask that you direct the Intelligence Community to provide unclassified answers to the following questions:

- How long has the NSA used PATRIOT Act authorities to engage in bulk collection of Americans' records? Was this collection underway when the law was reauthorized in 2006?
- Has the NSA used USA PATRIOT Act authorities to conduct bulk collection of any other types of records pertaining to Americans, beyond phone records?
- Has the NSA collected or made any plans to collect Americans' cell-site location data in bulk?
- Have there been any violations of the court orders permitting this bulk collection, or of the rules governing access to these records? If so, please describe these violations.
- Please identify any specific examples of instances in which intelligence gained by reviewing phone records obtained through Section 215 bulk collection proved useful in thwarting a particular terrorist plot.
- Please provide specific examples of instances in which useful intelligence was gained by reviewing phone records that could not have been obtained without the bulk collection authority, if such examples exist.
- Please describe the employment status of all persons with conceivable access to this data, including IT professionals, and detail whether they are federal employees, civilian or military, or contractors.

Thank you for your attention to this important matter. We look forward to further discussion in the weeks ahead.

Sincerely,

Diane Feinstein

Patrick Leahy

Dianne Feinstein

Mark Udall

Tom Harkin

Richard Durbin

Max Baucus

Jeanne Shaheen

Tom Heller

Jeffrey A. Merkley

Maria Cantwell

Al Franken

Mazie Hirono

Tom Udall

Patty Murray

Bernard Sanders

Mark Begich

Chris Coons

Elizabeth Warren

Cheung, Denise (OAG)

From: Cheung, Denise (OAG)
Sent: Friday, August 9, 2013 11:52 AM
To: Richardson, Margaret (OAG)
Cc: Thompson, Karl (OAG)
Subject: FW: Final BR White Paper
Attachments: BR White Paper -- Final v2--tracked changes.docx; BR White Paper -- Final v2.docx; BR White Paper -- Final v2.pdf

FYI

From (b)(6) per NSD (NSD)
Sent: Friday, August 09, 2013 11:43 AM
To: Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Kneedler, Edwin S (OSG); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD); (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

Duplicative Information - See Document ID 0.7.10663.25902

Cheung, Denise (OAG)

From: Cheung, Denise (OAG)
Sent: Friday, August 9, 2013 2:47 PM
To: Kendricks, David (OAG)
Cc: Thompson, Karl (OAG); Richardson, Margaret (OAG)
Subject: Final BR White Paper
Attachments: BR White Paper -- Final v3.docx; BR White Paper -- Final v3.pdf

This should be the final version of the White Paper. OPA should be releasing this in the next half hour or so, and OLA also is planning on providing it to Judiciary, Intelligence, and leadership staff at 3:00 p.m.

Thompson, Karl (OAG)

From: Thompson, Karl (OAG)
Sent: Friday, August 9, 2013 3:21 PM
To: Richardson, Margaret (OAG)
Cc: Cheung, Denise (OAG)
Subject: FW: Final BR White Paper
Attachments: Administration White Paper Section 215.pdf

It's out…

From: Fallon, Brian (OPA)
Sent: Friday, August 09, 2013 3:17 PM
To: Yang, Anthony (OSG) (b)(6) per NSD (NSD); Kneedler, Edwin S (OSG); Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Dreeben, Michael R (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA); (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD) (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

The attached version of the document has been released to the press.

From: Yang, Anthony (OSG)
Sent: Friday, August 09, 2013 2:39 PM
To (b)(6) per NSD (NSD); Kneedler, Edwin S (OSG); Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Dreeben, Michael R (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA); (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD) (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

Do we know approximately when the document will be released today? And could someone please let the group know once it has been publicly disseminated whether any additional edits were made?

Many thanks,
Tony

From (b)(6) per NSD (NSD)
Sent: Friday, August 09, 2013 1:00 PM
To: Kneedler, Edwin S (OSG); Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG);

Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD) (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

Thanks, Ed. We've made the change. Please find attached the most recent final version.

(b)(6) per NSD

<< File: BR White Paper -- Final v3.docx >> << File: BR White Paper -- Final v3.pdf >>

From: Kneedler, Edwin S (OSG)
Sent: Friday, August 09, 2013 12:54 PM
To (b)(6) per NSD (NSD); Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD) (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

I thin (b) (5)

From (b)(6) per NSD (NSD)
Sent: Friday, August 09, 2013 12:34 PM
To: Kneedler, Edwin S (OSG); Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD) (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

Hi Ed,

I appreciate your perspective on this sentence and understand the underlying concern. (b) (5)

(b)(6) per NSD

From: Kneedler, Edwin S (OSG)

Sent: Friday, August 09, 2013 12:19 PM
To (b)(6) per NSD (NSD); Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD) (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

On p.14, in the full paragraph, in the sentence beginnin (b) (5) -- can w (b) (5) an (b) (5)

Give (b) (5)

In th (b) (5) I think that (b) (5)

From (b)(6) per NSD (NSD)
Sent: Friday, August 09, 2013 11:43 AM
To: Wiegmann, Brad (NSD); Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Kneedler, Edwin S (OSG); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD); (b)(6) per NSD (NSD)
Subject: RE: Final BR White Paper

All,

Please find attached the final, final version of the White Paper. A version with tracked changes from the version sent at this morning is also attached.

Changes are largely limited to spacing issues with the following exceptions: (1) a minor change was made to a (b) (5); (2 (b) (5); and (3) o (b) (5). These changes were mad (b) (5), and we do not believe they should raise any concerns. Nevertheless, please let us know quickly if there are any objections.

Thanks again,
(b)(6) per NSD

<< File: BR White Paper -- Final v2--tracked changes.docx >> << File: BR White Paper -- Final v2.docx >> << File: BR White Paper -- Final v2.pdf >>

(b)(6) per NSD
Counsel | Office of Law & Policy | National Security Division | U.S. Department of Justice | ST (b) (6)

From: Wiegmann, Brad (NSD)
Sent: Friday, August 09, 2013 1:46 AM
To: Thompson, Karl (OAG); Anderson, Trisha (ODAG); Goldberg, Stuart (ODAG); Carlin, John (NSD); Singh, Anita (NSD); Gauhar, Tashina (NSD); Boyer, Robert (NSD); Hardee, Christopher (NSD) (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); (b)(6) per NSD (NSD); Evans, Stuart (NSD); Seitz, Virginia A (OLC); Krass, Caroline D. (OLC); Singdahlsen, Jeffrey (OLC); Kneedler, Edwin S (OSG); Dreeben, Michael R (OSG); Yang, Anthony (OSG); Bash, John (OSG); Coppolino, Tony (CIV); Delery, Stuart F. (CIV); Berman, Marcia (CIV); Brinkmann, Beth (CIV); Fallon, Brian (OPA); Ames, Andrew (OPA); Gilligan, Jim (CIV); Shapiro, Elizabeth (CIV); Agrast, Mark D. (OLA); Simpson, Tammi (OLA); Ruppert, Mary (OLA) (b)(6) per NSD (b)(6) per NSD (NSD) (b)(6) per NSD (NSD); Cheung, Denise (OAG); Taylor, Elizabeth G. (OAAG); Toscas, George (NSD); (b)(6) per NSD (NSD)
Subject: Final BR White Paper

Here is the final BR white paper (word doc and PDF), absent objection. Thanks to everyone for your help on this project.

<< File: BR White Paper -- Final.docx >>

<< File: BR White Paper -- Final.pdf >>

ADMINISTRATION WHITE PAPER

BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT

August 9, 2013

BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT

This white paper explains the Government's legal basis for an intelligence collection program under which the Federal Bureau of Investigation (FBI) obtains court orders directing certain telecommunications service providers to produce telephony metadata in bulk. The bulk metadata is stored, queried and analyzed by the National Security Agency (NSA) for counterterrorism purposes. The Foreign Intelligence Surveillance Court ("the FISC" or "the Court") authorizes this program under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted as section 215 of the USA PATRIOT Act (Section 215). The Court first authorized the program in 2006, and it has since been renewed thirty-four times under orders issued by fourteen different FISC judges. This paper explains why the telephony metadata collection program, subject to the restrictions imposed by the Court, is consistent with the Constitution and the standards set forth by Congress in Section 215. Because aspects of this program remain classified, there are limits to what can be said publicly about the facts underlying its legal authorization. This paper is an effort to provide as much information as possible to the public concerning the legal authority for this program, consistent with the need to protect national security, including intelligence sources and methods. While this paper summarizes the legal basis for the program, it is not intended to be an exhaustive analysis of the program or the legal arguments or authorities in support of it.

EXECUTIVE SUMMARY

Under the telephony metadata collection program, telecommunications service providers, as required by court orders issued by the FISC, produce to the Government certain information about telephone calls, principally those made within the United States and between the United States and foreign countries. This information is limited to telephony metadata, which includes information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted. Importantly, this information does *not* include any information about the content of those calls—the Government cannot, through this program, listen to or record any telephone conversations.

This telephony metadata is important to the Government because, by analyzing it, the Government can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States. The program is carefully limited to this purpose: it is not lawful for anyone to query the bulk telephony metadata for any purpose other than counterterrorism, and Court-imposed rules strictly limit all such queries. The program includes internal oversight mechanisms to prevent misuse, as well as external reporting requirements to the FISC and Congress.

Multiple FISC judges have found that Section 215 authorizes the collection of telephony metadata in bulk. Section 215 permits the FBI to seek a court order directing a business or other entity to produce records or documents when there are reasonable grounds to believe that the information sought is relevant to an authorized investigation of international terrorism. Courts have held in the analogous contexts of civil discovery and criminal and administrative

investigations that "relevance" is a broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated. Although broad in scope, the telephony metadata collection program meets the "relevance" standard of Section 215 because there are "reasonable grounds to believe" that this category of data, when queried and analyzed consistent with the Court-approved standards, will produce information pertinent to FBI investigations of international terrorism, and because certain analytic tools used to accomplish this objective require the collection and storage of a large volume of telephony metadata. This does not mean that Section 215 authorizes the collection and storage of all types of information in bulk: the relevance of any particular data to investigations of international terrorism depends on all the facts and circumstances. For example, communications metadata is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data, are particularly important to a broad range of investigations of international terrorism.

Moreover, information concerning the use of Section 215 to collect telephony metadata in bulk was made available to all Members of Congress, and Congress reauthorized Section 215 without change after this information was provided. It is significant to the legal analysis of the statute that Congress was on notice of this activity and of the source of its legal authority when the statute was reauthorized.

The telephony metadata collection program also complies with the Constitution. Supreme Court precedent makes clear that participants in telephone calls lack a reasonable expectation of privacy for purposes of the Fourth Amendment in the telephone numbers used to make and receive their calls. Moreover, particularly given the Court-imposed restrictions on accessing and disseminating the data, any arguable privacy intrusion arising from the collection of telephony metadata would be outweighed by the public interest in identifying suspected terrorist operatives and thwarting terrorist plots, rendering the program reasonable within the meaning of the Fourth Amendment. Likewise, the program does not violate the First Amendment, particularly given that the telephony metadata is collected to serve as an investigative tool in authorized investigations of international terrorism.

I. THE TELEPHONY METADATA COLLECTION PROGRAM

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States.

One important method that the Government has developed to accomplish this task is analysis of metadata associated with telephone calls within, to, or from the United States. The term "metadata" as used here refers to data collected under the program that is about telephone calls but does not include the content of those calls. By analyzing telephony metadata based on

telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. International terrorist organizations and their agents use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, terrorist operatives make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the homeland. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting communications between known or suspected terrorists who are operating outside of the United States and who are communicating with others inside the United States, as well as communications between operatives within the United States. In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.

Pursuant to Section 215, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce business records that contain information about communications between telephone numbers, generally relating to telephone calls made between the United States and a foreign country and calls made entirely within the United States. The information collected includes, for example, the telephone numbers dialed, other session-identifying information, and the date, time, and duration of a call. The NSA, in turn, stores and analyzes this information under carefully controlled circumstances. The judicial orders authorizing the collection do not allow the Government to collect the *content* of any telephone call, or the names, addresses, or financial information of any party to a call. The Government also does not collect cell phone locational information pursuant to these orders.

The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism. Under the FISC orders authorizing the collection, authorized queries may only begin with an "identifier," such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a "seed." Specifically, under Court-approved rules applicable to the program, there must be a "reasonable, articulable suspicion" that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. When the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. The "reasonable, articulable suspicion" requirement protects against the indiscriminate querying of the collected data. Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

Information responsive to an authorized query could include, among other things, telephone numbers that have been in contact with the terrorist-associated number used to query the data, plus the dates, times, and durations of the calls. Under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as "hops"). The first "hop" refers to the set of numbers directly in contact with the seed

identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers. Following the trail in this fashion allows focused inquiries on numbers of interest, thus potentially revealing a contact at the second or third "hop" from the seed telephone number that connects to a different terrorist-associated telephone number already known to the analyst. Thus, the order allows the NSA to retrieve information as many as three "hops" from the initial identifier. Even so, under this process, only a tiny fraction of the bulk telephony metadata records stored at NSA are authorized to be seen by an NSA intelligence analyst, and only under carefully controlled circumstances.

Results of authorized queries are stored and are available only to those analysts trained in the restrictions on the handling and dissemination of the metadata. Query results can be further analyzed only for valid foreign intelligence purposes. Based on this analysis of the data, the NSA then provides leads to the FBI or others in the Intelligence Community. For U.S. persons, these leads are limited to counterterrorism investigations. Analysts must also apply the minimization and dissemination requirements and procedures specifically set out in the Court's orders before query results, in any form, are disseminated outside of the NSA. NSA's analysis of query results obtained from the bulk metadata has generated and continues to generate investigative leads for ongoing efforts by the FBI and other agencies to identify and track terrorist operatives, associates, and facilitators.

Thus, critically, although a large amount of metadata is consolidated and preserved by the Government, the vast majority of that information is never seen by any person. Only information responsive to the limited queries that are authorized for counterterrorism purposes is extracted and reviewed by analysts. Although the number of unique identifiers has varied substantially over the years, in 2012, fewer than 300 met the "reasonable, articulable suspicion" standard and were used as seeds to query the data after meeting the standard. Because the same seed identifier can be queried more than once over time, can generate multiple responsive records, and can be used to obtain contact numbers up to three "hops" from the seed identifier, the number of metadata records responsive to such queries is substantially larger than 300, but it is still a tiny fraction of the total volume of metadata records. It would be impossible to conduct these queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries.

If the FBI investigates a telephone number or other identifier tipped to it through this program, the FBI must rely on publicly available information, other available intelligence, or other legal processes in order to identify the subscribers of any of the numbers that are retrieved. For example, the FBI could submit a grand jury subpoena to a telephone company to obtain subscriber information for a telephone number. If, through further investigation, the FBI were able to develop probable cause to believe that a number in the United States was being used by an agent of a foreign terrorist organization, the FBI could apply to the FISC for an order under Title I of FISA to authorize interception of the contents of future communications to and from that telephone number.

The telephony metadata collection program is subject to an extensive regime of oversight and internal checks and is monitored by the Department of Justice (DOJ), the FISC, and

Congress, as well as the Intelligence Community. No more than twenty-two designated NSA officials can make a finding that there is "reasonable, articulable suspicion" that a seed identifier proposed for query is associated with a specific foreign terrorist organization, and NSA's Office of General Counsel must review and approve any such findings for numbers believed to be used by U.S. persons. In addition, before the NSA disseminates any information about a U.S. person outside the agency, a high-ranking NSA official must determine that the information identifying the U.S. person is in fact related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance. Among the program's additional safeguards and requirements are: (1) audits and reviews of various aspects of the program, including "reasonable, articulable suspicion" findings, by several entities within the Executive Branch, including NSA's legal and oversight offices and the Office of the Inspector General, as well as attorneys from DOJ's National Security Division and the Office of the Director of National Intelligence (ODNI); (2) controls on who can access and query the collected data; (3) requirements for training of analysts who receive the data generated by queries; and (4) a five-year limit on retention of raw collected data.

In addition to internal oversight, any compliance matters in this program that are identified by the NSA, DOJ, or ODNI are reported to the FISC. The FISC's orders to produce records under the program must be renewed every 90 days, and applications for renewals must report information about how the authority has been implemented under the prior authorization. Significant compliance incidents are also reported to the Intelligence and Judiciary Committees of both houses of Congress. Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered as a result of DOJ and ODNI reviews and internal NSA oversight. In accordance with the Court's rules, upon discovery, these violations were reported to the FISC, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. These problems generally involved human error or highly sophisticated technology issues related to NSA's compliance with particular aspects of the Court's orders. The FISC has on occasion been critical of the Executive Branch's compliance problems as well as the Government's court filings. However, the NSA and DOJ have corrected the problems identified to the Court, and the Court has continued to authorize the program with appropriate remedial measures.

II. THE TELEPHONY METADATA COLLECTION PROGRAM COMPLIES WITH SECTION 215

The collection of telephony metadata in bulk for counterterrorism purposes, subject to the restrictions identified above, complies with Section 215, as fourteen different judges of the FISC have concluded in issuing orders directing telecommunications service providers to produce the data to the Government. This conclusion does *not* mean that any and all types of business records—such as medical records or library or bookstore records—could be collected in bulk under this authority. In the context of communications metadata, in which connections between individual data points are important, and analysis of bulk metadata is the only practical means to find those otherwise invisible connections in an effort to identify terrorist operatives and networks, the collection of bulk data is relevant to FBI investigations of international terrorism.

This collection, moreover, occurs only in a context in which the Government's acquisition, use, and dissemination of the information are subject to strict judicial oversight and rigorous protections to prevent its misuse.

A. Statutory Requirements

Section 215 authorizes the FISC to issue an order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism," except that it prohibits an "investigation of a United States person" that is "conducted solely on the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § l861(a)(1). The Government's application for an order must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to [such] an authorized investigation (other than a threat assessment)" and that the investigation is being conducted under guidelines approved by the Attorney General. *Id.* § 1861(b)(2)(A) and (a)(2)(A). Because Section 215 does not authorize the FISC to issue an order for the collection of records in connection with FBI threat assessments,[1] to obtain records under Section 215 the investigation must be "predicated" (e.g., based on facts or circumstances indicative of terrorism, consistent with FBI guidelines approved by the Attorney General). Finally, Section 215 authorizes the collection of records only if they are of a type that could be obtained either "with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." *Id.* § 1861(c)(2)(D).[2] The telephony metadata collection program complies with each of these requirements.

1. *Authorized Investigation.* The telephony metadata records are sought for properly predicated FBI investigations into specific international terrorist organizations and suspected terrorists. The FBI conducts the investigations consistent with the *Attorney General's Guidelines for Domestic FBI Operations,* U.S. Dep't of Justice (2008), which direct the FBI "to protect the United States and its people from . . . threats to the national security" and to "further the foreign intelligence objectives of the United States," a mandate that extends beyond traditional criminal law enforcement. *See id.* at 12. The guidelines authorize a full investigation into an international terrorist organization if there is an "articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged . . . in . . . international terrorism or other threat to the national security," or may be planning or

---

[1] "Threat assessments" refer to investigative activity that does not require any particular factual predication (but does require an authorized purpose and cannot be based on the exercise of First Amendment protected activity or on race, ethnicity, national origin, or religion of the subject). *FBI Domestic Investigations and Operations Guide,* § 5.1 (2011).

[2] Indeed, Section 215 was enacted because the FBI lacked the ability, in national security investigations, to seek business records in a way similar to its ability to seek records using a grand jury subpoena in a criminal case or an administrative subpoena in civil investigations. *See, e.g.,* S. Rep. No. 109-85, at 20 (2005) ("[A] federal prosecutor need only sign and issue a grand jury subpoena to obtain similar documents in criminal investigations, yet national security investigations have no similar investigative tool.").

supporting such conduct. *See id.* at 23. FBI investigations into the international terrorist organizations identified to the Court readily meet that standard, and there have been numerous FBI investigations in the last several years to which the telephony metadata records are relevant. The guidelines provide that investigations of a terrorist organization "may include a general examination of the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; [and] the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives." *Id.* And in investigating international terrorism, the FBI is *required* to "fully utilize the authorities and the methods authorized" in the guidelines, which include "[a]ll lawful . . . methods," including the use of intelligence tools such as Section 215. *Id.* at 12 and 31.

2. *Tangible Things.* The telephony metadata records are among the types of materials that can be obtained under Section 215. The statute broadly provides for the production of "any tangible things (including books, records, papers, documents, and other items)." *See* 50 U.S.C. § 1861(a)(1). There is little question that in enacting Section 215 in 2001 and then amending it in 2006, Congress understood that among the things that the FBI would need to acquire to conduct terrorism investigations were documents and records stored in electronic form. Congress may have used the term "tangible things" to make clear that this authority covers the production of items as opposed to oral testimony, which is another type of subpoena beyond the scope of Section 215. Thus, as Congress has made clear in other statutes involving production of records, "tangible things" include electronically stored information. *See* 7 U.S.C. § 7733(a) ("The Secretary shall have the power to subpoena . . . the production of all evidence (including books, papers, documents, electronically stored information, and *other* tangible things that constitute or contain evidence).") (emphasis added); 7 U.S.C. § 8314 (a)(2)(A) (containing the same language).[3]

The non-exhaustive list of "tangible things" in Section 215, moreover, includes the terms "documents" and "records," both of which are commonly used in reference to information stored in electronic form. The telephony metadata information is an electronically stored "record" of, among other information, the date, time, and duration of a call between two telephone numbers. And in the analogous context of civil discovery, the term "documents" has for decades been interpreted to include electronically stored information. The Federal Rules of Civil Procedure were amended in 1970 to make that understanding of the term "documents" explicit, *see Nat'l. Union Elec. Corp. v. Matsushita Elec. Indus. Co., Ltd.,* 494 F. Supp. 1257, 1261-62 (E.D. Pa. 1980), and again in 2006 to expressly add the term "electronically stored information." *See* Fed. R. Civ. Pro. 34 (governing production of "documents, electronically stored information, and tangible things").[4] Moreover, a judge may grant an order for production of records under

---

[3] The word "tangible" can be used in some contexts to connote not only tactile objects like pieces of paper, but also any other things that are "capable of being perceived" by the senses. *See Merriam Webster Online Dictionary* (2013) (defining "tangible" as "capable of being perceived *especially by* the sense of touch") (emphasis added).

[4] The notes of the Advisory Committee on the 2006 amendments to Rule 34 explain that:

> Lawyers and judges interpreted the term "documents" to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all

Section 215 only if the records could "be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of *records or tangible things*," and grand jury subpoenas can be and frequently are used to seek electronically stored telephony metadata records such as those sought under Section 215 or other electronically stored records. *See* 50 U.S.C. § 1861(c)(2)(D) (emphasis added); 18 U.S.C. § 2703(b)(1)(B)(i). That further confirms that Section 215 applies to electronically stored information.[5]

3. *Relevance to an Authorized Investigation.* The telephony metadata program also satisfies the statutory requirement that there be "reasonable grounds to believe" that the records collected are "relevant to an authorized investigation . . . to obtain foreign intelligence information . . . or to protect against international terrorism or clandestine intelligence activities." *See* 50 U.S.C. § 1861(b)(2)(A). The text of Section 215, considered in light of the well-developed understanding of "relevance" in the context of civil discovery and criminal and administrative subpoenas, as well as the broader purposes of this statute, indicates that there are "reasonable grounds to believe" that the records at issue here are "relevant to an authorized investigation." Specifically, in the circumstance where the Government has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information—and that it is necessary to collect a large volume of data in order

---

> forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a 'document.' Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended *to confirm* that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change *clarifies* that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. *At the same time, a Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and 'documents*.'

Fed. R. Civ. Pro 34, Notes of Advisory Committee on 2006 Amendments (emphasis added).

[5] The legislative history of Section 215 also supports this reading of the provision to include electronic data. In its discussion of Section 215, the House Report accompanying the USA PATRIOT Reauthorization Act of 2006 notes that there were electronic records in a Florida public library that might have been used to help prevent the September 11, 2001, attacks had the FBI obtained them. *See* H.R. Rep. No. 109-174(I), at 17-18 (2005). Specifically, the report describes "records indicat[ing] that a person using [the hijacker] Alhazmi's account used the library's computer to review September 11th reservations that had been previously booked." *Id.* at 18. Congress used this example to illustrate the types of "tangible things" that Section 215 authorizes the FBI to obtain through a FISC order. Moreover, the House Report cites testimony in 2005 by the Attorney General before the House Committee on the Judiciary, where the Attorney General explained that Section 215 had been used "to obtain driver's license records, public accommodation records, apartment leasing records, credit card records, *and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen-register devices*." *Id.* (emphasis added). Telecommunications service providers store such subscriber information electronically. Accordingly, the House Report suggests that Congress understood that Section 215 had been used to capture electronically stored records held by telecommunications service providers and reauthorized Section 215 based on that understanding.

to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied.

Standing alone, "relevant" is a broad term that connotes anything "[b]earing upon, connected with, [or] pertinent to" a specified subject matter. 13 Oxford English Dictionary 561 (2d ed. 1989). The concept of relevance, however, has developed a particularized legal meaning in the context of the production of documents and other things in conjunction with official investigations and legal proceedings. Congress legislated against that legal background in enacting Section 215 and thus "presumably kn[e]w and adopt[ed] the cluster of ideas that were attached to [the] word in the body of learning from which it was taken." *See FAA v. Cooper*, 132 S. Ct. 1441, 1449 (2012) (internal citation and quotation marks omitted). Indeed, as discussed above, in identifying the sort of items that may be the subject of a Section 215 order, Congress expressly referred to items obtainable with "a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation" or "any other order issued by a court of the United States directing the production of records or tangible things," 50 U.S.C. § 1861(c)(2)(D), indicating that it was well aware of this legal context when it added the relevance requirement. That understanding is also reflected in the statute's legislative history. *See* 152 Cong. Rec. 2426 (2006) (statement of Sen. Kyl) ("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.").

It is well-settled in the context of other forms of legal process for the production of documents that a document is "relevant" to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter. In civil discovery, for example, the Supreme Court has construed the phrase "relevant to the subject matter involved in the pending action" "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." *Oppenheimer Fund, Inc. v. Sanders,* 437 U.S. 340, 351 (1978) (emphasis added); *see also Condit v. Dunne*, 225 F.R.D. 100, 105 (S.D.N.Y. 2004) ("Although not unlimited, relevance, for purposes of discovery, is an extremely broad concept."). A similar standard applies to grand jury subpoenas, which will be upheld unless "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." *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).[6] And the Supreme Court has explained that a statutory "relevance" limitation on administrative subpoenas, even for investigations into matters not involving national security threats, is "not especially constraining" and affords an agency "access to virtually any material that might cast light on the allegations" at issue in an investigation. *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984). *See also United*

[6] One court has noted that the Court's reference to "category of materials," rather than to specific documents, "contemplates that the district court will assess relevancy based on the broad types of material sought by the Government," not by "engaging in a document-by-document [or] line-by-line assessment of relevancy." *In re Grand Jury Proceedings,* 616 F.3d 1186, 1202 (10th Cir. 2010). The court explained 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 adopted in *R. Enterprises.*" *Id.* at 1205.

States v. Arthur Young & Co., 465 U.S. 805, 814 (1984) (stating that IRS's statutory power to subpoena any records that may be relevant to a particular tax inquiry allows IRS to obtain items "of even *potential* relevance to an ongoing investigation") (emphasis in original). Relevance in that context is not evaluated in a vacuum but rather through consideration of the nature, purpose, and scope of the investigation, *see, e.g., Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946), and courts generally defer to an agency's appraisal of what is relevant. *See, e.g., EEOC v. Randstad*, 685 F.3d 433, 451 (4th Cir. 2012).

In light of that basic understanding of relevance, courts have held that the relevance standard permits requests for the production of entire repositories of records, even when any particular record is unlikely to directly bear on the matter being investigated, because searching the entire repository is the only feasible means to locate the critical documents.[7] More generally, courts have concluded that the relevance standard permits discovery of large volumes of information in circumstances where the requester seeks to identify much smaller amounts of information within the data that directly bears on the matter.[8] Federal agencies exercise broad subpoena powers or other authorities to collect and analyze large data sets in order to identify information that directly pertains to the particular subject of an investigation.[9] Finally, in the analogous field of search warrants for data stored on computers, courts permit Government agents to copy entire computer hard drives and then later review the entire drive for the specific evidence described in the warrant. *See* Fed. R. Crim. P. 41(e)(2)(B) ("A warrant … may

---

[7] *See, e.g., Carrillo Huettel, LLP v. SEC*, 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011) (holding that there is reason to believe that law firm's trust account information for all of its clients is relevant to SEC investigation, where the Government asserted the trust account information "may reveal concealed connections between unidentified entities and persons and those identified in the investigation thus far . . . [and] the transfer of funds cannot effectively be traced without access to all the records."); *Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC,* 2007 WL 3492762 at *1 (N.D. Ga. Nov. 5, 2007) (compelling production of business's entire underwriting database, despite business's assertion that it contained a significant amount of irrelevant data); *see also Chen-Oster v. Goldman, Sachs & Co.,* 285 F.R.D. 294, 305 (S.D.N.Y. 2012) (noting that production of multiple databases could be ordered as a "data dump" if necessary for plaintiffs' statistical analysis of business's employment practices).

[8] *See, e.g., In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000) (holding that subpoena to doctor to produce 15,000 patient files was relevant to investigation of doctor for healthcare fraud); *In re Grand Jury Proceedings,* 827 F.2d 301, 305 (8th Cir. 1987) (upholding grand jury subpoenas for all wire money transfer records of business's primary wire service agent in the Kansas City area that exceeded $1000 for a one year period despite claim that "the subpoena may make available to the grand jury records involving hundreds of innocent people"); *In re Adelphia Comm. Corp.,* 338 B.R. 546, 549 and 553 (Bankr. S.D.N.Y. 2005) (permitting inspection of "approximately 20,000 large bankers boxes of business records," and holding that "[i]t is well-settled . . . that sheer volume alone is an insufficient reason to deny discovery of documents"); *Medtronic Sofamor Danek, Inc. v. Michelson,* 229 F.R.D. 550, 552 (W.D. Tenn. 2003) (concerning discovery request for "approximately 996 network backup tapes, containing, among other things, electronic mail, plus an estimated 300 gigabytes of other electronic data that is not in a backed-up format, all of which contains items potentially responsive to discovery requests").

[9] *See, e.g., F.T.C. v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992) (upholding broad subpoena for financial information in FTC investigation of unfair or deceptive trade practices because it "could facilitate the Commission's investigation . . . in different ways, not all of which may yet be apparent"); *see also Associated Container Transp. (Aus.) Ltd. v. United States*, 705 F.2d 53, 58 (2nd Cir. 1983) ("recognizing the broad investigatory powers granted to the Justice Department by the Antitrust Civil Process Act," which are broad in scope due to the "'less precise nature of investigations'") (quoting H.R. Rep. No. 94-1343, at 11 (1976)).

authorize the seizure of electronic storage media … [and] authorize[] a later review of the media or information consistent with the warrant.").[10] These longstanding practices in a variety of legal arenas demonstrate a broad understanding of the requirement of relevance developed in the context of investigatory information collection.

It is reasonable to conclude that Congress had that broad concept of relevance in mind when it incorporated this standard into Section 215. The statutory relevance standard in Section 215, therefore, should be interpreted to be at least as broad as the standard of relevance that has long governed ordinary civil discovery and criminal and administrative investigations, which allows the broad collection of records when necessary to identify the directly pertinent documents. To be sure, the cases that have been decided in these contexts do not involve collection of data on the scale at issue in the telephony metadata collection program, and the purpose for which information was sought in these cases was not as expansive in scope as a nationwide intelligence collection effort designed to identify terrorist threats. While these cases do *not* demonstrate that bulk collection of the type at issue here would routinely be permitted in civil discovery or a criminal or administrative investigation, they do show that the "relevance" standard affords considerable latitude, where necessary, and depending on the context, to collect a large volume of data in order to find the key bits of information contained within. Moreover, there are a number of textual and contextual indications that Congress intended Section 215 to embody an even more flexible standard that takes into account the uniquely important purposes of the statute, the factual environment in which national security investigations take place, and the special facets of the statutory scheme in which Section 215 is embedded.

First, Section 215's standard on its face is particularly broad, because the Government need only show that there are "reasonable grounds to believe" that the records sought are relevant to an authorized investigation. 50 U.S.C. § 1861(b)(2)(A). That phrase reflects Congress's understanding that Section 215 permits a particularly broad scope for production of records in connection with an authorized national security investigation.[11]

Second, unlike, for example, civil discovery rules, which limit discovery to those matters "relevant to the subject matter involved in the action," Fed. R. Civ. P. 26(b)(1), Section 215 requires only that the documents be relevant to an "authorized *investigation*." 50 U.S.C.

---

[10] *See, e.g., United States v. Hill,* 459 F.3d 966, 975 (9th Cir. 2006) (recognizing that "blanket seizure" of the defendant's entire computer system, followed by subsequent review, may be permissible if explanation as to why it is necessary is provided); *United States v. Upham,* 168 F.3d 532, 535 (1st Cir. 1999) (explaining that "the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images" and that "[a] sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application").

[11] Some Members of Congress opposed Section 215 because in their view it afforded too broad a standard for collection of information. *See, e.g.,* 152 Cong. Rec. 2422 (2006) (statement of Sen. Feingold) ("[T]he deal would allow subpoenas in instances when there are reasonable grounds for simply believing that information is relevant to a terrorism investigation. That is an extremely low bar."); 156 Cong. Rec. S2108-01 (2010) (statement of Sen. Wyden) ("'Relevant' is an incredibly broad standard. In fact, it could potentially permit the Government to collect the personal information of large numbers of law-abiding Americans who have no connection to terrorism whatsoever.")

§ 1861(b)(2)(A) (emphasis added). This includes not only information directly relevant to the authorized object of the investigation—*i.e.*, "foreign intelligence information" or "international terrorism or clandestine intelligence activities"—but also information relevant to the investigative process or methods employed in reasonable furtherance of such national security investigations. In the particular circumstance in which the collection of communications metadata in bulk is necessary to enable discovery of otherwise hidden connections between individuals suspected of engaging in terrorist activity, the metadata records are relevant to the FBI's "investigation[s]" to which those connections relate. Notably, Congress *specifically rejected* proposals to limit the relevance standard so that it would encompass only records pertaining to individuals suspected of terrorist activity.[12]

Third, unlike most civil or criminal discovery or administrative inquiries, these investigations often focus on *preventing* threats to national security from causing harm, not on the retrospective determination of liability or guilt for prior activities. The basic purpose of Section 215, after all, is to provide a tool for discovering and thwarting terrorist plots and other national security threats that may not be known to the Government at the outset. For that reason, Congress recognized that in collecting records potentially "relevant to an authorized investigation" under Section 215, the FBI would not be limited to records known with certainty, or even with a particular level of statistical probability, to contain information that directly bears on a terrorist plot or national security threat. Rather, for Section 215 to be effective in advancing its core objective, the FBI must have the authority to collect records that, when subjected to reasonable and proven investigatory techniques, can produce information that will help the Government to identify previously unknown operatives and thus to prevent terrorist attacks before they succeed.

Fourth, and relatedly, unlike ordinary criminal investigations, the sort of national security investigations with which Section 215 is concerned often have a remarkable breadth—spanning long periods of time, multiple geographic regions, and numerous individuals, whose identities are often unknown to the intelligence community at the outset. The investigative tools needed to combat those threats must be deployed on a correspondingly broad scale. In this context, it is not surprising that Congress enacted a statute with a standard that enables the FBI to seek certain

---

[12] *See* S. 2369, 109th Cong. § 3 (2006) (requiring Government to demonstrate relevance of records sought to agents of foreign powers, including terrorist organizations, or their activities or contacts); 152 Cong. Rec. S1598-03 (2006) (statement of Sen. Levin) ("The Senate bill required a showing that the records sought were not only relevant to an investigation but also either pertained to a foreign power or an agent of a foreign power, which term includes terrorist organizations, or were relevant to the activities of a suspected agent of a foreign power who is the subject of an authorized investigation or pertained to an individual in contact with or known to be a suspected agent. In other words, the order had to be linked to some suspected individual or foreign power. Those important protections are omitted in the bill before us."); 152 Cong. Rec. H581-02 (2006) (statement of Rep. Nadler) ("The conference report does not restore the section 505 previous standard of specific and articulable facts connecting the records sought to a suspected terrorist. It should."); 151 Cong. Rec. S14275-01 (2005) (statement of Sen. Dodd) ("Unfortunately, the conference report differs from the Senate version as it maintains the minimal standard of relevance without a requirement of fact connecting the records sought, or the individual, suspected of terrorist activity. Additionally, the conference report does not impose any limit on the breadth of the records that can be requested or how long these records can be kept by the Government.").

records in bulk where necessary to identify connections between individuals suspected to be involved in terrorism.

Fifth, Congress built into the statutory scheme protections not found in the other legal contexts to help ensure that even an appropriately broad construction of the "relevance" requirement will not lead to misuse of the authority. Section 215, unlike the rules governing civil discovery or grand jury subpoenas, always requires prior judicial approval of the Government's assertion that particular records meet the relevance requirement and the other legal prerequisites. Once the information is produced, the Government can retain and disseminate the information only in accordance with minimization procedures reported to and approved by the Court. *See* 50 U.S.C. § 1861(g). The entire process is subject to active congressional oversight. *See, e.g.*, *id.* § 1862. Although Congress certainly intended the Government to make a threshold showing of relevance before obtaining information under Section 215, these more robust protections regarding collection, retention, dissemination, and oversight provide additional mechanisms for promoting responsible use of the authority.

In light of these features of Section 215, and the broad understanding of "relevance," the telephony metadata collection program meets the Section 215 "relevance" standard. There clearly are "reasonable grounds to believe" that this category of data, when queried and analyzed by the NSA consistent with the Court-imposed standards, will produce information pertinent to FBI investigations of international terrorism, and it is equally clear that NSA's analytic tools require the collection and storage of a large volume of metadata in order to accomplish this objective. As noted above, NSA employs a multi-tiered process of analyzing the data in an effort to identify otherwise unknown connections between telephone numbers associated with known or suspected terrorists and other telephone numbers, and to analyze those connections in a way that can help identify terrorist operatives or networks. That process is not feasible unless NSA analysts have access to telephony metadata in bulk, because they cannot know which of the many phone numbers might be connected until they conduct the analysis. The results of the analysis ultimately can assist in discovering whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, including persons and activities inside the United States. If not collected and held by the NSA, telephony metadata may not continue to be available for the period of time (currently five years) deemed appropriate for national security purposes because telecommunications service providers are not typically required to retain it for this length of time. Unless the data is aggregated, it may not be feasible to identify chains of communications that cross different telecommunications networks. Although NSA is exploring whether certain functions could be performed by the telecommunications service providers, doing so may not be possible without significant additional investment and new statutes or regulations requiring providers to preserve and format the records and render necessary technical assistance.

The national security objectives advanced by the telephony metadata program would therefore be frustrated if the NSA were limited to collection of a narrower set of records. In particular, a more restrictive collection of telephony metadata would impede the ability to identify a chain of contacts between telephone numbers, including numbers served by different telecommunications service providers, significantly curtailing the usefulness of the tool. This is therefore not a case in which a broad collection of records provides only a marginal increase in

the amount of useful information generated by the program. Losing the ability to conduct focused queries on bulk metadata would significantly diminish the effectiveness of NSA's investigative tools. As discussed above, the broad meaning of the relevance standard that Congress incorporated into Section 215 encompasses, in this particular circumstance, collection of a repository of information without which the Government might not be able to identify specific information that bears directly on a counterterrorism investigation. For that reason, the telephony metadata records are "relevant" to an authorized investigation of international terrorism.

This conclusion does not mean that the scope of Section 215 is boundless and authorizes the FISC to order the production of every type of business record in bulk—including medical records or library or book sale records, for example. As noted above, the Supreme Court has explained that determining the appropriate scope of a subpoena for the production of records "cannot be reduced to formula; for relevancy and adequacy or excess in the breadth of [a] subpoena are matters variable in relation to the nature, purposes and scope of the inquiry." *Okla. Press Pub. Co. v. Walling,* 327 U.S. 186, 209 (1946). In other contexts, the FISC might not conclude that collection of records in bulk meets the "relevance" standard because of the nature of the records at issue and the extent to which collecting such records in large volumes is necessary in order to produce information pertinent to investigations of international terrorism. For example, the Government's ability to analyze telephony metadata, including through the techniques discussed above, to discover connections between individuals fundamentally distinguishes such data from medical records or library records. Although an identified suspect's medical history might be relevant to an investigation of that individual, searching an aggregate database of medical records—which do not interconnect to one another—would not typically enable the Government to identify otherwise unknown relationships among individuals and organizations and therefore to ascertain information about terrorist networks. Moreover, given the frequent use of the international telephone system by terrorist networks and organizations, analysis of telephony metadata in bulk is a potentially important means of identifying terrorist operatives, particularly those persons who may be plotting terrorist attacks within the United States. Although there could be individual contexts in which the Government has an interest in obtaining medical records or library records for counterterrorism purposes, these categories of data are not in general comparable to communications metadata as a means of identifying previously unknown terrorist operatives or networks. The potential need for communications metadata is both persistent and pervasive across numerous counterterrorism investigations in a way that is not applicable to many other types of data. Communications metadata therefore presents a context in which using sophisticated analytic tools can be important to many investigations of international terrorism, and the use of those tools in turn requires collection of a large volume of data to be effective.

Under the telephony metadata program, the statutory requirement for judicial authorization serves as a check to focus Government investigations only on that information most likely to facilitate an authorized investigation. Under the FISC's orders, the amount of metadata actually reviewed by the Government is narrow. As noted above, those orders require, among other things, that NSA analysts have reasonable, articulable suspicion that the seed identifiers, such as telephone numbers, they submit to query the data are associated with specific foreign terrorist organizations that have previously been identified to and approved by the Court.

The vast majority of the telephony metadata is never seen by any person because it is not responsive to the limited queries that are authorized. But the information that is generated in response to these limited queries could be especially significant in helping the Government identify and disrupt terrorist plots. Thus, while the relevance standard provides the Government with broad authority to collect data that is necessary to conduct authorized investigations, the FISC's orders require that the data will be substantively queried *only* for that authorized purpose. That is the balanced scheme that Congress adopted when it joined the broad relevance standard with the requirement for judicial approval set forth in Section 215.

Indeed, given the rigorous protections imposed by the FISC, even if the statutory standard were not "relevance" as the term has been used in analogous legal contexts, but rather the Fourth Amendment reasonableness standard that the Supreme Court has adopted for searches not predicated on individualized suspicion, the telephony metadata program would be lawful. (For the reasons discussed below, the Fourth Amendment's reasonableness requirement does not apply in this context because individuals have no reasonable expectation of privacy in the telephony metadata records collected from providers under the program, *see* pp. 19-21, *infra*, but for present purposes we assume contrary to the facts that such a reasonable expectation exists.) The Supreme Court has held that "where a Fourth Amendment intrusion serves special government needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or . . . individualized suspicion in the particular context." *Nat'l Treas. Employees Union v. Von Raab,* 489 U.S. 656, 665-66 (1989). As noted above, the telephony metadata collected under Section 215 does not include the private content of any person's telephone calls, or who places or answers the calls, but only technical data, such as information concerning the numbers dialed and the time and duration of the calls. Even if there were an individual privacy interest in such telephony metadata under the Fourth Amendment, it would be limited, and any infringement on that interest would be substantially mitigated by the judicially approved restrictions on accessing and disseminating the data. *See Board of Educ. of Indep. School Dist. No. 92 of Pottawatomie County v. Earls,* 536 U.S. 822, 833 (2002) (finding that restrictions on access to drug testing information lessened testing program's intrusion on privacy). On the other side of the scale, the interest of the Government—and the broader public—in discovering and tracking terrorist operatives and thwarting terrorist attacks is a national security concern of overwhelming importance. *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.") (internal quotation marks omitted); *see also In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) ("Here, the relevant governmental interest—the interest in national security—is of the highest order of magnitude."). Moreover, the telephony metadata collection program is, at the very least, "a reasonably effective means of addressing" the Government's national security needs in this context. *Earls*, 536 U.S. at 837. Thus, even if the appropriate standard for the telephony metadata collection program were not relevance, but rather a Fourth Amendment reasonableness analysis, the Government's interest is compelling and immediate, the intrusion on privacy interests is limited, and the collection is a reasonably effective means of detecting and monitoring terrorist operatives and thereby obtaining information important to FBI investigations.

4. *Prospective Orders.* Section 215 authorizes the FISC to issue orders to produce telephony metadata records prospectively. Nothing in the text of the statute suggests that FISC orders may relate only to records previously created. The fact that the requested information has not yet been created at the time of the application, and that its production is requested on an ongoing basis, does not affect the basic character of the information as "documents," "records," or other "tangible things" subject to production under the statute. Nor do the orders require the creation or preservation of documents that would otherwise not exist. Section 215 orders are not being used to compel a telecommunications service provider to retain information that the provider would otherwise discard, because the telephony metadata records are routinely maintained by the providers for at least eighteen months in the ordinary course of business pursuant to Federal Communications Commission regulations. *See* 47 C.F.R. § 42.6. In this context, the continued existence of the records and their continuing relevance to an international terrorism investigation will not change over the 90-day life of a FISC order.

Prospective production of records has been deemed appropriate in other analogous contexts. For example, courts have held that the Federal Rules of Civil Procedure give a court the "authority to order [the] respondent to produce materials created after the return date of the subpoena." *Chevron v. Salazar*, 275 F.R.D. 437, 449 (S.D.N.Y 2011); *see also United States v. I.B.M.*, 83 F.R.D. 92, 96 (S.D.N.Y. 1979). Other courts have held that, under the Stored Communications Act, because the statute does not "limit the ongoing disclosure of records to the Government as soon as they are created," the Government may seek prospective disclosure of records. *See, e.g., In re Application for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008) ("prospective . . . information sought by the Government . . . becomes a 'historical record' as soon as it is recorded by the provider."). Neither Section 215 nor any other part of the FISA statutory scheme prohibits the ongoing production of business records that are generated on a daily basis to the Government soon after they are created. Nor is there any legislative history indicating that Congress intended to prevent courts from issuing prospective orders under Section 215 in these circumstances.

This type of prospective order also provides efficient administration for all parties involved—the Court, the Government, and the provider. There is little doubt that the Government could seek a new order on a daily basis for the records created within the last 24 hours. But the creation and processing of such requests would impose entirely unnecessary burdens on both the Court and the Government—and no new information would be anticipated in such a short period of time to alter the basis of the Government's request or the facts upon which the Court has based its order. Providers would also be forced to review daily requests of differing docket numbers, rather than merely complying with one ongoing request, which would be more onerous on the providers and raise potential and unnecessary compliance issues. Importantly, the FISC orders do not allow the Government to receive this information in perpetuity: the 90-day renewal requires the Government to make continuing justifications for the business records on a routine basis. Therefore, the prospective orders merely ensure that the records can be sought in a reasonable manner for a reasonable period of time while avoiding unreasonable and burdensome paperwork.

B. Congressional Reauthorizations

The telephony metadata collection program satisfies the plain text and basic purposes of Section 215 (as well as the Constitution, *see infra* pp. 20-24) and is therefore lawful. But to the extent there is any question as to the program's compliance with the statute, it is significant that, after information concerning the telephony metadata collection program carried out under the authority of Section 215 was made available to Members of Congress, Congress twice reauthorized Section 215. When Congress reenacts a statute without change, it is presumed to have adopted the administrative or judicial interpretation of the statute if it is aware of the interpretation. *See Lorillard v. Pons*, 434 U.S. 575, 580 (1978). The FISC's conclusion that Section 215 authorized the collection of telephony metadata in bulk was classified and not publicly known. However, it is important to the legal analysis of the statute that the Congress was on notice of this program and the legal authority for it when the statute was reauthorized.

Although the proceedings before the FISC are classified, Congress has enacted legislation to ensure that its members are aware of significant interpretations of law by the FISC. FISA requires "the Attorney General [to] submit to the [Senate and House Intelligence and Judiciary Committees] . . . a summary of significant legal interpretations of this chapter involving matters before the [FISC or Foreign Intelligence Surveillance Court of Review (FISCR)], including interpretations presented in applications or pleadings filed with the [FISC or FISCR] by the Department of Justice and . . . copies of all decisions, orders, or opinions of the [FISC or FISCR] that include significant construction or interpretation of the provisions of this chapter." 50 U.S.C. § 1871(a). The Executive Branch not only complied with this requirement with respect to the telephony metadata collection program, it also worked to ensure that *all* Members of Congress had access to information about this program and the legal authority for it. Congress was thus on notice of the FISC's interpretation of Section 215, and with that notice, twice extended Section 215 without change.

In December 2009, DOJ worked with the Intelligence Community to provide a classified briefing paper to the House and Senate Intelligence Committees that could be made available to all Members of Congress regarding the telephony metadata collection program. A letter accompanying the briefing paper sent to the House Intelligence Committee specifically stated that "it is important that all Members of Congress have access to information about this program" and that "making this document available to all members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215." *See* Letter from Assistant Attorney General Ronald Weich to the Honorable Silvestre Reyes, Chairman, House Permanent Select Committee on Intelligence (Dec. 14, 2009). Both Intelligence Committees made this document available to all Members of Congress prior to the February 2010 reauthorization of Section 215. *See* Letter from Sen. Diane Feinstein and Sen. Christopher S. Bond to Colleagues (Feb. 23, 2010); Letter from Rep. Silvestre Reyes to Colleagues (Feb. 24, 2010); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden) ("[T]he Attorney General and the Director of National Intelligence have prepared a classified paper that contains details about how some of the Patriot Act's authorities have actually been used, and this paper is now available to all members of Congress, who can read it in the Intelligence Committee's secure office spaces. I would certainly encourage all of my colleagues to come down to the Intelligence

Committee and read it."). That briefing paper, which has since been released to the public in redacted form, explained that the Government and the FISC had interpreted Section 215 to authorize the collection of telephony metadata in bulk.[13]

Additionally, the classified use of this authority has been briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees, including in connection with reauthorization efforts. Several Members of Congress have publicly acknowledged that the Executive Branch extensively briefed these committees on the telephony metadata collection program and that, beyond what is required by law, the Executive Branch also made available to all Members of Congress information about this program and its operation under Section 215.[14] Moreover, in early 2007, the Department of Justice began providing all significant FISC pleadings and orders related to this program to the Senate and House Intelligence and Judiciary committees. By December 2008, all four committees had received the initial application and primary order authorizing the telephony metadata collection. Thereafter, all pleadings and orders reflecting significant legal developments regarding the program were produced to all four committees.

After receiving the classified briefing papers, which were expressly designed to inform Congress' deliberations on reauthorization of Section 215, Congress twice reauthorized this statutory provision, in 2010 and again in 2011. These circumstances provide further support to the FISC's interpretation of Section 215 as authorizing orders directing the production of telephony metadata records in bulk, as well as the Executive Branch's administrative construction of the statute to the same effect. *See Shell Oil Co.*, 466 U.S. at 69 ("Congress undoubtedly was aware of the manner in which the courts were construing the concept of 'relevance' and implicitly endorsed it by leaving intact the statutory definition of the

---

[13] An updated version of the briefing paper, also recently released in redacted form to the public, was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year. *See Letter from Assistant Attorney General Ronald Weich to the Honorable Dianne Feinstein and the Honorable Saxby Chambliss, Chairman and Vice Chairman, Senate Select Committee on Intelligence (Feb. 2, 2011); Letter from Assistant Attorney General Ronald Weich to the Honorable Mike Rogers and the Honorable C.A. Dutch Ruppersberger, Chairman and Ranking Minority Member, House Permanent Select Committee on Intelligence (Feb. 2, 2011).* The Senate Intelligence Committee made this updated paper available to all Senators later that month. *See Letter from Sen. Diane Feinstein and Sen. Saxby Chambliss to Colleagues* (Feb. 8, 2011).

[14] *See, e.g.*, Press Release of Senate Select Committee on Intelligence, *Feinstein, Chambliss Statement on NSA Phone Records Program* (June 6, 2013) ("The executive branch's use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each reauthorization of this law."); *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence*, 113 Cong. (2013) (statements of Rep. Rogers and Rep. Ruppersberger, Chair and Ranking Member, H. Permanent Select Comm. on Intelligence) (confirming extensive executive branch briefings for HPSCI on the telephony metadata collection program); Michael McAuliff & Sabrina Siddiqui, *Harry Reid: If Lawmakers Don't know about NSA Surveillance, It's Their Fault*, Huffington Post, June 11, 2013, *available at www.huffingtonpost.com/2013/06/11/harry-reid-nsa_n_3423393.html* (quoting Sen. Reid) ("For senators to complain that 'I didn't know this was happening,' we've had many, many meetings . . . that members have been invited to. . . . [T]hey've had every opportunity to be aware of these programs.")

Commission's investigative authority."); *Haig v. Agee*, 453 U.S. 280, 297-98 (1981) (finding that where Congress used language identical to that in an earlier statute and there was "no evidence of any intent to repudiate the longstanding administrative construction" of the earlier statute, the Court would "conclude that Congress . . . adopted the longstanding administrative construction" of the prior statute); *Atkins v. Parker*, 472 U.S. 115, 140 (1985) ("Congress was thus well aware of, and legislated on the basis of, the contemporaneous administrative practice . . . and must be presumed to have intended to maintain that practice absent some clear indication to the contrary.") (citing *Haig*, 453 U.S. 297-98).[15]

III. THE TELEPHONY METADATA COLLECTION PROGRAM IS CONSTITUTIONAL

The telephony metadata collection program also complies with the Constitution. Supreme Court precedent makes clear that participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the metadata records generated by their telephone calls and held by telecommunications service providers. Moreover, any arguable privacy intrusion arising from the collection of telephony metadata would be outweighed by the critical public interest in identifying connections between terrorist operatives and thwarting terrorist plots, rendering the program reasonable within the meaning of the Fourth Amendment. The program is also consistent with the First Amendment, particularly given that the database may be used only as an investigative tool in authorized investigations of international terrorism.

A. Fourth Amendment

A Section 215 order for the production of telephony metadata is not a "search" as to any individual because, as the Supreme Court has expressly held, participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the Government's collection of dialed telephone numbers from a telephone company did not constitute a search of the petitioner under the Fourth Amendment, because persons making phone calls lack a reasonable expectation of privacy in the numbers they call. *Id.* at 743-46.

---

[15] Moreover, in both 2009 and 2011, when the Senate Judiciary Committee was considering possible amendments to Section 215, it made clear that it had no intention of affecting the telephony metadata collection program that had been approved by the FISC. The Committee reports accompanying the USA PATRIOT Act Sunset Extension Acts of 2009 and 2011 explained that proposed changes to Section 215 were "not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities." S. Rep. No. 111-92, at 7 (2009); S. Rep. No. 112-13, at 10 (2011). Ultimately, Section 215 and other expiring provisions of the USA PATRIOT Act were extended to June 1, 2015 without change. *See* Patriot Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011). Likewise, Senators in the minority expressed the desire not to interfere with any activities carried out under Section 215 that had been approved by the FISC. *See* S. Rep. No. 111-92, at 24 (2009) (additional views from Senators Sessions, Hatch, Grassley, Kyl, Graham, Cornyn, and Coburn) ("It should be made clear that the changes to the business record and pen register statutes are intended to codify current practice under the relevance standard and are not intended to prohibit or restrict any activities approved by the FISA Court under existing authorities."). This record is further evidence of awareness and approval by Members of Congress of the FISC's decision that Section 215 authorizes the telephony metadata collection program.

Even if a subscriber subjectively intends to keep the numbers dialed secret, the Court held, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. The Court explained that someone who uses a phone has "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and therefore has "assumed the risk that the company would reveal to the police the numbers [] dialed." *Id.* at 744.

Although the telephony metadata obtained through Section 215 includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information, under the reasoning adopted by the Supreme Court in *Smith*, there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes. Under longstanding Supreme Court precedent, this conclusion holds even if there is an understanding that the third party will treat the information as confidential. *See, e.g., SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a *third* party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.") (emphasis added). Nothing in *United States v. Jones,* 132 S. Ct. 945 (2012), changed that understanding of the Fourth Amendment. The Court's decision in that case concerned only whether physically attaching a GPS tracking device to an automobile to collect information was a Fourth Amendment search or seizure. The telephony metadata collection program does not involve tracking locations from which telephone calls are made, and does not involve physical trespass. *See United States v. Anderson-Bagshaw,* 2012 WL 774964, at *2 (N.D. Ohio. Mar. 8, 2012) ("The [*Jones*] majority limited its analysis to the trespassory nature of the GPS installation, refusing to establish some point at which uninterrupted surveillance might become constitutionally problematic.").

The scope of the program does not alter the conclusion that the collection of telephony metadata under a Section 215 court order is consistent with the Fourth Amendment. Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search. Further, Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald v. United States*, 451 U.S. 204, 219 (1981); *accord, e.g.*, *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.'") (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Because the Fourth Amendment bestows "a personal right that must be invoked by an individual," a person "claim[ing] the protection of the Fourth Amendment . . . must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998). No Fourth Amendment-protected interest is generated by virtue of the fact that the telephony metadata records of many individuals are collected rather than those of a single individual. *Cf. In re Grand Jury Proceedings,* 827 F.2d at 305 (rejecting a money transfer business' argument that a subpoena for records of all transfers made from a certain office was

unreasonable and overbroad under the Fourth Amendment because it "may make available to the grand jury records involving hundreds of innocent people").

Even if one were to assume *arguendo* that the collection of telephony metadata involved a "search" within the meaning of the Fourth Amendment, for the reasons discussed above (*see* p. 15, *supra*), that search would satisfy the reasonableness standard that the Supreme Court has established in its cases authorizing the Government to conduct large-scale, but minimally intrusive, suspicionless searches. That standard requires a balancing of "the promotion of legitimate Governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (internal citation and quotation marks omitted). Such a balance of interests overwhelmingly favors the Government in this context. If any Fourth Amendment privacy interest were implicated by collection of telephony metadata, which does not include the content of any conversations, it would be minimal. Moreover, the intrusion on that interest would be substantially reduced by judicial orders providing that the data may be examined by an NSA analyst only when there is a "reasonable, articulable suspicion" that the seed identifier that is proposed for querying the data is associated with a specific foreign terrorist organization previously approved by the Court. Indeed, as the program has been conducted, only an exceedingly small fraction of the data collected has ever been seen—a fact that weighs heavily in the Fourth Amendment calculus. *See, e.g., id.* at 1979 (relying on safeguards that limited DNA analysis to identification information alone, without revealing any private information, as reducing any intrusion into privacy); *Vernonia School District 47J v. Acton,* 515 U.S. 646, 658 (1995) (finding it significant that urine testing of student athletes looked only for certain drugs, not for any medical conditions, as reducing any intrusion on privacy).

On the other side of the balance, there is an exceptionally strong public interest in the prevention of terrorist attacks, and telephony metadata analysis can be an important part of achieving that objective. This interest does not merely entail "ordinary crime-solving," *King*, 133 S. Ct. at 1982 (Scalia, J., dissenting), but rather the forward-looking prevention of the loss of life, including potentially on a catastrophic scale. Given that exceedingly important objective, and the minimal, if any, Fourth Amendment intrusion that the program entails, the program would be constitutional even if the Fourth Amendment's reasonableness standard applied.

B. First Amendment

The telephony metadata collection is also consistent with the First Amendment. It merits emphasis again in this context that the program does not collect the content of any communications and that the data may be queried only when the Government has a reasonable, articulable suspicion that a particular number is associated with a specific foreign terrorist organization. Section 215, moreover, expressly prohibits the collection of records for an investigation that is being conducted solely on the basis of protected First Amendment activity, if the investigation is of a U.S. person. The FBI is also prohibited under applicable Attorney General guidelines from predicating an investigation solely on the basis of activity protected by the First Amendment. The Court-imposed rules that restrict the Government's queries to those based on terrorist-associated seed identifiers and preclude indiscriminate use of the telephony

metadata substantially mitigate any First Amendment concerns arising from the breadth of the collection.

In any event, otherwise lawful investigative activities conducted in good faith—that is, not for the purpose of deterring or penalizing activity protected by the First Amendment—do not violate the First Amendment. *See, e.g., Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1051 (D.C. Cir. 1978) (First Amendment protects activities "*subject to* the general and incidental burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves" directed at First Amendment conduct) (emphasis added); *United States v. Aguilar,* 883 F.2d 662, 705 (9th Cir. 1989) ("use of undercover informants to infiltrate an organization engag[ed] in protected first amendment activities" must be part of an investigation "conducted in good faith; i.e., not for the purpose of abridging first amendment freedoms"). The Government's collection of telephony metadata in support of investigative efforts against specific foreign terrorist organizations are not aimed at curtailing any First Amendment activities, whether free speech or associational activities. Rather, the collection is in furtherance of the compelling national interest in identifying and tracking terrorist operatives and ultimately in thwarting terrorist attacks, particularly against the United States. It therefore satisfies any "good faith" requirement for purposes of the First Amendment. *See Reporters Comm.*, 593 F.2d at 1052 ("[T]he Government's good faith inspection of defendant telephone companies' toll call records does not infringe on plaintiffs' First Amendment rights, because that Amendment guarantees no freedom from such investigation.")

Nor does the Government's collection and targeted analysis of metadata violate the First Amendment because of an asserted "chilling effect" on First Amendment-protected speech or association. The Supreme Court has held that an otherwise constitutionally reasonable search of international mail, though not based on probable cause or a warrant, does not impermissibly chill the exercise of First Amendment rights, at least where regulations preclude the Government from reading the content of any correspondence without a warrant. *See United States v. Ramsey*, 431 U.S. 606, 623-24 (1977) (noting that because envelopes are opened at the border only when customs officers have reason to suspect they contain something other than correspondence, and reading of correspondence is forbidden absent a warrant, any "chill" that might exist is both minimal and subjective and there is no infringement of First Amendment rights). Similarly, the bulk telephony metadata is queried only where there is a reasonable, articulable suspicion that the identifier used to query the data is associated with a particular foreign terrorist organization, and the program does not involve the collection of any content, let alone the review of such content.

The Executive Branch and the FISC have enacted strict oversight standards to guard against any potential for misuse of the data, and mandatory reporting to the FISC and Congress are designed to make certain that, when significant compliance problems are identified, they are promptly addressed with the active engagement of all three branches of Government. This system of checks and balances guarantees that the telephony metadata is not used to infringe First Amendment protected rights while also ensuring that it remains available to the Government to use for one of its most important responsibilities—protecting its people from international terrorism.

Anderson, Trisha (ODAG)

From: Anderson, Trisha (ODAG)
Sent: Tuesday, October 29, 2013 11:43 AM
To: Cole, James (ODAG)
Cc: Goldberg, Stuart (ODAG); O'Neil, David (ODAG (b)(6) per NSD (NSD)
Subject: RE: Materials for hearing tomorrow
Attachments: usa-freedom-act-two-pager-final.pdf

(b)(6) per NSD

Here is a press release announcing the introduction of Sensenbrenner's bill, now also co-sponsored by Leahy and others. Their own summary of the bill is attached; it appears largely similar to the earlier version of the bill summarized in your binder.

Leahy & Sensenbrenner Join To Introduce USA FREEDOM Act

Legislation Ends Dragnet Collection Of Phone Data & Adds Meaningful Oversight Of Surveillance Programs

WASHINGTON (Tuesday, October 29, 2013) -- Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) and Congressman Jim Sensenbrenner (R-Wisc.), chairman of the Crime and Terrorism Subcommittee in the House, introduced on Tuesday legislation that seeks to restore Americans' privacy rights by ending the government's dragnet collection of phone records and requiring greater oversight, transparency, and accountability with respect to domestic surveillance authorities.

"The government surveillance programs conducted under the Foreign Surveillance Intelligence Act are far broader than the American people previously understood. It is time for serious and meaningful reforms so we can restore confidence in our intelligence community," Leahy said. "Modest transparency and oversight provisions are not enough. We need real reform, which is why I join today with Congressman Sensenbrenner, and bipartisan coalitions in both the Senate and House, to introduce the USA FREEDOM Act."

"Following 9/11, the USA PATRIOT Act passed the judiciary committees with overwhelming bipartisan support. The bill has helped keep Americans safe by ensuring information is shared among those responsible for defending our country and by enhancing the tools the intelligence community needs to identify and track terrorists," Sensenbrenner said. "But somewhere along the way, the balance between security and privacy was lost. It's now time for the judiciary committees to again come together in a bipartisan fashion to ensure the law is properly interpreted, past abuses are not repeated and American liberties are protected. Washington must regain Americans' trust in their government. The USA FREEDOM Act is an essential first step. I would like to thank Congressmen Conyers and Amash, Congresswoman Lofgren, Chairman Issa and others for working with us to draft this important legislation and encourage all my colleagues to support it."

The USA FREEDOM Act would end the dragnet collection of Americans' phone records under Section 215 of the USA PATRIOT Act and ensure that other authorities cannot be used to justify similar dragnet collection. The bill also provides more safeguards for warrantless surveillance under the FISA Amendments Act.

The bill includes other significant privacy and oversight provisions, provides for the creation of a Special Advocate to focus on the protection of privacy rights and civil liberties before the FISA Court, and requires more detailed public reporting about the numbers and types of FISA orders that are issued.

The bill has 16 cosponsors in the Senate including Senators Mike Lee (R-Utah), Dick Durbin (D-Ill.), Dean Heller (R-Nev.), Richard Blumenthal (D-Conn.), Lisa Murkowski (R-Alaska), Mazie Hirono (D-Hawaii), Tom Udall (D-N.M.), Mark Begich (D-Alaska), Tammy Baldwin (D-Wisc.), Martin Heinrich (D-N.M.), Ed Markey (D-Mass.), Mark Udall (D-Colo.), Elizabeth Warren (D-Mass.), Jeff Merkley (D-Ore.), Jon Tester (D-Mont.), and Joe Schatz (D-Hawaii). The measure also has more than 70 bipartisan cosponsors in the House and enjoys the diverse support of groups ranging from the National Rifle Association to the American Civil Liberties Union. A list of supporters can be found here.

Leahy and Sensenbrenner's joint op-ed on the USA FREEDOM Act, which Tuesday appeared in *Politico*, can be viewed here. An outline of the legislation can be found here, and text of legislation can be found online.

# # # # #

From: Anderson, Trisha (ODAG)
Sent: Monday, October 28, 2013 8:00 PM
To: Cole, James (ODAG)
Cc: Goldberg, Stuart (ODAG); O'Neil, David (ODAG) (b)(6) per NSD (NSD)
Subject: RE: Materials for hearing tomorrow

Attached is a shortened version of your remarks that you might consider using. Given the timing, I have not yet vetted these with NSD or OLA but will do so tonight.

<< File: 102913 HPSCI Opening Remarks (short version).docx >>

From: Anderson, Trisha (ODAG)
Sent: Monday, October 28, 2013 7:32 PM
To: Cole, James (ODAG)
Cc: Goldberg, Stuart (ODAG); O'Neil, David (ODAG) (b)(6) per NSD (NSD)
Subject: Materials for hearing tomorrow

(b)(6) per NSD – Attached are three documents that are relevant to tomorrow's hearing:

1) Summaries of the HPSCI bills (majority, minority, and two amendments);
2) A summary of Sensenbrenner's bill, which parallels Wyden's bill and could be the subject of questions tomorrow (b) (5) [redacted];
3) DNI's statement associated with today's FOIA release of additional 215-related documents, which includes a list of the documents released – there wasn't really any new news here; and

The talking points from your last hearing generally still cover the waterfront of legislative proposals that could be the subject of the hearing, with the exception of th (b) (5) [redacted], which presumably will be handled by the other two witnesses. Unfortunately the talking points are sti (b) (5) [redacted]

Finally, OLA has just offered a revised take on your opening remarks – namely, that you could give very abbreviated remarks, just a paragraph or two, or no remarks at all. I'm going to take a stab at a 2-3 paragraph version that you could use tomorrow if it seems the more appropriate thing to do. I'll send that version along shortly.

Hard copies of these materials – as well as your remarks and the talking points I mentioned – will be included in a binder that I'll send with the detail coming to pick you up at airport tomorrow.

Trisha

<< File: HPSCI Bill Summaries_10_28_13.docx >> << File: USA FREEDOM Act Summary_10_28_13.docx >>

<< File: DNI Statement.pdf >>

Kellner, Kenneth E. (OLA)

From: Kellner, Kenneth E. (OLA)
Sent: Friday, December 6, 2013 12:15 PM
To: Kadzik, Peter J (OLA); Agrast, Mark D. (OLA); Burton, Faith (OLA); Ruppert, Mary (OLA (b)(6) per NSD (NSD); Singh, Anita (NSD (b)(6) per NSD (NSD); Wiegmann, Brad (NSD); Hardee, Christopher (NSD (b)(6) per NSD (NSD); Werner, Sharon (OAG); Price, Allison W (OPA); Richardson, Margaret (OAG); Colborn, Paul P (OLC); Cheung, Denise (OAG); O'Neil, David (ODAG); Walsh, James (ODAG); Krass, Caroline D. (OLC); Siger, Steven B. (OLP); Tyrangiel, Elana (OLP)
Subject: Material for Carlin Prep
Attachments: NSD Briefing Book Issue Papers 12 05 13.zip; NSD Briefing Book - Index of Issues FINAL.docx

These may have dropped off when the invite was revised.

Ruemmler, Kathryn H.

From:	Ruemmler, Kathryn H.
Sent:	Monday, January 6, 2014 10:12 AM
To:	Richardson, Margaret (OAG)
Subject:	FW: PCLOB Draft Report Sections
Attachments:	Statutory Analysis 1-3-14.pdf; Balancing Section 1-3-14.pdf; FISC Section 1-3-14.pdf

Very close hold. Please keep to a very limited distribution.

And, happy new year!

From: Maltby, Jeremy
Sent: Friday, January 03, 2014 5:13 PM
To: Ruemmler, Kathryn H.; Monaco, Lisa; Heinzelman, Kate; Canegallo, Kristie A.
Cc: McCombs, Claire
Subject: Fw: PCLOB Draft Report Sections

I just received this from David Medine.

Best,

Jeremy

From: David Medine [(b) (6) [redacted]]
Sent: Friday, January 03, 2014 05:09 PM
To: Maltby, Jeremy
Subject: PCLOB Draft Report Sections

Jeremy,

Attached please find three draft sections from the Privacy and Civil Liberties Oversight Board's forthcoming report on the Section 215 Program and the operations of the Foreign Intelligence Surveillance Court. I request that neither the contents nor the substance of these documents be publicly released as they have not yet been finalized by the Board and will not be issued as part of a fuller report for several weeks. However, given our statutory role of advising the Executive Branch, we felt it important to provide these drafts at this time. Individual Board members will not be submitting separate statements but will express their views as part of the discussion next week.

The Board looks forward to meeting with the President and senior staff on Wednesday, January 8, at 10:45 pm, to discuss the 215 Program, FISC reform, and related matters. Please let me know if you need clearance information for Board members or have any questions regarding the attached materials.

Thanks.

David

David Medine
Chairman

Privacy and Civil Liberties Oversight Board

(b) (6) [redacted]

(b) (6) [redacted]

Cheung, Denise (OAG)

From: Cheung, Denise (OAG)
Sent: Tuesday, January 7, 2014 3:55 PM
To: Richardson, Margaret (OAG)
Subject: White paper
Attachments: Section215.pdf

I'm putting this in the AG's binder.

Krass, Caroline D. (OLC)

From:	Krass, Caroline D. (OLC)
Sent:	Wednesday, January 8, 2014 7:45 AM
To:	Walsh, James (ODAG)
Cc:	O'Neil, David (ODAG); Thompson, Karl (OAG)
Subject:	Krass.HearingQFRs.ForWHReview.docx
Attachments:	ATT00536.docx

Jim - please find attached the current version of my QFRs, which are in the final stages of WH review and are hopefully going over to the Committee later today. OLC has cleared. Thanks - Caroline

QUESTIONS FOR THE RECORD
CAROLINE D. KRASS

Covert Action v. Traditional Military Activities

In an interview conducted shortly after the raid that killed Osama bin Laden, then-CIA Director Leon Panetta acknowledged that the operation was a CIA "covert operation," yet it was carried out by DOD personnel using DOD helicopters and other equipment and, because it was acknowledged, it was not "covert." By contrast, until recently, DOD's use of unmanned aerial vehicles to conduct targeted strikes outside of the "hot" battlefields of Afghanistan and Iraq was a secret.

When asked about the difference between "covert actions" conducted by CIA and clandestine military activities conducted by DOD in the prehearing questions provided by this Committee you wrote, "*the President selects which element is best suited for the particular mission based on his assessment of how best to further the national interest*." Historically speaking, however, Congress sought to impose a higher standard of oversight on "covert action," at least in part, because of the unique foreign policy implications of unacknowledged paramilitary operations.

- ***Has the distinction between covert action and clandestine military activities become a legal technicality left entirely to the discretion of the President?***

ANSWER (b) (5) [redacted]

(b) (5)

- ***What types of paramilitary operations, if any, would be lawful only if carried out as a "covert action" pursuant to a Presidential finding?***

ANSWER (b) (5) [redacted]

Covert Action and the UN Charter and Geneva Conventions

In your answers to the Committee's pre-hearing questions about the UN Charter and the Geneva Conventions, you wrote, "*As a general matter, and including with respect to the use of force, the United States respects international law and complies with it to the extent possible in the execution of covert action activities*."

You also wrote that the U.N. Charter and the Geneva Conventions are NOT self-executing treaties, and therefore they are NOT legally binding upon actions carried out by the U.S. government, including covert actions.

- ***If, as you wrote in your answers to the Committee's pre-hearing questions, the U.S. respects international law and complies with it to the extent possible in the execution of covert action activities, how does the U.S. decide when to abide by international law and when it does not apply?***

ANSWER: (b) (5) [redacted]

(b) (5) [redacted]

- ***Should there be, and is there, special consideration when debating and approving a covert action, if that action would violate non-self-executing treaties or customary international law?***

ANSWER (b) (5) [redacted]

QUESTIONS FROM SENATOR WYDEN

1) On March 18, 2011, the Justice Department released a redacted version of a May 6, 2004, Office of Legal Counsel (OLC) opinion written by Assistant Attorney General Jack Goldsmith in response to a Freedom of Information Act action. As described in the public listing on the Justice Department's online FOIA reading room, this opinion was a "Memorandum Regarding Review of the Legality of the [President's Surveillance] Program."

   - Did any of the redacted portions of the May 2004 OLC opinion address bulk telephony metadata collection?

     ANSWER: (b) (5) [redacted]

   - If so, did the OLC rely at that time on a statutory basis other than the Foreign Intelligence Surveillance Act for the authority to conduct bulk telephony metadata collection? If so, please describe this statutory basis.

     ANSWER (b) (5) [redacted]

   - Has the OLC taken any action to withdraw this opinion?

     ANSWER (b) (5) [redacted]

- In light of the recent declassification of information regarding various domestic surveillance programs, do you agree that the redactions of the May 2004 opinion should be reviewed, and that an updated version should be publicly released?

ANSWER (b) (5) [redacted]

QUESTIONS FROM SENATOR UDALL

1) Other than the AUMF, are you aware of any existing authorities—legal, policy, or other authorities—that allow the President to use "all necessary and appropriate force" against "those nations, organizations, or persons" determined to plan authorize, commit or aide terrorist attacks against the United States?

ANSWER: (b) (5) [redacted]

2) Are you aware of any existing authorities—legal, policy, or other authorities—that allow the President to use "all necessary and appropriate force" against groups or individuals that haven't been designated "associated forces," e.g., affiliates or those who adhere to the beliefs of any terrorist organization that pose a significant threat to U.S. interests?

ANSWER (b) (5) [redacted]

(b) (5)

3) Who determines whether such "nations, organizations or persons" are designated "associated forces"? Into which nations may the President or other authority send military forces to use "all necessary and appropriate force" against "those nations, organizations, or persons" determined to plan authorize, commit or aid terrorist attacks against the United States?

ANSWER: (b) (5)

(b) (5)

4) What is the process for identifying "associated forces"? Is this process in writing? What is the notification and approval process prior to action being taken against those "nations, organizations, or persons"?

ANSWER (b) (5)

(b) (5) [redacted]

5) Are operations against these forces dependent upon notification to the President before they are conducted under AUMF or any other authorities?

ANSWER (b) (5) [redacted]

6) Article II of the U.S. Constitution states that President shall "shall take Care that the Laws be faithfully executed." Article VI of the U.S. Constitution, known as the "Supremacy Clause," states that "this Constitution, and the Laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land."

- If you learned of a covert action that, in your opinion, violated the Convention Against Torture or the Geneva Conventions, but did not necessarily violate a particular statute such as the Anti-Torture Act or the War Crimes Act, would you advise the Director of Central Intelligence that the action was unlawful?

ANSWER: (b) (5) [redacted]

(b) (5) [redacted]

(b) (5) [redacted]

- If the Director of Central Intelligence decided to proceed with such an action against your advice, would you inform this committee?

ANSWER (b) (5) [redacted]

7) How do you see the role of the General Counsel's office, if any, in determining whether information has been properly classified?

ANSWER: (b) (5) [redacted]

8) In 2007, after the passage of the 2006 Military Commissions Act and the 2005 Detainee Treatment Act and the Supreme Court's decision in *Hamdan v. Rumsfeld*, the Office of Legal Counsel concluded that a number of "enhanced interrogation" techniques remained lawful. The harshest of these was "sleep deprivation," carried out by shackling naked, diapered detainees to the ceiling for up to 96 consecutive hours. As you noted during your testimony in 2009, President Obama forbade the CIA from using these techniques, or any interrogation technique outlined in the Army Field Manual—but that prohibition is an Executive Order, which a future President could rescind. If President Obama's Executive Orders on CIA interrogation and detention were overturned, what binding legal authorities would prevent the CIA from engaging in the techniques authorized by the 2007 OLC memos?

ANSWER (b) (5) [redacted]

(b) (5) [redacted].

QUESTIONS FROM SENATOR HEINRICH

1) What is your legal opinion on the participation of CIA officers in the interrogations of detainees in liaison custody in which harsh or extreme interrogation techniques are used? In your opinion, is it legal for CIA officers to continue their participation in these interrogations when they witness, know, or otherwise suspect that a detainee has been tortured by a liaison service?

ANSWER: (b) (5) [redacted]

- In such a circumstance, is there any requirement—legal or policy—that the CIA officer involved report these activities either to the CIA Office of Inspector General, or to anybody?

ANSWER: (b) (5) [redacted]

2) How do you see the role of the General Counsel's office, if any, in determining whether information has been be properly classified?

(b) (5) [redacted]

QUESTION FROM SENATOR LEVIN

1) At your confirmation hearing, you stated that, if confirmed, you would ensure that the Committee had access to information "as appropriate." Please identify any types of documents that you believe is appropriate for the Intelligence Community to withhold from the committee.

ANSWER: (b) (5) [redacted]

Werner, Sharon (OAG)

From:	Werner, Sharon (OAG)
Sent:	Thursday, January 16, 2014 3:23 PM
To:	Gaston, Molly (OLA)
Subject:	FW: AG SJC briefing papers
Attachments:	NSD - Boston Marathon Bombings 1-9.dc.docx; NSD - Targeted Killings 1-10 (odag).dc.docx; NSD Fact Sheet Section 215 Authority.doc

Here are some more papers.

From: Cheung, Denise (OAG)
Sent: Thursday, January 16, 2014 2:25 PM
To: Werner, Sharon (OAG); Moran, Molly (OAG); Phillips, Channing D. (OAG); Thompson, Karl (OAG); Mosier, Jenny (OAG)
Cc: Richardson, Margaret (OAG)
Subject: RE: AG SJC briefing papers

I've reviewed all of the NSD items below. Karl has already submitted his proposed changes/questions regarding FISA Derived/Case Review. The FISA Reform Generally piece, as noted, will have to be revised once we have a final copy of the POTUS speech. Below are the my comments/proposed changes on some of these.

NSD	AUMF	N/A	Jim Walsh
NSD	Benghazi	N/A	Jim Walsh
NSD	Boston Marathon Bombings	N/A	Jim Walsh
NSD	Civilian Trials of Terror Suspects	N/A	Jim Walsh
NSD	FISA Derived/Case Review	N/A	Jim Walsh
NSD	FISA Reform Generally	N/A	Jim Walsh
NSD	Section 215 Litigation	N/A	Jim Walsh
NSD	Snowden Amnesty	N/A	Jim Walsh
NSD	Targeted Killings	Elizabeth Taylor	Jim Walsh

From: Werner, Sharon (OAG)
Sent: Tuesday, January 14, 2014 7:07 PM
To: Cheung, Denise (OAG); Moran, Molly (OAG); Phillips, Channing D. (OAG); Thompson, Karl (OAG); Mosier, Jenny (OAG)
Cc: Richardson, Margaret (OAG)
Subject: Fw: AG SJC briefing papers

As promised, here is a big chunk of the briefing papers. I'll send along the stragglers to individuals as they come in. Let me know if you have questions. Thanks.

From: Columbus, Eric (ODAG)
Sent: Tuesday, January 14, 2014 06:21 PM Eastern Standard Time
To: Werner, Sharon (OAG)

Cc: Burrows, Charlotte (ODAG); Martinez, Brian (OAAG)
Subject: AG SJC briefing papers

Sharon,

Attached are 53 of the 75 papers that OLA commissioned. I've also attached a chart that lists each paper along with the drafting component and the ODAG/OASG reviewers. The 18 papers highlighted in blue are still being reviewed by ODAG/OASG (in some cases pending info from the drafting component). The 4 papers highlighted in yellow have yet to be drafted (candor compels me to note that 2 of those 4 are to be drafted by ODAG). Would you like me to send you the remaining 22 as they come in, or some other way? I expect a few more will come in tonight.

I've left in track-changes if they arrived that way, just in case it's useful to see the original text, and I've left in comments where possibly helpful to the OAG reviewer.

Eric

<<AG SJC Hearing ODAG+OASG Reviewers.docx>> <<ATF - Gun Violence - Assault Weapons 1-9.docx>> <<ATF - Gun Violence - Declining Federal Prosecutions 1-9 - OASG edits.docx>> <<ATF - Gun Violence - Firearms Trafficking 1-9 - OASG edits.docx>> <<ATF - Gun Violence - Undetectable Firearms 1-9.docx>> <<ATF - Regulation for Background Checks 1-9.docx>> <<ATF - Storefronts 11414 clean.docx>> <<ATR - American Airlines-USAir Merger 1-9_OASG edits.doc>> <<ATR - Antitrust Enforcement 1-9.docx>> <<ATR - E-Books Settlement 1-9.doc>> <<ATR - FCC - DOJ Spectrum Comments 1-9.doc>> <<ATR - Telecom Mergers 1-9.docx>> <<CIV - Affordable Care Act Fraud 1-13_OASG Edits.docx>> <<CIV - False Claims Act 1-10.docx>> <<CIV - Health Care Fraud 1-10.docx>> <<CRM - Cybersecurity 1-9.docx>> <<CRM - Financial and Mortgage Fraud 1-10.docx>> <<CRM - IP Paper 1-9.docx>> <<CRM - Media Investigations and Media Shield 1-9 KSR Edits.docx>> <<CRM - Sentencing 1-9.docx>> <<CRT - NYPD Muslim Surveillance with OASG edits.docx>> <<CRT - Voting Rights - Texas and North Carolina 1-10 (2) with OASG and ODAG edits.docx>> <<CRT - Voting Rights - UOCAVA 1-10 (2) with OASG edits.ODAG cleared.docx>> <<DEA - Designer Drugs 1-10.docx>> <<DEA - Drug Disposal Regulations 1-9.docx>> <<DEA - Honduras 1-10.docx>> <<DEA - SOD Programs 1-10.docx>> <<ENRD - Native Hawaiians 1-9 with OASG edits.docx>> <<ENRD - Wildlife Trafficking 1-9.docx>> <<EOIR - Detainees with Mental Disorders 1-9.odag cleared oasg edits.docx>> <<EOIR - Immigration Reform 1-9 oasg and odag cleared.docx>> <<JMD - DOJ Aircraft.docx>> <<JMD - Sequestration.docx>> <<JMD - Thomson Prison 1-10.docx>> <<NSD - AUMF 1-9 (odag).docx>> <<NSD - Boston Marathon Bombings 1-9.docx>> <<NSD - FISA Derived Information 1-10.docx>> <<NSD - FISA reform 1-10 (odag).docx>> <<NSD - Section 215 litigation 1-10 (odag).docx>> <<NSD - Snowden Amnesty 1-9 (odag)(2).docx>> <<NSD - Targeted Killings 1-10 (odag).docx>> <<OASG - Farmer Discrimination Settlements 1-10 - OASG and ODAG edits.docx>> <<OASG - JP Morgan Settlement 1-10.docx>> <<ODAG - Domestic radicalization 1-10.docx>> <<ODAG - NIST Forensics 1-10.docx>> <<OIP - FOIA 1-13.docx>> <<OJP - PREA 1-10 (ODAG edits).docx>> <<OLP - Electronic Surveillance - ECPA Amendments 1-10 OASG.docx>> <<OLP - Electronic Surveillance -- Location Information 1-9.docx>> <<OLP - Unmanned Aerial Systems 1-9 (odag).docx>> <<OLP - Use of Race Guidance 1-9.odag and oasg edits.qus for OLP.docx>> <<TAX - Offshore Banking 1-10 (2) bms rev 011414.DOC>> <<TAX - SIRF summary 1-10.docx>> <<TAX - Swiss Bank Program 1-10 (2) bms rev 011414.docx>>

Krass, Caroline D. (OLC)

From: Krass, Caroline D. (OLC)
Sent: Monday, January 27, 2014 3:55 PM
To: Goldberg, Stuart (ODAG); O'Neil, David (ODAG)
Cc: Walsh, James (ODAG); Koffsky, Daniel L (OLC); Singdahlsen, Jeffrey (OLC); Pulham, Thomas (OLC)
Subject: DEA Program
Attachments: Draft DEA Program Questions.January 27.docx

Stuart/Dave –

As you requested, please find attached a list of questions that we have put together regarding the DEA program. We left it in "draft" form in case there were others you wanted to add, or in case you had any questions for us.

Best,

Caroline

Goldberg, Stuart (ODAG)

From: Goldberg, Stuart (ODAG)
Sent: Monday, February 3, 2014 7:19 PM
To: Cole, James (ODAG)
Subject: FW: PPD-28
Attachments: ppd-28.pdf

Stuart M. Goldberg
Principal Associate Deputy Attorney General
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 4208
Washington, D.C. 20530
(b) (6) [redacted]

From: Walsh, James (ODAG)
Sent: Monday, February 03, 2014 7:16 PM
To: Dix, Melanie (ODAG); Brinkley, Winnie (ODAG)
Cc: Goldberg, Stuart (ODAG); O'Neil, David (ODAG)
Subject: PPD-28

Melanie/Winnie,

The DAG requested that I leave him a copy of the attached document for his review first thing in the morning. Can you please make sure that it is available for his review?

Thanks,

Jim

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 counterintelligence[2] 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 advantage[4] 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 bulk[5] 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.[6]

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.[8]

(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

---

[6] 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.

[8] 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.

# # #

From: Burrows, Charlotte (ODAG)
Sent: Wednesday, March 19, 2014 6:43 PM
To: Walsh, James (ODAG); Fitzpatrick, Benjamin (NSD); Brown Lee, Erika (ODAG)
Cc: Zebrak, Julie R. (ODAG)
Subject: FW: PDF of signed letter transmitting corrected transcript of DAG Cole from 2-4-14 hearing re: Recommendations to Reform foreign Intelligence Programs

FYI

From: Freeman, Andria D (OLA)
Sent: Wednesday, March 19, 2014 4:32 PM
To: Ruppert, Mary (OLA); Burrows, Charlotte (ODAG); Columbus, Eric (ODAG)
Subject: PDF of signed letter transmitting corrected transcript of DAG Cole from 2-4-14 hearing re: Recommendations to Reform foreign Intelligence Programs


3-19-14 Ltr returning correc...


03-18-14 Ltr transmitting cor...

For your files

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

February 21, 2014

Mr. James Cole
Deputy Attorney General
U.S. Department of Justice
Washington, D.C. 20530

Dear Mr. Cole,

On behalf of the Committee on the Judiciary, I want to express our sincere appreciation for your participation in the hearing entitled "Recommendations to Reform Foreign Intelligence Programs" on Tuesday, February 4, 2014. Your testimony was informative and will assist us in future deliberations on the important issues addressed during the hearing.

Also, please find a **verbatim** transcript of the hearing enclosed for your review. The Committee's Rule III (e) pertaining to the printing of transcripts is as follows:

> *The transcripts...shall be published in **verbatim form**, with the material requested for the record...as appropriate. Any requests to correct any errors other than errors in the transcription, or disputed errors in transcription, shall be appended to the record, and the appropriate place where the change is requested will be footnoted.*

Additionally, during the hearing a Member asked a specific question. This question can be found on page 68. Please include your response to this question with the return of the transcript. Your reply to this question will be made part of the official printed hearing record.

Please return your transcript edits to the Committee on the Judiciary by Friday, March 7, 2014. Please send them to the Committee on the Judiciary, Attention: Kelsey Deterding, 2138 Rayburn House Office Building, Washington, DC 20515. If you have any further questions or concerns, please contact Ms. Deterding at (b) (6) or by email: (b) (6)

Thank you again for your testimony.

Sincerely,

Bob Goodlatte

Bob Goodlatte
Chairman

Enclosure

1 ALDERSON REPORTING COMPANY
2 GREGORY ALTHAM
3 HJU035000

4 EXAMINING RECOMMENDATIONS TO REFORM FISA AUTHORITIES
5 Tuesday, February 4, 2014
6 House of Representatives
7 Committee on the Judiciary
8 Washington, D.C.

9 The committee met, pursuant to call, at 10:14 a.m., in
10 Room 2141, Rayburn House Office Building, Hon. Bob Goodlatte
11 [chairman of the committee] presiding.
12 Present: Representatives Goodlatte, Sensenbrenner,
13 Coble, Smith of Texas, Chabot, Bachus, Issa, Forbes, King,
14 Franks, Gohmert, Jordan, Poe, Chaffetz, Gowdy, Labrador,
15 Farenthold, Holding, Collins, DeSantis, Smith of Missouri,
16 Conyers, Nadler, Scott, Lofgren, Jackson Lee, Cohen, Johnson,
17 Chu, Deutch, DelBene, Garcia, Jeffries, and Cicilline.
18 Staff Present: Shelley Husband, Majority Staff
19 Director; Branden Ritchie, Majority Deputy Chief of
20 Staff/Chief Counsel; Allison Halataei, Majority

21 Parliamentarian; Kelsey Deterding, Clerk; Caroline Lynch,
22 Majority Counsel; Sam Ramer, Majority Counsel; Perry
23 Apelbaum, Minority Staff Director; Danielle Brown, Minority
24 Parliamentarian; and Aaron Hiller, Minority Counsel.

25 Chairman GOODLATTE. Good morning. The Judiciary
26 Committee will come to order. And without objection, the
27 chair is authorized to declare recesses of the committee at
28 any time.
29 Before we begin today's hearing, I would like to take a
30 moment to welcome the newest member of the House Judiciary
31 Committee, David Cicilline of Rhode Island's First
32 Congressional District.
33 Born in Providence, Congressman Cicilline moved to
34 Washington, D.C., shortly after law school to work as a
35 public defender before returning to Rhode Island. In 1994,
36 he was elected to the Rhode Island State legislature and
37 ultimately elected Mayor of Providence in 2002 and again in
38 2006.
39 He was elected to the U.S. House of Representatives in
40 2010 and is also a member of the House Committee on Foreign
41 Affairs. And we welcome you to the Judiciary Committee.
42 [Applause.]
43 Mr. CONYERS. Mr. Chairman?
44 Chairman GOODLATTE. And I would like to recognize the
45 ranking member for any comments that he would like to make.
46 Mr. CONYERS. Thank you.
47 On behalf of all of us on this side of the aisle, we
48 join Chairman Goodlatte in welcoming our newest member to the
49 committee, Congressman David Cicilline, First District, Rhode

50 Island. A Mayor, a public defender, practiced law in Rhode
51 Island, and I am confident that his depth of experience will
52 be a great asset to this committee.
53 Mr. Cicilline, we welcome you and look forward to
54 working with you.
55 [Applause.]
56 Mr. CONYERS. Thank you.
57 Chairman GOODLATTE. And we welcome everyone to this
58 afternoon's hearing on Examining Recommendations to Reform
59 FISA Authorities, and I will begin by recognizing myself for
60 an opening statement.
61 Today's hearing will examine the various recommendations
62 to reform programs operated under the Foreign Intelligence
63 Surveillance Act, or FISA. Last summer's unauthorized public
64 release of these classified programs has sparked a national
65 debate about the extent of these programs and whether they
66 pose a threat to Americans' civil liberties and privacy.
67 There have been myriad proposals to reform or end these
68 programs. We are here today to vet these proposals and
69 discuss their impact on America's national security and their
70 value in enhancing civil liberty protections.
71 Following last year's leaks, Obama administration
72 officials appeared before this and other committees in
73 Congress to defend these programs and urge Congress not to
74 shut them down, including the bulk metadata collection

75 program operated under Section 215 of the PATRIOT Act. But
76 just 2 weeks ago, President Obama announced that he supports
77 "a transition that will end Section 215 bulk metadata program
78 as it currently exists and establish a mechanism that
79 preserves the capabilities we need without the Government
80 holding this bulk metadata."
81 I am glad the President has finally acknowledged what I
82 and many others concluded long ago, namely that the Section
83 215 bulk metadata program is in need of significant reform in
84 order to restore the trust of the American people and to
85 protect Americans' civil liberties. But I am disappointed
86 that the President was unable or unwilling to clearly
87 articulate to Congress and the American people the value of
88 this information in thwarting terror plots.
89 Instead, he simply declared that it is "important that
90 the capability that this program is designed to meet is
91 preserved," while simultaneously announcing that he was
92 ending the program as it currently exists.
93 The 5-year storage of bulk metadata by the NSA is
94 arguably the most critical and the most controversial aspect
95 of the Section 215 program. But transferring storage to
96 private companies could raise more privacy concerns than it
97 solves.
98 We need to look no further than last month's Target
99 breach or last week's Yahoo breach to know that private

100 information held by private companies is susceptible to cyber
101 attacks. And transferring storage to private companies would
102 require the Government to request data from multiple
103 companies to connect the dots it currently stores, thereby
104 complicating its ability to quickly and efficiently compile
105 valuable intelligence.

106 Of equal importance is the impact such a storage mandate
107 would have on the ability of American companies to compete in
108 a global market. American technology companies are
109 experiencing a lack of customer trust and a loss of
110 international business as a result of the Snowden leaks,
111 based upon the fear that information about their customers is
112 readily and routinely turned over to the American Government.

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

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

125 On January 17th, President Obama also announced his
126 desire to transfer the query approval of metadata from the
127 NSA to the FISA court. I am interested to hear from today's
128 witnesses whether such a reform will, in fact, result in
129 greater privacy protections without weakening national
130 security.
131 President Obama also endorsed additional privacy
132 protections for foreigners overseas. He instructed the
133 Attorney General and Director of National Intelligence to
134 take the unprecedented step of extending certain protections
135 that we have for the American people to people overseas.
136 Specifically, President Obama called for limiting the
137 duration that personal information about foreign nationals is
138 stored while also restricting the use of this information.
139 Is it wise to restrain our national security agencies by
140 extending to foreigners the rights and privileges afforded
141 Americans?
142 In addition to President Obama's proposed reforms, two
143 panels, the President's Review Group on Intelligence and
144 Communications Technology and the Privacy and Civil Liberties
145 Oversight Board, have issued reports with their own proposals
146 and conflicting legal analysis. On December 12th, the review
147 group issued its report.
148 While the review group questioned the value of the bulk
149 collection of telephone metadata by the Government, the

150 review group did conclude that the program is constitutional,
151 legal, and has not been abused and recommended the program
152 continue with third-party or company storage.
153 A majority of the PCLOB, however, issued a report on
154 January 23rd that questioned whether the program is
155 constitutional and concluded operated illegally under the
156 statute since 2006. And recommended the metadata program end
157 entirely.
158 I look forward to a discussion today of the
159 constitutional and statutory analysis and recommendations of
160 these two panels. The House Judiciary Committee has primary
161 jurisdiction over the legal framework of these programs and
162 has conducted aggressive oversight on this issue.
163 Any reforms Congress enacts must ensure our Nation's
164 intelligence collection programs effectively protect our
165 national security and include real protections for Americans'
166 civil liberties, robust oversight, and additional
167 transparency.
168 It is now my pleasure to recognize the ranking member of
169 the committee, the gentleman from Michigan, Mr. Conyers, for
170 his opening statement.
171 Mr. CONYERS. Thank you.
172 I welcome the witnesses today, the Deputy Attorney
173 General in the first panel, and the witnesses coming up in
174 the second panel.

175 Now the 9/11 Commission, observing that Congress had
176 "vested substantial new powers in the investigative agencies
177 of the Government" with the passage of the PATRIOT Act,
178 argued that it would be healthy for the country to engage in
179 full and informed debate on these new authorities.
180 The commission concluded that when that debate
181 eventually takes place, the burden of proof for retaining a
182 particular Government power should be on the executive to
183 explain that the power actually and materially enhances
184 security. Today, we are now engaged in that debate.
185 For the first time, the public understands that our
186 Government is engaged in widespread domestic surveillance.
187 This surveillance includes, but isn't limited to, the
188 Government's collection of records on virtually every phone
189 call placed in the United States under Section 215 of the
190 PATRIOT Act.
191 Consensus is growing that this telephone metadata
192 program is largely ineffective, inconsistent with our
193 national values, and inconsistent with the statute as this
194 committee wrote it. As the 9/11 Commission proposed, the
195 burden rests with the Government to convince us otherwise.
196 Reasonable people can disagree with me about whether or
197 not the Government has met that burden, but there are several
198 points to guide us in this debate that I believe are
199 incontrovertible. First, the status quo is unacceptable.

200 President Obama, his own Review Group on Intelligence and
201 Communication Technology, and the Privacy and Civil Liberties
202 Oversight Board all agree that the telephone metadata
203 program, as currently exists, must end.
204 The review group had full access to the leadership of
205 the intelligence community. It concluded that there has been
206 no instance in which the National Security Agency could say
207 with confidence that the outcome of a case would have been
208 different without the Section 215 metadata program.
209 The Privacy and Civil Liberties Oversight Board came to
210 the same conclusion and also observed that the operation of
211 the bulk telephone record program bears almost no resemblance
212 to the actual text of the statute.
213 In his remarks at the Department of Justice, President
214 Obama observed that because expanding technological
215 capabilities place fewer and fewer technical restraints on
216 what we can do, we have a special obligation to ask tough
217 questions about what we should do. The President ordered
218 immediate changes to the telephone metadata program and asked
219 the Attorney General and the Director of National Security to
220 develop options for a new approach that takes these records
221 out of Government hands.
222 I commend President Obama for his willingness to make
223 these necessary changes. It cannot be easy for a sitting
224 President to restrain his own intelligence capabilities, even

225 if it is the right thing to do. After all, in the
226 President's own words, there is an inevitable bias within the
227 intelligence community to collect more information about the
228 world, not less.
229 My second point is that the administration cannot solve
230 this problem without Congress. The House Judiciary Committee
231 must act. We are the primary committee of jurisdiction in
232 the House for the Foreign Intelligence Surveillance Act, the
233 exclusive means by which the Government may conduct domestic
234 surveillance.
235 We are the proper forum for a debate about
236 constitutional rights and civil liberties. More acutely, the
237 Government is dependent on this committee to renew the legal
238 authorities now under review.
239 Section 215 is scheduled to sunset on June 1, 2015. If
240 it expires, all Section 215 programs, not merely bulk
241 collection, expire with it. We should address bulk
242 collection today, or we risk losing all of Section 215 this
243 time next year. Unless this committee acts and acts soon, I
244 fear we will lose valuable counterterrorism tools, along with
245 the surveillance programs many of us find objectionable.
246 And finally, as this committee moves forward, H.R. 3361,
247 the USA FREEDOM Act, represents a reasonable consensus view
248 and remains the right vehicle for reform. I am struck by the
249 growing partisan -- bipartisan consensus here. More and more

250 of us seem to agree that the Congress should end bulk
251 collection under Section 215 but allow the FBI's continued
252 use of normal business records orders on a case-by-case
253 basis.
254 We should retain the basic structure of Section 702 of
255 the Foreign Intelligence Surveillance Act but enact
256 additional protections for United States persons whose
257 communications are intercepted without a warrant. We should
258 create an opportunity for an independent advocate to
259 represent privacy and civil liberties interests before the
260 FISA court.
261 And in the service of meaningful public debate, we
262 should declassify significant opinions of the FISA court,
263 enhance reporting to the Congress, and allow companies to
264 disclose more about their cooperation with the Government.
265 These reforms are consistent with the President's
266 remarks, the recommendations of the review group, and the
267 report of the Privacy and Civil Liberties Oversight Board.
268 They are also, point for point, the main objectives of the
269 measure called the USA FREEDOM Act.
270 Our colleague and former chairman of this committee, Mr.
271 Sensenbrenner, is credited as the original author of the
272 PATRIOT Act, is our lead on this bill in the House. Senator
273 Leahy has introduced an identical measure in the Senate.
274 The USA FREEDOM Act enjoys the support of 130 Members in

275 the House, evenly divided between Democrats and Republicans.
276 More than half of this committee now supports the bill, and
277 our numbers grow every week.
278 And so, Mr. Chairman, I urge that you bring this bill up
279 for consideration before the House Judiciary Committee as
280 soon as possible because our mandate is clear. We have heard
281 from the President, from his panel of experts, and from an
282 independent oversight board. We will examine their proposals
283 today, but the time for reform is now.
284 And so, at the risk of making too much reference to the
285 attacks of September 11, 2001, I close my remarks with
286 another passage from the 9/11 Commission report.
287 "We must find ways of reconciling security with liberty
288 since the success of one helps protect the other. The choice
289 between security and liberty is a false choice, as nothing is
290 more likely to endanger America's liberties than the success
291 of a terrorist attack at home.
292 "Our history has shown that insecurity threatens
293 liberty. Yet if our liberties are curtailed, we lose the
294 values that we are struggling to defend."
295 I thank you and yield back my time.
296 Chairman GOODLATTE. Thank you, Mr. Conyers.
297 And without objection, all other Members' opening
298 statements will be made a part of the record.
299 [The information follows:]

300 ********** COMMITTEE INSERT **********

301 Chairman GOODLATTE. It is now our pleasure to welcome
302 our first panel today, and if the members of the panel would
303 rise, I will begin by swearing in the witnesses.
304 [Witnesses sworn.]
305 Chairman GOODLATTE. Let the record reflect that all of
306 the witnesses responded in the affirmative.
307 Thank you, and I will begin by introducing our
308 witnesses.
309 Our first witness is Mr. James Cole, the Deputy Attorney
310 General of the United States at the Department of Justice.
311 Mr. Cole first joined the agency in 1979 as part of the
312 Attorney General's Honors Program and served the department
313 for 13 years as a trial lawyer in the Criminal Division.
314 He entered private practice in 1992 and was a partner at
315 Bryan Cave, LLP, from 1995 to 2010, specializing in white
316 collar defense. Mr. Cole has also served as chair of the
317 American Bar Association White Collar Crime Committee and as
318 chair-elect of the ABA Criminal Justice Section.
319 Mr. Cole received his bachelor's degree from the
320 University of Colorado and his J.D. from the University of
321 California at Hastings.
322 Our second witness is Mr. Peter Swire, a member of the
323 Review Group on Intelligence and Communications Technologies.
324 The review group's mission is to review and provide
325 recommendations on how, in light of advancements in

326 communications technologies, the United States can employ its
327 technical collection capabilities in a manner that optimally
328 protects national security and advances our foreign policy
329 while respecting our commitment to privacy and civil
330 liberties, recognizing our need to maintain the public trust,
331 and reducing the risk of unauthorized disclosure.
332 Mr. Swire is also a senior fellow at the Future of
333 Privacy Forum and the Center for American Progress, and
334 policy fellow at the Center for Democracy and Technology.
335 Mr. Swire is a professor at the Scheller College of Business
336 at Georgia Tech, having previously served as a C. William
337 O'Neill Professor of Law at the Ohio State University.
338 Mr. Swire worked for the Clinton administration as chief
339 counselor for privacy in the U.S. Office of Management and
340 Budget, where he held Government-wide responsibility for
341 privacy policy. In 2009 and 2010, Mr. Swire served as
342 Special Assistant to President Obama for Economic Policy,
343 serving in the National Economic Council with Lawrence
344 Summers. Mr. Swire earned his undergraduate degree from
345 Princeton and his juris doctor from Yale Law School.
346 Our third witness is Mr. David Medine, the chairman of
347 the Privacy and Civil Liberties Oversight Board. Mr. Medine
348 started full time as chairman on May 27, 2013. Prior to
349 serving as chairman, he was an attorney fellow for the
350 Securities and Exchange Commission and a special counsel at

351 the Consumer Financial Protection Bureau.

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

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

362 I want to welcome all of you. I would ask each of you
363 summarize your testimony in 5 minutes or less, and to help
364 you stay within that time, there is a timing light on your
365 table. When the light switches from green to yellow, you
366 will have 1 minute to conclude your testimony. When the
367 light turns red, it signals the witness' 5 minutes have
368 expired.

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

371 TESTIMONY OF HON. JAMES M. COLE, UNITED STATES DEPARTMENT OF
372 JUSTICE; PETER P. SWIRE, REVIEW GROUP ON INTELLIGENCE AND
373 COMMUNICATIONS TECHNOLOGY; AND DAVID MEDINE, PRIVACY AND
374 CIVIL LIBERTIES OVERSIGHT BOARD

375 TESTIMONY OF HON. JAMES M. COLE

376 Mr. JAMES COLE. Thank you, Mr. Chairman, Ranking Member
377 Conyers, and members of the committee, for inviting us here
378 to continue the discussion of certain intelligence collection
379 activities and our efforts to protect privacy and civil
380 liberties at the same time.
381 We have all invested a considerable amount of energy
382 over these past few months in reviewing specific intelligence
383 collection programs and the legal framework under which they
384 are conducted. I think it is fair to say that all of us --
385 the members of the Privacy and Civil Liberties Oversight
386 Board, the members of the Presidential review group, the
387 administration, and the Congress -- want the same thing -- to
388 maintain our national security while upholding the liberties
389 that we all cherish.
390 It is not always easy to agree on how best to accomplish
391 these objectives, but we will continue to work in earnest to

392 advance our common interests, and we appreciate the good
393 faith in which everyone has engaged in this endeavor.
394 We have benefited from the consideration of these
395 difficult issues by the PCLOB and the PRG, and it's a
396 pleasure to appear with them today. In his speech on January
397 17th, the President laid out a series of measures to reform
398 our surveillance activities that draw upon many of the core
399 recommendations issued by the PCLOB and the PRG.
400 The work to develop or carry out these measures is well
401 underway, and I would like to highlight just a few of the
402 most significant initiatives announced by the President that
403 the Department of Justice is working to implement in close
404 coordination with the intelligence community.
405 First, we are examining alternatives to the collection
406 of bulk telephony metadata under Section 215, which, as you
407 noted, the President has said will end as it currently
408 exists. The President has said that the capability that this
409 program was designed to provide is important and must be
410 preserved, but we must find a new approach that does not
411 require the Government to hold this bulk metadata.
412 The Section 215 program, as currently constituted, is
413 subject to an extensive framework of laws and judicial orders
414 and to oversight by all three branches of Government,
415 designed to prevent abuse. Neither the PCLOB nor the PRG has
416 questioned the rigor of that oversight system, nor has anyone

417 identified any intentional misuse of the telephony metadata.
418 Nevertheless, we recognize that any time large amounts
419 of data are collected, whether by the Government or private
420 companies, there is a potential for misuse, and it will be
421 important that the new approach remains subject to a rigorous
422 oversight regime. Insofar as the legality of the program is
423 concerned, it is important to remember that the courts, the
424 final arbiters of the law, have repeatedly found the program
425 lawful, including 15 separate judges of the Foreign
426 Intelligence Surveillance Court and two District Courts.
427 There has been only one contrary District Court ruling, which
428 is now on appeal.
429 The PCLOB undertook its own analysis of the legality,
430 but the members were unable to agree on whether it was
431 authorized under the statute. Although we continue to
432 believe the program is lawful, we recognize that it has
433 raised significant controversy and legitimate privacy
434 concerns. And as I have said, we are working to develop a
435 new approach, as the President has directed.
436 Second, we are working to develop additional
437 restrictions on Government's ability to retain, search, and
438 use in criminal cases U.S. person information incidentally
439 collected when we target non-U.S. persons overseas under
440 Section 702 of FISA.
441 Third, the President recognized that our global

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

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

459 Fifth, the President called upon Congress to authorize
460 the establishment of a panel of advocates from outside the
461 Government to provide an independent voice in significant
462 cases before the FISC. We believe the ex parte process has
463 functioned well. The court, however, should be able to hear
464 independent views in certain FISA matters that present
465 significant or novel questions. We will provide our
466 assistance to Congress as it considers legislation on this

467 subject.

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

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

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

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

483 ********** INSERT 1 **********

484 Chairman GOODLATTE. Thank you.

485 Mr. Swire, welcome.

486 TESTIMONY OF PETER P. SWIRE

487 Mr. SWIRE. Thank you, Mr. Chairman and Ranking Member
488 Conyers and members of the committee.
489 I appreciate the opportunity to testify today on behalf
490 of the five members of the review group and the invitation
491 and the request was rather than this being my personal
492 statement, that it be reflecting the group's effort and our
493 report that was issued in December.
494 The review group is a group of five people. I'll
495 briefly describe them in the context of our work and how we
496 came to our recommendations.
497 One of the members is Michael Morell, who had more than
498 30 years in the CIA as a professional intelligence officer,
499 and he finished his time there as Deputy Director of the CIA.
500 So we had the benefit in our group of somebody with many
501 years of deep experience in the intelligence community.
502 Richard Clarke had been the senior cybersecurity and
503 anti-terrorism adviser, both to President Clinton and
504 President George W. Bush. So he came to this with both
505 technological and Government experience in many different

506 respects.

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

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

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

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

529 The second thing is that in 2004, I published an
530 extensive article on the history and issues surrounding FISA,

531 which touches on some of the issues we'll address today.

532 In terms of the review group, in August, the five of us

533 were invited to come meet with the President and be named to

534 the review group, and I'd like to just take a moment on the

535 charter of our group. The charter was to try to bring

536 together things that are hard to bring together.

537 How do we do national security? How do we maintain our

538 foreign allies and relationships with other countries,

539 including commercial relationships? How do we preserve

540 privacy and civil liberties in this new technological age?

541 How do we maintain public trust? And finally, how do we

542 address the insider threat, which we've seen can be a very --

543 a big problem in terms of maintaining classified secrets?

544 So, within these national security, commercial, civil

545 liberties and public trust things, how do we put this all

546 together in a package? The -- our job was to be -- as tasked

547 by the President, was to be forward looking. Where should we

548 go from here? So I'd like to emphasize we did not do a

549 constitutional analysis of any of the programs. That was not

550 what we thought our job was.

551 We also did not do a specific statutory analysis of

552 whether something was or was not lawful that was being done

553 specifically around 215. Others have taken on those tasks.

554 Our group did not do that constitutional or statutory

555 analysis. We thought putting these five major goals together

556 into a report was plenty for us to take on during the fall.
557 One of the things about our group is that we, in
558 addition to being forward looking, were not limited to
559 counterterrorism in our mission. And so, the PCLOB, as David
560 Medine will talk about, has statutory authorities
561 specifically focused on counterterrorism. We were asked to
562 take on broader issues around foreign affairs, et cetera,
563 that in some cases go beyond that scope.
564 We met during the fall each week. We got briefed
565 extensively on a classified basis from the agencies. We had
566 detailees from the agencies. Every question we asked for, we
567 got answered. The agencies were outstanding in their
568 cooperation.
569 We presented our preliminary findings orally to the
570 President's top advisers during the fall and, on December
571 11th, transmitted our report to the White House. This was
572 our report. It was submitted for declassification review to
573 make sure we weren't releasing classified secrets, but the
574 recommendations were the group of five, it was our own.
575 And as it turned out, after we did this work together,
576 the civil liberties people in our group, the anti-terrorism,
577 the CIA people in the group, all of us came to consensus. So
578 every sentence of the report turned out to be agreed to by
579 all five of us. As I testify and as I answer your questions
580 today, my effort will be to accurately reflect the report

581 that brought these disparate views together.

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

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

590 Thank you.

591 [The statement of Mr. Swire follows:]

592 ********** INSERT 2 **********

593 Chairman GOODLATTE. Thank you.

594 Mr. Medine, welcome.

595 TESTIMONY OF DAVID MEDINE

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

598 Chairman GOODLATTE. You want to hit the button there on
599 your -- good. Pull it close to you as well.

600 Mr. MEDINE. There we go. Thank you, Mr. Chairman,
601 Ranking Member Conyers, and members of the committee, for the
602 opportunity to testify regarding recommendations to reform
603 the Nation's intelligence gathering program.

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

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

615 But before I start, I'd like to express the board's
616 respect and admiration for the men and women in the
617 intelligence community, who work tirelessly to protect our
618 country day and night and uphold our values. We hold them in
619 the highest regard, based on everything we have observed
620 during the course of conducting our study.
621 In June, many Members of Congress and the President
622 asked us to prepare a report on the 215 and 702 programs
623 conducted by NSA. Our 702 report will be issued in a couple
624 of months.
625 In the course of conducting our study, we had briefings
626 with a number of intelligence agencies, had an opportunity to
627 see the 215 program in action. We held two public events to
628 get public input, as well as soliciting public comment, and
629 met with industry groups, trade associations, and advocates
630 regarding this program. This culminated in our release on
631 January 23rd of our report addressing, again, the 215 program
632 and reforms to the FISC.
633 With regard to the 215 program, we conducted a statutory
634 analysis and concluded that the program lacks a viable
635 foundation in the law. We also looked at the First and
636 Fourth Amendment of the Constitution and concluded that the
637 program raised serious concerns under both of those
638 amendments.
639 We examined the privacy and civil liberties consequences

640 of the program and found them serious because the program
641 contains highly sensitive information. Citizens may be
642 chilled, their associational rights in engaging with
643 reporters or religious groups or political organizations,
644 knowing that the Government is collecting information about
645 them.
646 And is also information that's subject to potential
647 abuse. We did not see any abuse now, but we certainly know
648 lessons from the 20th century where there were abuses of
649 surveillance of civil rights leaders and anti-war activists
650 and others. And so, gathering this information by the
651 Government does raise serious privacy and civil liberties
652 consequences.
653 But we also looked at the efficacy of the program, and
654 we looked at each of the instances in which there were
655 claimed successes in the program. We had classified
656 information, and we checked our facts with the intelligence
657 community. And after that analysis, we concluded that the
658 benefits of the program are modest at best, and they are
659 outweighed by the privacy and civil liberties consequences.
660 As a result, a majority of the board recommended that
661 the program be discontinued, and the entire board recommended
662 that there be immediate changes to the program to add privacy
663 and civil liberties protections. The dissenting members of
664 the board felt that the Government's interpretation of the

665 program in the law was reasonable and that with the privacy
666 changes that we are proposing on the interim basis, that they
667 would be comfortable with having the program continue with
668 those changes.
669 Turning to the Foreign Intelligence Surveillance Court,
670 the board unanimously recommends changes to that operation of
671 the court, both to bolster the court's confidence in the
672 public and as well as let the court benefit from adversary
673 proceedings, which are the heart of the judicial process.
674 So, accordingly, the board recommends that a panel of
675 special advocates be created, made up of private attorneys
676 appointed by the court in cases involving significant legal
677 and policy issues and new technologies so that there is
678 another side presented besides the Government's position to
679 argue on both statutory and constitutional grounds.
680 We also recommend that there be an opportunity to appeal
681 decisions by -- of the court by the advocate. There have
682 only been two appeals ever to the Foreign Intelligence
683 Surveillance Court of review, and we think there's a benefit
684 from the appellate process and, therefore, recommend a
685 mechanism by which we think you can constitutionally have the
686 special advocate obtain appellate review of the decisions.
687 And then we also encourage the court to obtain more
688 technical assistance and outside legal views because these
689 are complex issues that the court is confronting, and the

690 court could benefit from technology advice.

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

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

698 [The statement of Mr. Medine follows:]

699 ********** INSERT 3 **********

700 Chairman GOODLATTE. Thank you, Mr. Medine.

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

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

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

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

725 This is a tool that gives us one of those pieces of
726 information, the connections from one person to another. And
727 in order to be able to get it in a useful way, the initial
728 view and the most expeditious way to do it was to have the
729 bulk collection of the mass of telephone records with
730 significant restrictions on how we could access it.
731 So that we could, when we find a phone number associated
732 with a certain terrorist group, we can search through the
733 other records and find those connections. Now we can find
734 other ways, and we are finding other ways to try and
735 approximate and gain that same kind of information.
736 Chairman GOODLATTE. Let me ask you about one subset of
737 that that is very, very important and seems to be the thing
738 that concerns many people the most. The President's review
739 group has recommended that the storage of bulk metadata be
740 transferred to a third party or to company storage. The
741 President also indicated that it is his preference as well.
742 How does third-party storage protect Americans' privacy
743 more than Government storage, and does the President have
744 additional ideas for reform beyond third-party storage?
745 Mr. JAMES COLE. Well, Mr. Chairman, we're trying to
746 work through the best way to go about this, and the President
747 has given us this direction, and we are looking for all the
748 possible alternatives. The President's review group made
749 that recommendation. The PCLOB noted that there are issues

750 with all of the different alternatives that you can use here.

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

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

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

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

772 Mr. JAMES COLE. I think that's the process we're going
773 through right now. I don't want to try and get too far ahead
774 of it and hypothesize about where we may end up by the time

775 we have to make recommendations to the President and he makes
776 a decision. But obviously, the providers already --
777 Chairman GOODLATTE. You have heard the ranking member.
778 There is legislation before the committee. There are other
779 legislative ideas than the one he referenced. But he and
780 many others are chomping at the bit to move forward, and
781 having the administration's position on this critical aspect
782 of this is important.
783 So we need to know the answer to that sooner rather than
784 later.
785 Mr. JAMES COLE. And we're working on trying to get that
786 answer, and we'll provide it to you. The providers already
787 keep these records for a certain period of time, and some
788 keep it longer than what is required under regulations.
789 And so, we have to work through what we think is the
790 optimal period of time that the records need to be kept if
791 there's going to be a provider keeping it solution.
792 Chairman GOODLATTE. And I want to direct one question
793 to Mr. Medine before my time expires. The PCLOB majority
794 recommends ending the bulk collection of telephony metadata
795 under Section 215. The majority also recommends, however,
796 that the program continue with certain modifications.
797 Why did the majority not recommend the immediate end to
798 the program?
799 Mr. MEDINE. The majority looked to how other programs

800 have been discontinued when, say, courts have struck them
801 down. Even the Supreme Court has found programs
802 unconstitutional and, nonetheless, gave the Government an
803 opportunity to transition to a new program.
804 And so, rather than shut it off, we felt we followed the
805 approach that the courts have taken, which is to say let's
806 quickly transition into another program, either keeping the
807 information with providers or some other mechanism as
808 developed.
809 Chairman GOODLATTE. Well, you are talking about courts
810 in other cases because the court --
811 Mr. MEDINE. Nothing -- not in this case.
812 Chairman GOODLATTE. I haven't heard them say that in
813 this case.
814 Mr. MEDINE. But we've looked at precedent of how if a
815 program has been found to be illegal or unconstitutional,
816 courts oftentimes don't just shut it down. They give an
817 opportunity to transition, and we thought that that --
818 especially since we're not a court, that it was reasonable to
819 recommend that there be a period of transition, hopefully
820 brief, to a different program.
821 Chairman GOODLATTE. Thank you.
822 The gentleman from Michigan, Mr. Conyers, is recognized
823 for 5 minutes.
824 Mr. CONYERS. Thank you.

825 And I thank the witnesses.

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

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

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

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

842 Mr. SWIRE. Thank you, Congressman.

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

848 We also, on bulk collection, on 215 in particular, found
849 that there had not been any case where it had been essential

850 to preventing an attack. The review group did find, as a
851 group, that there was usefulness in Section 215 bulk
852 collection, and we thought that transitioning it away from
853 Government holding of the data was better within our system
854 of checks and balances than having it held by the Government.
855 Mr. CONYERS. Thank you.
856 The report also says that the Government should no
857 longer hold telephone metadata. If the Government can only
858 collect metadata with a particularized showing of suspicion
859 and the Government cannot hold information in bulk, what is
860 left of the telephone metadata program?
861 Mr. SWIRE. Well, what's left is similar to metadata in
862 other circumstances. This committee knows about trap and
863 trace and pen register authorities, which are done under
864 standards much less than probable cause. It's much easier to
865 get the metadata as step one to an investigation, and
866 everything in our approach is consistent with using a
867 judicial step, but a step with less than probable cause to go
868 forward with the investigations.
869 Mr. CONYERS. Mr. Deputy Attorney General, in his
870 January 17th remarks, President Obama asked the Justice
871 Department to develop options for a new approach that can
872 match the capabilities and fill the gaps that the Section 215
873 program was designed to address without the Government
874 holding this metadata itself.

875 What range of options might we consider as alternatives
876 to the Government storing this information, if your group has
877 gotten that far in its work?
878 Mr. JAMES COLE. Well, certainly, Mr. Ranking Member,
879 there are three options that come to mind just off the top of
880 my head, which is -- or two options. One is a third party
881 who would gather all of the data together so that the access
882 could be across providers, which was the -- one of the
883 efficient and effective aspects of the metadata bulk
884 collection program.
885 The other is to have the providers keep it. At this
886 point, under regs, they're required to keep it for about 18
887 months. It might require legislation, if we deem that not to
888 be a sufficient amount of time, to require them to keep it
889 longer. I don't think they really favor that option.
890 We're also trying to think outside the box and see if
891 there are any other options that we can come up with.
892 There's a lot of very talented and very capable people trying
893 to think through this problem and trying to find whatever
894 creative solutions we can.
895 Mr. CONYERS. Thank you.
896 And my last question is to Mr. Medine. Both your board
897 and the review group find that the bulk collection program
898 has never disrupted a terrorist -- a terror plot. The report
899 also closely examines the 12 cases in which the Government

900 says the telephone metadata program has contributed to a
901 success story in a counterterrorism investigation.
902 What were those contributions, and do any of them to you
903 justify a massive domestic call records database?
904 Mr. MEDINE. Mr. Ranking Member, we have analyzed
905 carefully all of the success stories and, as you indicate,
906 did not find any instance in which a plot was disrupted or an
907 unknown terrorist was identified. However, there are some
908 aspects of the program that have produced some benefits.
909 One, a material assistance case benefited from use of the 215
910 program.
911 And there are also the "peace of mind" concept, which is
912 sometimes it's helpful to know there isn't a U.S. connection
913 to a potential plot that's underway overseas. But we found
914 in those and any other instances where the program had had
915 successes, that those successes could have been replicated
916 using other legal authorities without the need to collect
917 bulk telephone metadata and all of the privacy and civil
918 liberties problems associated with that collection.
919 Mr. CONYERS. Mm-hmm. Thank you, Mr. Chairman.
920 Chairman GOODLATTE. Thank you.
921 The chair recognizes the gentleman from Wisconsin, the
922 chairman of the Crime, Terrorism, Homeland Security, and
923 Investigations Subcommittee, Mr. Sensenbrenner, for 5
924 minutes.

925 Mr. SENSENBRENNER. Thank you very much, Mr. Chairman.
926 I was the principal author of the PATRIOT Act that was
927 signed by President Bush in 2001, and I also was the
928 principal author of the two reauthorizations in 2006 and in
929 2011. Let me say that the revelations about Section 215 were
930 a shock and that if the bulk collection program was debated
931 by the Congress in each of these three instances, it never
932 would have been approved.
933 And I can say that without qualification. Congress
934 never did intend to allow bulk collections when it passed
935 Section 215, and no fair reading of the text would allow for
936 this program.
937 The PCLOB said, "The Section 215 bulk telephone records
938 program lacks a viable legal foundation under Section 215,
939 implicates constitutional concerns under the First and Fourth
940 Amendments, raises serious threat to privacy and civil
941 liberties as a policy matter, and has shown only limited
942 value."
943 I agree with that. Now the administration, the argument
944 that they use under Section 215 is essentially that if the
945 administration and the intelligence community wants
946 something, it is relevant. And that is not a limiting
947 principle, which everybody thought relevant was, it is a
948 vacuum cleaner, and that is why there has been such outrage,
949 both here and overseas, that has impacted our intelligence

950 community and also implicated the commercial relationship
951 between us and foreign countries, particularly major trading
952 partners in the European Union.
953 And I am very worried about an intelligence review
954 structure where the administration and the FISCs could
955 sanction this. That is why Mr. Conyers and I, together with
956 a lot of Members equally divided between Republicans and
957 Democrats, have sponsored the USA FREEDOM Act.
958 We attempted to make the FREEDOM Act a balance between
959 the civil liberties concerns that have been expressed in the
960 last 7 months, as well as the need to have an active
961 intelligence operation. Now Section 215 expires in June of
962 next year. And unless Section 215 is fixed, you, Mr. Cole,
963 and the intelligence community will end up getting nothing
964 because I am absolutely confident that there are not the
965 votes in this Congress to reauthorize Section 215.
966 Now the FREEDOM Act is the only piece of legislation
967 that attempts to comprehensively address this problem in a
968 way that I think will get the support of a majority of the
969 Members of both the House and the Senate. The Feinstein bill
970 I think is a joke because it basically prohibits bulk
971 collection, except as authorized under a subsection, which
972 authorizes the intelligence community to keep on doing
973 business as usual.
974 Mr. Cole, I think that we are smart enough to recognize

975 that for what it is. And it is a joke. There hasn't been
976 anything else that has come from the administration or
977 elsewhere to deal with this issue, and the clock, sir, is
978 a-ticking. And it is ticking rapidly, and this is going to
979 have to be addressed in this year, even though it is an
980 election year.
981 Now will the Department of Justice, Mr. Cole, support
982 the FREEDOM Act? And all I need is a "yes" or "no" answer.
983 Mr. JAMES COLE. Uh --
984 Mr. SENSENBRENNER. Not "yes, but" or, "no, of course."
985 But "yes" or "no."
986 Mr. JAMES COLE. The Department of Justice is a big
987 place, Senator, and at this point, we have not taken a
988 position on the FREEDOM Act. We'd be more than happy to --
989 Mr. SENSENBRENNER. Well, then I --
990 Mr. JAMES COLE. -- work with you on that.
991 Mr. SENSENBRENNER. Well, then -- well, I haven't seen
992 any indication of that to date, and I would urge you to hurry
993 up and to get the big place together. Because the FREEDOM
994 Act are reasonable reforms that have been emphasized as
995 necessary and responsible by both the PCLOB and the review
996 panel. There is nothing else out there to fix this up.
997 So you have a choice between reaching something that
998 will be supported by a majority of the Congress or letting
999 the clock tick, and come June 1st of next year, there will be

1000 no authority for anything under Section 215.

1001 Now if the administration has got problems with the
1002 Leahy-Sensenbrenner-Conyers bill, let us talk about it. But
1003 it is past time for genuine reform, and I can tell you, sir,
1004 that if the administration doesn't want to weigh in on this,
1005 I am sure that Congress will do so. And I don't want to hear
1006 any ex post facto complaining.

1007 My time is up.

1008 Chairman GOODLATTE. The chair recognizes the gentleman
1009 from New York, Mr. Nadler, for 5 minutes.

1010 Mr. NADLER. Thank you very much, Mr. Chairman.

1011 Let me first do something I rarely do, which is to
1012 express my complete and total agreement with the gentleman
1013 from Wisconsin.

1014 [Laughter.]

1015 Mr. NADLER. Both in his analysis of the misuse and
1016 abuse of Section 215 and of what will happen to Section 215
1017 if it is not substantially modified either this year or early
1018 next year.

1019 Mr. Conyers and I and various others opposed the Section
1020 215 version that was adopted back in 2001 and again in 2006
1021 and 2011. We thought it was too broad. But now we have even
1022 that very broad version completely taken over the side by the
1023 administration, by two administrations, actually, and by --
1024 and by the FISC.

1025 And the fact that the FISC several times determined that
1026 the use of Section 215 as authorization for what amounts to a
1027 general warrant, all right? You can collect all data, and
1028 then you can access that data without a specific warrant to
1029 access it or even a court order to access it, based on
1030 reasonable and articulable suspicion, but simply by an NSA or
1031 CIA officer saying, "We really need to look at that
1032 particular phone," is a derogation of all of American
1033 history, frankly, since 17 -- it is why we put the Fourth
1034 Amendment in because we objected to the British general
1035 warrants.
1036 And we have, in effect, reestablished that here. And
1037 that will not stand. It cannot be allowed to stand.
1038 So let me simply echo that it has got to change. There
1039 is no excuse for picking everything and then allowing access
1040 to that without some sort of a specific court order.
1041 And the fiction that the warrant that the FISA court
1042 grants and says Verizon or AT&T shall give the Government
1043 access, you know, all telephone metadata over a 3-month
1044 period is a warrant, is a specific warrant that negates the
1045 necessity for a warrant or a court order for more specific
1046 information is just that, a fiction, and it is a general
1047 warrant. And it cannot be permitted to stand, and it won't
1048 be permitted to stand.
1049 So I will second Mr. Sensenbrenner and urge you to

1050 swiftly get the department together and to if you don't want
1051 the FREEDOM Act to pass it the way it is or Section 215
1052 simply to not be extended, which might be the best solution,
1053 frankly, from my point of view, you better come in with very
1054 specific recommendations.
1055 Now let me say last week in testimony before the Senate,
1056 some administration officials suggested that terrorist plots
1057 thwarted is not the appropriate metric for evaluating the
1058 effectiveness of the program. And yet for months, the
1059 administration has made precisely the opposite argument.
1060 For example, in a September letter to NSA employees,
1061 General Alexander wrote that the agency has "contributed to
1062 keeping the U.S. and its allies safe from 54 terrorist
1063 plots."
1064 We have heard this 54 terrorist plots line repeated on
1065 several other occasions, although PCLOB and a lot of others
1066 have discredited it. Why has the argument changed? Why are
1067 we now to apply a different set of metrics to the program?
1068 Mr. JAMES COLE. I assume that's directed to me, Mr.
1069 Nadler.
1070 Mr. NADLER. Yes, it is.
1071 Mr. JAMES COLE. Well, first of all, I think to a degree
1072 you're going to have to ask the people who made those
1073 statements. I don't think any of them were from the
1074 Department of Justice.

1075 We have been, and actually, some of the members of the
1076 PCLOB have agreed that that is -- the past success or failure
1077 is not the only metric to use, or necessarily the best one.
1078 That there are many different ways to assess the utility of
1079 the 215 program that doesn't always have to be, as I said
1080 earlier, the smoking gun or the nail in the coffin that gives
1081 you the single piece of evidence that will lead to success.
1082 It's one piece of evidence.
1083 Mr. NADLER. Okay. Thank you.
1084 I am sorry to cut you off, but I have another question I
1085 must get in. National security letters empower the FBI and
1086 other Government agencies to compel individuals and
1087 organizations to turn over many of the same records that can
1088 be obtained by Section 215. But NSLs are issued by FBI
1089 officials, not by a judge or by a prosecutor in the context
1090 of a grand jury investigation.
1091 As the Government has explained their use of this to
1092 this committee, NSLs are used primarily to obtain telephone
1093 records, email subscriber information, and banking and credit
1094 card records. The FBI issued 21,000 NSLs in fiscal year
1095 2012. The oversight and minimization requirements for these
1096 NSLs are far less rigorous than those in place for Section
1097 215 orders.
1098 The review group recommends "that all statutes
1099 authorizing the use of national security letters should be

1100 amended to require the use of the same oversight
1101 minimization, retention, and dissemination standards that
1102 currently govern the use of Section 215 orders."
1103 Should we adopt that recommendation? Is there any
1104 reason that the two programs should not be harmonized? For
1105 that matter, is there any reason that NSLs should exist in
1106 addition to Section 215 authorization in whatever form we
1107 extend it, if we do?
1108 Mr. JAMES COLE. Well, actually, under the NSL program,
1109 you can't get the same records you can get with 215. It's
1110 much more limited under NSLs as to just specific categories
1111 of records. Whereas, 215, grand jury subpoenas, things like
1112 that, the records are almost unlimited as to the nature or
1113 the type that you can get.
1114 So there's a restriction in NSLs. They're used really
1115 in the main as part of preliminary inquiries --
1116 Mr. NADLER. Yes, but my point is if you can get it as
1117 under 215, if, in fact, 215 is broader, why do you need NSLs
1118 ever?
1119 Mr. JAMES COLE. It may just be a question of, again,
1120 how many times you need that information and whether or not
1121 you go to a court. In a grand jury situation, subpoenas are
1122 issued without the involvement of the court many, many, many
1123 times, probably as frequently, if not more so, as NSLs.
1124 Mr. SENSENBRENNER. [Presiding] The gentleman's time has

1125 expired.

1126 Mr. NADLER. Thank you.

1127 Mr. SENSENBRENNER. The gentleman from North Carolina,

1128 Mr. Coble?

1129 Mr. COBLE. I thank the chairman.

1130 Gentlemen, good to have you all with us.

1131 Mr. Cole, I was going to talk to you about bulk

1132 collection, but I think that has been pretty thoroughly

1133 examined.

1134 Mr. Swire, let me go to you. The review group's report

1135 recommended a transition of Section 215 bulk metadata from

1136 Government storage to storage providers or third parties.

1137 This recommendation is consistent with recent guidance put

1138 forth by the administration after its own review.

1139 Last week, it was reported by Yahoo that information

1140 relating to email accounts and passwords, likely in the hands

1141 of such a party database, had been compromised due to a

1142 security breach. Are you concerned that Section 215 metadata

1143 could be similarly compromised after transitioning to a

1144 private provider or third-party storage?

1145 Mr. SWIRE. Thank you, Congressman.

1146 A couple of observations. One is, of course, that the

1147 National Security Agency itself has had leaks and lack of

1148 complete security for its documents. So we're not comparing

1149 perfect with perfect. We face these challenges for databases

1150 in each case.

1151 A second observation is that the telephone companies
1152 hold telephone records. That's part of what they do and have
1153 done, and one of the options that we put forward is that the
1154 telephone companies would continue to hold these.

1155 So it's not a question of some new risk that we bring
1156 into the world. It's a risk that we face both from the
1157 Government side and the private sector side when we have
1158 these databases.

1159 I'm not sure if I -- your --

1160 Mr. COBLE. I think that was appropriate. Thank you,
1161 sir.

1162 Mr. SWIRE. Okay.

1163 Mr. COBLE. Mr. Medine? The FISA court has repeatedly
1164 upheld through its orders approving the NSA metadata program
1165 production of records to an agency other than the FBI. Did
1166 the privacy and civil liberties oversight majority take this
1167 into account?

1168 Mr. MEDINE. Yes, sir. The 215, on its face, only
1169 permits the FBI to make requests and obtain access to
1170 telephone records, despite the fact that under the current
1171 system is the NSA that obtains that information. And so, we
1172 think that was one of a number of respects in which the
1173 current program does not match the requirements of Section
1174 215.

1175 Mr. COBLE. So you have no discomfort with that?
1176 Mr. MEDINE. Excuse me?
1177 Mr. COBLE. You have no discomfort or problem with that?
1178 Mr. MEDINE. Yes. We have discomfort with a number of
1179 aspects of compliance. As was discussed earlier, the scope
1180 of relevance under the statute, the fact that information has
1181 to be linked to a specific investigation, and something that
1182 we haven't touched on yet, which is the Electronic
1183 Communications Privacy Act does not permit telephone
1184 companies to provide information to the Government under the
1185 215 program at all in either an individual request or on a
1186 bulk basis.
1187 The Electronic Communications Privacy Act only has an
1188 exception for national security letters and a few other
1189 areas. So we think that it makes sense to discontinue -- the
1190 majority does, to discontinue the 215 program and move to
1191 other legal authorities.
1192 Mr. COBLE. Thank you again, gentlemen, for being with
1193 us this morning.
1194 I yield back, Mr. Chairman.
1195 Mr. SENSENBRENNER. The gentleman from Virginia, Mr.
1196 Scott?
1197 Mr. SCOTT. Thank you, Mr. Chairman.
1198 Mr. Cole, you offered several procedural changes as
1199 recommendations. To paraphrase President Reagan, we need to

1200 trust, but codify. Would you object to those recommendations
1201 being codified rather than just remaining as administrative
1202 process?
1203 Mr. JAMES COLE. I think as the President mentioned in
1204 his speech, he's anxious to work with Congress on many of
1205 these things to try and find the right solutions that we
1206 have. I know the USA FREEDOM Act, many of the goals that are
1207 set out there are goals that we share.
1208 As I said in my opening, sometimes we have different
1209 ways of getting there, but we all seem to share the right
1210 goal together.
1211 Mr. SCOTT. And follow-up, several other questions. We
1212 frequently hear that the information gathered was helpful. I
1213 find that legally irrelevant. So let me just ask a question.
1214 If a collection of data were illegal, would a finding that
1215 it was helpful provide retroactive immunity for illegally
1216 collecting evidence?
1217 Mr. JAMES COLE. No, Mr. Scott, it would not. If the
1218 collection is illegal, the standard would not be met.
1219 Mr. SCOTT. Thank you.
1220 Mr. Swire, there was a case a couple of months ago in
1221 DNA that found that if DNA is legally collected, that there
1222 is no -- there is no prohibition against running it through
1223 the database to see if the person had committed another
1224 crime. If I were to go up to you, if a law enforcement

1225 agency would go up to you and say, "I would like some DNA to
1226 see if you have committed crime," that would be legally
1227 laughable.
1228 There appears to be no statutory limitation on what you
1229 can do with this information. So I guess my question is
1230 under -- you recommended under 702 that if you have collected
1231 information about a U.S. person, you can never use it in any
1232 proceeding. That would, of course, eliminate any incentive
1233 to get the information in the first place if it was for
1234 something other than foreign intelligence.
1235 If that is your recommendation for 702, would that also
1236 be your recommendation on 215, that you cannot use this data
1237 for other proceedings?
1238 Mr. SWIRE. Thank you, Congressman.
1239 Under Section 702, the target, by statute, is supposed
1240 to be somebody outside the United States. But sometimes
1241 they're in communication with people in the United States,
1242 and the concern behind our recommendation here is the
1243 possibility, which we have not seen in practice, is the
1244 possibility that the 702, do it overseas, could turn out to
1245 be a way to gather lots of information about United States
1246 people.
1247 And so, we made a recommendation to say that that would
1248 not be used in evidence in court as a way to prevent that
1249 temptation to use the authority to go after U.S. persons.

1250 In terms of 215, we don't have the same statute that's
1251 specifically targeted at overseas. 215 can be for domestic
1252 phone calls as well. So we didn't have this using our
1253 overseas authorities to get people domestically --
1254 Mr. SCOTT. But you're using foreign intelligence excuse
1255 to gather information that is subsequently used for criminal
1256 investigation.
1257 Mr. SWIRE. We did not make a recommendation about
1258 subsequent use, but we, I think -- I think all of us
1259 recognize using foreign intelligence powers for purely
1260 domestic phone calls has been something that's drawn a huge
1261 amount of attention to these issues and is something that
1262 historically has been something that's been looked at
1263 carefully when the CIA or other agencies have done it.
1264 So that's a concern using foreign intelligence issues
1265 authorities for domestic purposes.
1266 Mr. SCOTT. Let me follow through with another question
1267 that has been kind of alluded to, and that is that you want
1268 to limit Section 215 by ensuring that there is reasonable
1269 grounds to believe that it is relevant to an authorized
1270 investigation and the order is reasonably focused in scope
1271 and breadth.
1272 Can you explain how that recommendation varies from what
1273 everybody up here thought was present law?
1274 Mr. SWIRE. Well, I think when we talk about like a

1275 subpoena, an order should be reasonable in focus, scope, and
1276 breadth.
1277 Mr. SCOTT. We wouldn't have to put that in a statute to
1278 assume that to be the case, right?
1279 Mr. SWIRE. Well this gets into the statutory
1280 interpretation of the current 215. Our group did not take a
1281 position on that. The Government and the Privacy and Civil
1282 Liberties Oversight Board have come to different views on
1283 that.
1284 Mr. SCOTT. That we would have to put reasonable in
1285 scope and breadth in the statute for that to be assumed?
1286 Mr. SWIRE. Our recommendation was that a judge be
1287 involved in these things and that there be a reasonable
1288 breadth requirement explicitly in statute so that it's clear
1289 from Congress that that's what you intend.
1290 Mr. SCOTT. You also indicated a recommendation that the
1291 NSA not be involved in collection of data other than foreign
1292 intelligence. Can you explain what the NSA is doing that is
1293 not involved in foreign intelligence?
1294 Mr. SWIRE. In our -- in our report, we talk about two
1295 other areas the NSA currently has or bears very important
1296 responsibilities. Currently, the Director of the NSA is also
1297 the Director of Cyber Command, which is part of the military
1298 operation for combat-related activities in cyberspace. We
1299 thought that was quite a different function from foreign

1300 intelligence collection.

1301 The NSA also has responsibilities for what's called
1302 information assurance, protecting our classified and other
1303 systems, and we thought that defensive role is quite
1304 different from the offensive role of gathering intelligence
1305 and recommended those functions be split. The President has
1306 not decided to adopt either of those recommendations.

1307 Mr. SCOTT. Thank you.

1308 And Mr. Cole, are you aware of any abuses in the use of
1309 classified information? Things like I think there is a thing
1310 called LOVEINT. Are you familiar with that?

1311 Mr. JAMES COLE. I've heard that phrase, yes, sir.

1312 Mr. SCOTT. What is that?

1313 Mr. JAMES COLE. I think it's when you have somebody who
1314 is dating somebody, and they have access to one of these
1315 databases or a database and uses it to look at their -- the
1316 person they're dating and find out who they're talking to and
1317 who they're in contact with. That's what I understand it to
1318 mean.

1319 Mr. SCOTT. And that happens?

1320 Mr. JAMES COLE. I think there have been a few
1321 instances. I think the NSA had noted a few instances of it.
1322 I don't think they existed under 215. I think they may have
1323 existed under other authorities, but I think there has been
1324 just a handful of those over time.

1325 Mr. SCOTT. And what happens?

1326 Mr. JAMES COLE. And they've been dealt with

1327 immediately.

1328 Mr. SCOTT. And what has happened to the culprits?

1329 Mr. JAMES COLE. I know that most, if not all of them,

1330 lost their jobs. There ~~was~~ were referrals in many of those cases

1331 to the Justice Department to consider whether or not

1332 prosecution would be appropriate.

1333 Mr. SCOTT. Thank you, Mr. Chairman.

1334 Chairman GOODLATTE. [Presiding] Thank you.

1335 The chair recognizes the gentleman from Alabama, Mr.

1336 Bachus, for 5 minutes.

1337 Mr. BACHUS. Thank you.

1338 I would ask all three of the panelists is relevancy for

1339 purposes of intelligence gathering different from relevancy

1340 for purposes of, say, a criminal investigation or civil

1341 investigation? Shouldn't it be a -- shouldn't the standard

1342 be somewhat different, or is it? Start with Mr. Cole.

1343 Mr. JAMES COLE. I think as you've seen from the court's

1344 opinions, they borrow both from criminal investigations,

1345 civil proceedings, and do that and use those as analogies to

1346 get to the standard in foreign intelligence. And they find

1347 it to be the same standard.

1348 Mr. BACHUS. You know, as just a Member of Congress, I

1349 sort of have the opinion that it is much more urgent for us

1350 to defend ourselves as a country. But does sometimes
1351 applying a civil court standard of relevancy or even a
1352 criminal court standard of relevancy sort of diminish their
1353 ability at -- in defending the country from terrorists?
1354 Mr. JAMES COLE. Well, I think if you look at Judge
1355 Eagan's opinion from the FISA court, her view and her finding
1356 was that the term "relevancy" was very broad and was very
1357 useful in both criminal, civil, and foreign intelligence
1358 investigations and can be applied very broadly when it's
1359 necessary.
1360 It's not without limitation. It's not completely
1361 unrestrained. It's only when there is an actual need to get
1362 a broad scope of documents that it's authorized under that
1363 standard. And so, I think she had corporately found that
1364 scope.
1365 Mr. BACHUS. All right. Ask the other two gentlemen.
1366 Mr. MEDINE. The majority of the PCLOB has also
1367 considered relevancy in the context of criminal and civil
1368 proceedings as the statute suggests. And we looked at every
1369 case cited by the Government and more on criminal discovery,
1370 and I'm using the relevant standard, grand jury subpoenas, as
1371 well as civil. And our conclusion was that the 215 program
1372 far exceeded in scope anything that had been previously
1373 approved ever, and even the Government's white paper
1374 acknowledges that.

1375 And so, we in our -- at least the majority's view, it
1376 goes well beyond the face of the statute and a reasonable
1377 reading of relevance.
1378 Mr. BACHUS. Right. Now that was a majority opinion.
1379 Mr. MEDINE. That's correct.
1380 Mr. BACHUS. So did two members dissent from that?
1381 Mr. MEDINE. Yes, they did. And they -- and they felt
1382 that the Government's reading of the statute was a reasonable
1383 one, as was the court's interpretation.
1384 Mr. BACHUS. Okay. Mr. Swire?
1385 Mr. SWIRE. Yes, Congressman. So our group did not do
1386 that legislative history and statutory analysis as part of
1387 our work. In our forward-looking recommendation, we used the
1388 word "relevant" for the scope of a 215 order but said like a
1389 subpoena, it should be reasonable in focus, scope, and
1390 breadth. So we tried to hem it in with that reasonable scope
1391 language.
1392 Mr. BACHUS. I just, if we are talking about an EPA
1393 violation or we are talking about a criminal offense, a minor
1394 criminal offense, just applying those standards in that case
1395 law to public enemy and our foreign enemies of the United
1396 States, I feel like that lacks somewhat.
1397 Judge John Bates wrote a letter I think after both of
1398 you all's reviews came out, and I think he raised some very
1399 legitimate concerns over things you have assigned to the

1400 court, including reviewing every national security letter, a
1401 public advocate. He and I think others in judiciary believe
1402 that could be a hindrance.
1403 After his letter, have you reviewed it, and do you agree
1404 that he brings up some very valid points that ought to be
1405 considered? Mr. Swire? Professor?
1406 Mr. SWIRE. After our report was complete, we did
1407 receive the judge's letter. In terms of the public advocate,
1408 I'd make a following observation, which is the PCLOB report
1409 did extremely thorough analysis of the legality under the
1410 statute of 215 that was really much more detailed than
1411 anything any of the District Courts had done.
1412 And I think for just myself, not speaking for the whole
1413 group, I think that that supports our group's recommendation
1414 that having detailed briefing with thorough analysis on these
1415 issues not just from the Government can really help us
1416 understand the statute better. So that's part of why we
1417 thought the advocate would be helpful in some way because
1418 there would be a sort of thoroughness of a position --
1419 Mr. BACHUS. Could you -- could you all review his
1420 letter and maybe give this committee additional comments in
1421 view of his letter? Particularly with the increasing
1422 caseload, if you are going to increase their caseload, you
1423 are going to have to increase their resources.
1424 Mr. MEDINE. I should add that the PCLOB's

1425 recommendation is that there be a special advocate only in
1426 those cases which involve unique law and technology issues,
1427 not the everyday 215 order where judges are very well
1428 equipped to make those judgments.
1429 Mr. BACHUS. Yes, but I am talking about their
1430 caseloads. You have assigned -- under you all's -- both of
1431 your all's proposals, it is going to increase quite a bit.
1432 Mr. MEDINE. Yes. Sure.
1433 Mr. BACHUS. Thank you.
1434 Chairman GOODLATTE. The gentlewoman from California,
1435 Ms. Lofgren, is recognized for 5 minutes.
1436 Ms. LOFGREN. Well, thank you, Mr. Chairman.
1437 And thank you to all the witnesses for your appearance
1438 here today and for answering our questions.
1439 I would like to concur with many of the comments made by
1440 our colleague Mr. Sensenbrenner as to the surprise that many
1441 of us had at the interpretation of the word "relevant" in
1442 Section 215. I would like to explore -- we have talked a lot
1443 about the metadata for telephone records. But what I would
1444 like to explore with you, Mr. Cole, and perhaps others of you
1445 have an opinion, is not what is happening now, but what you
1446 believe the statute would authorize if, if the bulk
1447 collection of telephone data is relevant because there might
1448 be in that massive data information that would be useful for
1449 an investigation.

1450 What other tangible items would the statute authorize,
1451 not saying that we are doing this, the Government to collect?
1452 Would we be authorized to collect bulk credit card records,
1453 Mr. Cole?
1454 Mr. JAMES COLE. Ms. Lofgren, I think what you have to
1455 look at, which is a very important part of the analysis that
1456 Judge Eagan described, I thought, quite well, is that it's
1457 not everything. It's what is necessary to gather the
1458 relevant information.
1459 Ms. LOFGREN. Well, let me -- let me -- what we are
1460 trying to explore here is really the role of the Government
1461 versus the citizen.
1462 Mr. JAMES COLE. Correct.
1463 Ms. LOFGREN. And if you can compile the record of every
1464 communication between every American because within that
1465 massive data there might be something useful to keep us safe,
1466 I am trying to explore with you, if that is your reading of
1467 Section 215 vis-a-vis metadata and the phone company, would
1468 that include cookies?
1469 Mr. JAMES COLE. Cookies?
1470 Ms. LOFGREN. Yes. Could it?
1471 Mr. JAMES COLE. Again, I think the issue here really is
1472 under 215 with telephony metadata, the issue that was
1473 presented to the court was we needed the connections from one
1474 phone number to another.

1475 Ms. LOFGREN. Okay. Well, let me --
1476 Mr. JAMES COLE. And so, that was necessary. In a
1477 credit situation --
1478 Ms. LOFGREN. Let me ask you ask you this. Let me go to
1479 Mr. Swire because you are clearly not going to address this
1480 issue.
1481 Mr. JAMES COLE. I'm trying to, Congresswoman.
1482 Ms. LOFGREN. I think you are trying to use up my time.
1483 The -- if relevance allows for the collection of mass data
1484 because within that haystack, to use General Alexander's
1485 words, there is the needle, would 215, under that reading of
1486 the act, allow for the collection of all the photos taken at
1487 ATM machines, all the cookies selected by commercial
1488 providers?
1489 We have special standards for records of gun sales and
1490 credit card records, but it doesn't preclude their selection.
1491 Did your group look at that from a legal basis, not what we
1492 are actually doing?
1493 Mr. SWIRE. Well, we did not go through that list. But
1494 what I would observe is that a judge would have to make that
1495 decision. So the Department of Justice would need to go to
1496 the judge and say --
1497 Ms. LOFGREN. Right.
1498 Mr. SWIRE. -- we want ATM photographs for this reason,
1499 and the judge would have to say that it meets all the other

1500 standards for 215. So that's something beyond just the
1501 Justice Department on its own.
1502 Ms. LOFGREN. Right. Let me ask about NSLs because NSL,
1503 as I think Rich Clarke gave some very pointed comments about
1504 how many were collected, thousands each day, with no
1505 supervision whatsoever. And that is directed to electronic
1506 communications.
1507 Could you under the Section I think, what is it, 502, do
1508 mass collection under 502? It doesn't seem to be precluded
1509 as --
1510 Mr. SWIRE. So I'm not remembering the section. Under
1511 NSLs, we were not aware of bulk collection under NSLs.
1512 Ms. LOFGREN. I am not saying what is happening. Do you
1513 think it provides the legal authority to do so? It is not
1514 precluded.
1515 Mr. SWIRE. I haven't -- I haven't seen a theory under
1516 which the NSL authority could be used in that bulk way. I'm
1517 not aware of such a document that would --
1518 Ms. LOFGREN. All right. What about 702, and do you
1519 think that 702 provides the legal authority for bulk
1520 collection?
1521 Mr. SWIRE. 702, that partly depends on your idea of
1522 bulk. 702 does allow targeting of people outside the United
1523 States and allows content and allows accumulation of allotted
1524 data about those individuals and the people they're in

1525 communication with.

1526 That, by itself, would not be the way that we'd have the

1527 entire database of everything that happens. It has to be

1528 targeted to an individual overseas.

1529 Ms. LOFGREN. Let me -- just a final question. Have the

1530 metadata of Senators and Members of Congress been collected?

1531 Mr. SWIRE. I'm not aware of any way that they're

1532 scrubbed out of the database. So whatever databases exist, I

1533 don't know why your phone calls would be screened out. We

1534 haven't heard any evidence -- I'm not aware of any evidence

1535 that that screening out happens.

1536 Chairman GOODLATTE. The time of the gentlewoman has

1537 expired.

1538 Ms. LOFGREN. My time has expired. Thank you.

1539 Chairman GOODLATTE. The chair recognizes the gentleman

1540 from California, Mr. Issa, for 5 minutes.

1541 Mr. ISSA. Thank you, Mr. Chairman.

1542 Following up on that, the gentlelady's question was do

1543 you collect? Your answer apparently is, yes, you do because

1544 you scrub everything. Is that correct?

1545 Mr. SWIRE. Is -- so --

1546 Mr. ISSA. You take it, yes?

1547 Mr. SWIRE. In terms of whether Members of Congress'

1548 records are collected, first of all, the names are not

1549 listed. It's based on phone numbers.

1550 Mr. ISSA. Well, no, but the simple question. 202-225
1551 and four digits. Do you collect it?
1552 Mr. SWIRE. At this point, I'm not the U.S. Government,
1553 and maybe --
1554 Mr. ISSA. Okay. Mr. Cole, do you collect 202-225 and
1555 four digits afterwards?
1556 Mr. JAMES COLE. Without going specifically, probably we
1557 do, Congressman.
1558 Mr. ISSA. So separation of powers, this is the --
1559 another branch. You gather the logs of Members of the House
1560 and Senate in their officials calls, including calls to James
1561 Rosen. Is that right?
1562 Mr. JAMES COLE. We're not allowed to look at any of
1563 those, however, unless we make a reasonable, articulable
1564 suspicion finding that that number is associated with a
1565 terrorist organization. So while they may be in the
1566 database, we can't look at any of those numbers under the
1567 court order without violating the court order.
1568 Mr. ISSA. Well, speaking of court orders, Mr. Rosen, is
1569 he, in fact, a criminal?
1570 Mr. JAMES COLE. Is he, in fact, a criminal?
1571 Mr. ISSA. Well, the Attorney General had said that
1572 James Rosen, a Fox reporter, you know, there was a wiretap
1573 placed on his family, he and his family. Correct? Not, and
1574 this was --

1575 Mr. JAMES COLE. No, there was not a wiretap, sir.
1576 Mr. ISSA. There wasn't? I am sorry. You collected
1577 personal emails. Let me get it correct.
1578 There was a warrant for -- there was a warrant for
1579 personal emails, but there was also the -- they wiretapped
1580 his family.
1581 Let me rephrase that. Let me go on, and I will come
1582 back to that because I want to make sure I get the
1583 terminology right.
1584 Do you screen executive branch numbers?
1585 Mr. JAMES COLE. We don't screen any numbers, as far as
1586 --
1587 Mr. ISSA. So you collect all numbers? The President's
1588 phone call log record is in the NSA database?
1589 Mr. JAMES COLE. I believe every phone number that is
1590 with the providers that get those orders comes in under the
1591 scope of that order.
1592 Mr. ISSA. Would you get back to us for the record as to
1593 whether all phone calls of the executive branch, including
1594 the President, are in those logs?
1595 Mr. JAMES COLE. Be happy to get that back to you,
1596 Congressman.
1597 Mr. ISSA. Okay. Especially if he calls Chancellor
1598 Merkel, it would be good to know.
1599 The freedom of association is a basic constitutional

1600 right, wouldn't you agree, Mr. Cole?

1601 Mr. JAMES COLE. Yes, it is.

1602 Mr. ISSA. And if you are looking at our associations,

1603 and then if we have associations with somebody that you

1604 believe is "a terrorist," then you take the next step, right?

1605 Mr. JAMES COLE. Well, we don't look at your

1606 associations, Congressman.

1607 Mr. ISSA. Well, what does the metadata do if it is not

1608 --

1609 Mr. JAMES COLE. We don't look at the metadata unless we

1610 have a reasonable, articulable suspicion that the specific

1611 phone number we want to query is associated with terrorists.

1612 That's the only way we can get into that metadata.

1613 Mr. ISSA. Do you -- you collect the phone number

1614 metadata of all embassies here in Washington, all the foreign

1615 embassies?

1616 Mr. JAMES COLE. I believe we would. Again, we don't

1617 screen anything out, to my knowledge. But that's something

1618 that NSA would know. My understanding is we don't screen

1619 anything.

1620 Mr. ISSA. And they have conversations with large

1621 amounts of numbers back in their home countries, right?

1622 Mr. JAMES COLE. All the telephone numbers have large

1623 amounts of conversations with lots of other telephone

1624 numbers. We don't look at them unless we have that

1625 reasonable, articulable suspicion for a specific --
1626 Mr. ISSA. But isn't it true that the reasonable,
1627 articulable suspicion goes a little like this? I talk to
1628 somebody in Lebanon, who talks to somebody in Lebanon, who
1629 talks to somebody in Lebanon, who talks to somebody in
1630 Lebanon, who talks to somebody in Lebanon.
1631 If you gather all that data, then I have talked to
1632 somebody who has indirectly talked to a terrorist. Isn't
1633 that right?
1634 Mr. JAMES COLE. That's not how it would work,
1635 Congressman, no.
1636 Mr. ISSA. How do I know that? How do I know that a
1637 12-step removed, somebody talked to somebody, who talked to
1638 somebody, who talked to somebody, who talked to somebody who
1639 is on the list wouldn't occur? And I will just give you an
1640 example.
1641 The Deputy Prime Minister of Lebanon at one time gave
1642 $10,000 to a group associated with a Hezbollah element. If I
1643 called the Deputy Prime Minister, which I did, from my
1644 office, wouldn't I have talked to somebody who was under
1645 suspicion of being connected to a terrorist organization?
1646 The answer, by the way, is yes. But go ahead and give
1647 yours.
1648 Mr. JAMES COLE. Well, we wouldn't be querying your
1649 phone number, Congressman, unless we had evidence that you

1650 were, in fact, involved with a terrorist organization.
1651 That's the requirement under the court order --
1652 Mr. ISSA. But you would query the Deputy Prime
1653 Minister, who had made a contribution and was under
1654 suspicion, right?
1655 Mr. JAMES COLE. If we queried his phone number, we
1656 might find that connection.
1657 Mr. ISSA. And at that point, you would have a
1658 connection between somebody who you had a warrant for and me.
1659 So you could have a warrant for me. Is that right?
1660 Mr. JAMES COLE. Well, I do not think we would
1661 necessarily have enough to have a warrant for you with just
1662 that one phone call, Congressman. That is not how it works.
1663 Again, there are a lot of restrictions in those court orders
1664 and in the rest of the law as to what we can do, and we can
1665 get warrants for, and what we cannot get warrants for.
1666 Mr. ISSA. Well, we will follow up with the James Rosen
1667 thing later. Thank you. I yield back.
1668 Chairman GOODLATTE. The chair recognizes the
1669 gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.
1670 Ms. JACKSON LEE. Let me thank the chair and the ranking
1671 member for someone who was here, as a number of other
1672 members, in the aftermath of 9/11 and the intensity of
1673 writing the Patriot Act that came out of this committee in a
1674 bipartisan approach. Ultimately it did not reach the floor

1675 of the House in that way.

1676 As I try to recollect, I do not remember testimony that
1677 contributes to the massive data collecting that we have now
1678 wound up with. So I will pose as quickly as I can a series
1679 of questions. And, first, thank everyone for their service.
1680 It is good to see you, General Cole, and all of the other
1681 witnesses, the head of the Privacy and Oversight Board, and
1682 Mr. Swire as well. We thank you.

1683 Quickly, you have been, I think, a lifer to a certain
1684 extent, working for United States justice and the United
1685 States of America. Again, we thank you. Did you all have an
1686 immediate interpretation of mega collecting under the final
1687 passage of the Patriot Act? Was that what first came to
1688 mind?

1689 Mr. JAMES COLE. I was not in the government at the time
1690 the Patriot Act was passed, so I can honestly tell you I did
1691 not really think about it at that moment.

1692 Ms. JACKSON LEE. As you proceeded to be in government
1693 and as you have continued in service now and over these past
1694 couple of years, was that a firm conclusion that you could
1695 gather everything?

1696 Mr. JAMES COLE. As I became aware of what was being
1697 done under 215, and looking at the prior court precedents
1698 that came out that it had been approved and the descriptions
1699 of it, and some of the notices that were given to Congress, I

1700 was of the view that it was lawfully authorized under the
1701 Patriot Act and under 215.
1702 Ms. JACKSON LEE. Well, you are as well required to
1703 follow the law, but I note that justice is in the U.S.
1704 Department of Justice, and what you are suggesting is that no
1705 lawyers as far as you know may have gathered to say that this
1706 may be extreme?
1707 Mr. JAMES COLE. I am not aware of anybody saying that
1708 at the time, but again, I was not in the Justice Department
1709 at the time.
1710 Ms. JACKSON LEE. Not at that time. I am coming forward
1711 now in the time that you have been in the Justice Department.
1712 Mr. JAMES COLE. As far as the legal basis, I think
1713 everyone that I have talked to has been comfortable with the
1714 legal basis.
1715 Ms. JACKSON LEE. So as you have listened to members of
1716 Congress, what is your commitment to coming back to us,
1717 working with the Department of Justice to address and to help
1718 change what we are presently dealing with?
1719 Mr. JAMES COLE. Well, I can tell you is that the
1720 President's commitment, and we work for the President, and we
1721 are there to fulfill that commitment to try and change 215 on
1722 the telephony metadata as we know it and find another way
1723 where the government does not hold --
1724 Ms. JACKSON LEE. So you have a commitment based upon

1725 the President's representation to come back and look at a
1726 better way of handling the trolling of Americans' data that
1727 may not be relevant.
1728 Mr. JAMES COLE. We are looking for another way that
1729 will accomplish what we have been accomplishing under 215 as
1730 best we can and not involve the government holding the
1731 metadata.
1732 Chairman GOODLATTE. You may want to use an adjoining
1733 microphone if you can get to one.
1734 Ms. JACKSON LEE. Can you all hear me?
1735 VOICE. No.
1736 Ms. JACKSON LEE. You cannot hear?
1737 VOICE. No, we cannot hear. We cannot hear.
1738 Ms. JACKSON LEE. Testing, testing. Can you hear me
1739 now? Thank you. That is what happens when you start
1740 trolling and collecting data.
1741 [Laughter.]
1742 Ms. JACKSON LEE. I am sorry. Mr. Chairman, will I be
1743 indulged my time? Thank you.
1744 Chairman GOODLATTE. No.
1745 [Laughter.]
1746 Ms. JACKSON LEE. I did not hear that.
1747 [Laughter.]
1748 Ms. JACKSON LEE. Please indulge me, Mr. Chairman.
1749 Technological troubles here.

1750 In the report, there was a comment, "The idea of
1751 balancing has an element of truth, but it is also inadequate
1752 and misleading." Mr. Swire, when we are talking about
1753 security and privacy, what do you think that means? And I am
1754 going to go ahead to my good friend over the Oversight Board,
1755 Mr. Medine. Thank you very much. I think it is going to be
1756 in your hands to be as aggressive as you possibly can be, and
1757 I want you to give me your interpretation of two things: the
1758 question of relevance and the question of the importance of
1759 having an advocacy for the people in the FISA Court. Mr.
1760 Swire?
1761 Mr. SWIRE. The review group supported having an
1762 advocate, exactly. Had to have amicus versus party, so there
1763 are some tricky legal issues. And we did not make a legal
1764 decision about our view on the word "relevance."
1765 Chairman GOODLATTE. Without objection, the gentlewoman
1766 will be granted an additional minute on her time.
1767 Ms. JACKSON LEE. Thank you. Mr. Medine, could you
1768 answer the question as extensively as you can on that? Thank
1769 you, and thank you for your service.
1770 Mr. MEDINE. You are welcome. Nice to see you again.
1771 On relevance, again, the majority of the board is concerned
1772 about the almost unlimited scope of relevance, and I think
1773 that we have heard questioning earlier today that it
1774 encompasses members of Congress, the executive branch, and

1775 also dissidents, and protestors, and religious organizations.
1776 And so we think that it is written too broadly under this
1777 program, and there should be much more targeted requests for
1778 information, which can be legitimately done without the need
1779 to gather information. Right now, relevance is almost
1780 whatever the government can pull in and analyze as the scope
1781 of relevance. And we think that there needs to be a narrower
1782 concept to protect privacy and civil liberties.
1783 I mean, with regard to having an advocate in the Foreign
1784 Intelligence Surveillance Court, I think it is critical that
1785 there be another voice to respond to the government. As Mr.
1786 Swire mentioned earlier, if all the briefing that we have
1787 done on this program could have been presented to the Court,
1788 the Court could have made a more balanced decision. It was
1789 only until 2013 that the Court issued its first opinion
1790 regarding the legality of this program. We think in the
1791 adversary process, the Court would have carefully considered
1792 all the arguments pro and con, rendered its decision. And we
1793 also recommend that there be an opportunity for appeal to the
1794 FISCR, which is the Court of Appeals, and ultimately to the
1795 Supreme Court to resolve these important statutory and
1796 constitutional issues.
1797 Ms. JACKSON LEE. Let me just indicate that in addition
1798 as an aside, the President put on the record that he thought
1799 that we needed to haul in, from another perspective, the

1800 contractors dealing with the vetting of all those who work in
1801 this area just as a protection. If we are so interested in
1802 trolling Americans, we need to also make sure that our
1803 contractors or our workers in the intelligence are fully
1804 vetted. Just in your own mindset, do you think the
1805 government can handle its vetting and narrow the sort of
1806 outside contractors that are doing that now?
1807 Chairman GOODLATTE. The time of the gentlewoman has
1808 expired. The gentleman will be allowed to answer the
1809 question.
1810 Mr. MEDINE. And actually with due respect, that is not
1811 on our board's domain, but, I mean, maybe the deputy attorney
1812 general might be able to address that.
1813 Chairman GOODLATTE. Mr. Cole?
1814 Mr. JAMES COLE. I am sorry, could you repeat the
1815 question?
1816 Ms. JACKSON LEE. The President indicated that maybe we
1817 should reduce our outside contractors that are vetting those
1818 who have access to our security data. Would you be also in
1819 agreement with that approach?
1820 Mr. JAMES COLE. I think we need to make sure that we
1821 take care of the insider threat. That has been something the
1822 President has talked about. We need to make sure that people
1823 who work for the government are suitable and have been vetted
1824 properly. We have always thought that from both a cost

1825 perspective and a security perspective, the more we can
1826 reduce contractors the better. But as we hire contractors,
1827 we hire employees as well. They just need to be vetted very
1828 well when they are given very sensitive and classified
1829 positions.

1830 Ms. JACKSON LEE. I thank the chairman, and I thank the
1831 witness. I yield back.

1832 Chairman GOODLATTE. The chair recognizes the gentleman
1833 from Virginia, Mr. Forbes, for 5 minutes.

1834 Mr. FORBES. Mr. Chairman, thank you, and, gentlemen,
1835 thank you so much for taking your time and your expertise to
1836 be here with us today.

1837 Mr. Cole, it is my understanding that the review group's
1838 recommendation was that the use of private organizations to
1839 collect and store bulk telephony metadata should be
1840 implemented only if expressly authorized by the Congress. My
1841 question to you is not for the word "should," but we have
1842 watched the President when he was all in on healthcare and
1843 promised us all we could keep our insurance if we wanted it.
1844 It later changed. We listened to his words say he could not
1845 change immigration laws without Congress. He changed. We
1846 listened to him about military force without congressional
1847 permission. He changed. We heard his State of the Union
1848 where he said he had a pen and he had a phone regardless of
1849 what Congress did.

1850 My question to you is, in your professional opinion, do
1851 you believe that the President of the United States has the
1852 authority to use private organizations to collect and store
1853 bulk telephony metadata without the express approval of the
1854 Congress of the United States?
1855 Mr. JAMES COLE. Congressman, that is an issue that is
1856 probably part of the mix that we are looking at --
1857 Mr. FORBES. My question to you is do you have it, and
1858 we have seen you kind of slide off of the answers to the
1859 questions today. I am not asking you what ultimately would
1860 be determined. I am talking about your professional opinion
1861 today sitting there, is it your professional opinion that the
1862 President has authority or does not have the authority?
1863 Mr. JAMES COLE. I am going to give you a lawyer's
1864 opinion.
1865 Mr. FORBES. That is what we hired you for.
1866 Mr. JAMES COLE. Okay. There may be ways we could find
1867 for him either through contract or executive order to do it.
1868 It could also be done through legislation. There may be a
1869 number of different ways that you can --
1870 Mr. FORBES. So then basically if this Congress wants to
1871 avoid that, we had better to get to work and expressly
1872 prohibit the President from doing that, because he could do
1873 that the same way he is threatening to do certain other
1874 things.

1875 Mr. JAMES COLE. I think the President has clearly
1876 indicated he is looking forward to working with Congress to
1877 achieve a lot of these things.
1878 Mr. FORBES. Yes, but he also said that "working" means
1879 if Congress does not do what he says, he has got the pen, he
1880 will do it anyway.
1881 Mr. Swire, if I could ask you, and I appreciate your
1882 comments about wanting to have specific and targeted
1883 collection, I believe, as opposed to bulk collection. Is
1884 that a fair representation?
1885 Mr. SWIRE. Our report emphasizes the usefulness of the
1886 targeted collection.
1887 Mr. FORBES. Mr. Swire, I represent a lot of people. We
1888 have a lot communications from groups in the country who
1889 believe that even with specific and targeted collection, they
1890 are concerned because they have seen what the IRS, the
1891 Justice Department, and other agencies have done in targeting
1892 conservative groups and individuals in the faith community.
1893 What would you suggest that we do to try to protect those
1894 groups, because it is not going to be much consolation to
1895 them to say we can do specific and targeted collection if
1896 they have seen that they have been specifically targeted
1897 already by this Administration. Any suggestions that your
1898 group might have for that?
1899 Mr. SWIRE. Well, we have a couple of statements or

1900 conclusions in our report that I think are relevant to that.
1901 One is we found no evidence that there was in these
1902 surveillance activities any political targeting of Americans.
1903 So this is not where they are picking phone numbers based on
1904 politics or faith groups or whatever, and that includes
1905 people with a lot of experience in the intelligence community
1906 who are on our group.
1907 And the second thing is we found a very substantial
1908 compliance effort, much of which has been built up over the
1909 last 4 or 5 years, and so, a very earnest effort to comply
1910 with these rules, and so, in both of those cases, not
1911 political targeting and following the rules. We were
1912 distinctly heartened by what we found as we went through our
1913 --
1914 Mr. FORBES. Well, let me ask you this because it is
1915 also my understanding that your group did not conclude that
1916 the Section 215 Bulk Telephony Metadata Collection Program
1917 had been operating illegally with respect to these statutes
1918 or the Constitution. You further found no allegations in the
1919 report of abuse of this authority by members of the law
1920 enforcement and intelligence community. You further found
1921 that there was no allegation that the National Security
1922 Letter Program operated illegally, that no allegation of
1923 misuse or abuse by the law enforcement or intelligence
1924 community was made in the report. And yet you made

1925 substantial recommendations to change them.

1926 So as to these groups who are very concerned about that,
1927 what would be your recommendations to protect the interests
1928 of those groups?

1929 Mr. SWIRE. Congressman, we were interested in
1930 traditional American checks and balances and having the
1931 different branches of government doing their jobs, and going
1932 forward having within the executive branch bulk collection
1933 held in secret without judicial or congressional
1934 participation in that. We thought that was not a good way to
1935 go. And so, for the bulk collection, we recommended being
1936 very skeptical of the bulk collection, and we recommended
1937 having judicial safeguards in instances where it went forward
1938 as a way to maintain these sorts of checks and balances.

1939 Mr. FORBES. Good. Mr. Chairman, thank you, and I yield
1940 back the balance of my time.

1941 Chairman GOODLATTE. The chair thanks the gentleman, and
1942 recognizes the gentleman from Tennessee, Mr. Cohen, for 5
1943 minutes.

1944 Mr. COHEN. Thank you, Mr. Chairman. Would it be
1945 improper for me to recognize the Delta Sigma Thetas, who are
1946 here today?

1947 Chairman GOODLATTE. I think it would be very proper.

1948 Mr. COHEN. Well, welcome. They are here and a great
1949 sorority that does a lot of good for our country. Thank you,

1950 Mr. Chairman.

1951 Mr. Cole, before we talk about the NSA, which is indeed
1952 the subject of this, I want to go to another subject and give
1953 you some praise. You recently spoke before the New York
1954 State Bar Association, and I was so encouraged by your
1955 speech. It was about criminal justice issues that relate to
1956 this committee as well.

1957 And you indicated that the President is open to using
1958 his commutation power in a much more manifest way than he has
1959 in the past. You called on attorneys to come forward and try
1960 to help people with clemency requests, and that notice will
1961 be given to individuals in prison maybe with mandatory
1962 minimums that are unjust, people who had no violence in their
1963 background, may be first-time offenders who were sentenced
1964 for long times who judges said, I hate this, but I have to.
1965 And you give them notice. I thank you for that. And you and
1966 the President deserve praise for this effort.

1967 It is my opinion that the President can leave a legacy
1968 for justice that could be unmatched if he used that power
1969 that you have discussed, and I am sure you have worked with
1970 him on, in a manifold way. There are thousands of people
1971 that need justice and should receive it, and this is probably
1972 the only way they can. I know he is waiting on the
1973 legislature, the Congress, to act. I think he should
1974 probably act on his own.

1975 The FISA Court is appointed entirely by the Chief
1976 Justice, and I have great regard for the Chief Justice. He
1977 and I are friends. But I do not know that that makes for a
1978 good balance of power on the FISA Court. His appointments,
1979 and it may just folks he kind of knows, but 10 of the 11
1980 judges who have been currently sitting were appointed by
1981 Republicans presidents. And it may just be how that
1982 happened, you know, but it could be that there is a certain
1983 ideological link there, and it should be changed.
1984 I would think that the FISA Court ought to have a wide
1985 expanse of ideology, and some people are more skeptical of
1986 the government's perspective and more inclined toward looking
1987 toward civil liberties. I do not know that we have that in
1988 that Court. Does it trouble you, Mr. Cole, that the Chief
1989 Justice names every single of those people?
1990 Mr. JAMES COLE. Congressman, I do not think it
1991 particularly troubles me. I think we have seen judges
1992 throughout the Court, and everyone that I have dealt with at
1993 the Court has just been straight down on the facts and the
1994 law, and making sure that they honored civil liberties. We
1995 have seen released any number of opinions of judges when
1996 there were compliance problems, and the judges coming down
1997 hard on the Justice Department and on NSA to make sure that
1998 we fix them, and to make sure that we protected people's
1999 privacy and people's civil liberties.

2000 So I think you have got a good group of judges that have
2001 been there over the years.
2002 Mr. COHEN. Let me ask you this. You said the judges
2003 down the line. Do they not almost unanimously agree? How
2004 many times have you seen a split opinion?
2005 Mr. JAMES COLE. Well, there is only one judge that
2006 looks at a FISA application, so you would not have the split.
2007 And what has been discussed any number of times is that we
2008 present these applications to the FISA Court. They go to the
2009 staff. They go to the judges. Sometimes the judges will
2010 kick them back, and they will say you need more information
2011 about this, or, I do not find you have met the standard on
2012 that. And sometimes we will provide more information, other
2013 times we will withdraw it.
2014 So the statistics of how many have been granted that
2015 were submitted are a little bit misleading because it does
2016 not take into account some of the dialogue that goes on
2017 between the Justice Department and the Court that results in
2018 the applications being withdrawn.
2019 Mr. COHEN. And they do not sit en banc?
2020 Mr. JAMES COLE. No. There is a review group, an
2021 appellate group, which is 3 judges, and they will sit as 3
2022 judges.
2023 Mr. COHEN. How often are they split?
2024 Mr. JAMES COLE. I would have to go back and look. I do

2025 not really know the statistics off the top of my head.

2026 Mr. COHEN. Would "rare" be a good term to apply to

2027 their outcomes?

2028 Mr. JAMES COLE. It might be, but I just do not know the

2029 statistics.

2030 Mr. COHEN. Did the President not come out for some type

2031 of change and think that maybe each of the judges should

2032 rotate and pick somebody?

2033 Mr. JAMES COLE. I think that is one of the things that

2034 has been proposed in some of the pieces of legislation. I

2035 think generally as long as we get good judges who are there

2036 and we do not inject politics into it, I think we are happy

2037 as long as we have got judges that are there, and that fully

2038 staff the --

2039 Mr. COHEN. I understand not getting politics in it, but

2040 the Pope is politics. I mean, everything is politics. The

2041 justices are politics. Would it be wrong if the

2042 congressional leaders, equal Democrat and Republican,

2043 suggested some people to the judges and they pick from that

2044 group so there would be more of a check and balance on the

2045 choices?

2046 Mr. JAMES COLE. I think there are any number of models

2047 that might be workable in this regard to try and find a way

2048 to staff that Court. We are more than happy to work with the

2049 Congress on trying to find good ways to do that.

2050 Mr. COHEN. Thank you. Thank you. I appreciate it, and
2051 I thank the chairman for his indulgence in recognizing the
2052 greatest group of ladies in red since the Biograph Theater.
2053 Chairman GOODLATTE. That is an interesting comparison.
2054 [Laughter.]
2055 Chairman GOODLATTE. The gentleman from Texas, Mr.
2056 Gohmert, is recognized for 5 minutes.
2057 Mr. GOHMERT. Thank you, Mr. Chairman, and I appreciate
2058 the witnesses being here. Mr. Cole, if you had been
2059 testifying in front of this committee back before Edward
2060 Snowden took the documents he did, and you were asked if it
2061 was possible that any contractor would be able to access and
2062 take the documents that we now know he did, based on your
2063 comment that nobody can access these documents without proper
2064 cause, back then you would have said nobody could access
2065 those documents without proper cause and authorization, would
2066 you not?
2067 Mr. JAMES COLE. I think what I was saying, Congressman,
2068 is under the law and the court order nobody is allowed to do
2069 that without violating the --
2070 Mr. GOHMERT. So you are making a distinction that it is
2071 possible that they could access those documents, just like
2072 Edward Snowden did, correct?
2073 Mr. JAMES COLE. Things are possible. You know, this is
2074 something that we would like to nail down, but exactly what

2075 --

2076 Mr. GOHMERT. Well, you answered my question on that.
2077 The answer, though, accurately would be that not only members
2078 of Congress, but anybody is subject to having that data
2079 looked at or accessed by someone who may not follow the law.
2080 But let me tell all of you witnesses, in my first term
2081 we went through the process of debating whether or not we
2082 were going to renew the Patriot Act, and 215 was of
2083 particular importance. And I asked the question, for
2084 example, you know, under 215 where it says -- here we go --
2085 that you would only access these documents to protect against
2086 international terrorism or clandestine intelligence
2087 activities. I said what is "clandestine intelligence
2088 activities," and I was assured that since we are talking
2089 about international terrorism, our intelligence activities
2090 have to do with foreigners, and we were assured that was the
2091 case. And Chairman Sensenbrenner at the time assured that he
2092 had been assured that that was the case, and that is why he
2093 was initially totally opposed to any more sunsets that I
2094 fought so hard for and we did finally get in here. And now
2095 we find out those representations were not accurate.
2096 And let me tell you something else that concerns me is,
2097 yes, I know the Constitution and the 4th Amendment does say
2098 that we have the right to be secure in our persons, houses,
2099 papers, and effects against unreasonable searches and

2100 seizures. And that is not to be violated, and no warrants
2101 are to be issued but upon probable cause supported by oath or
2102 affirmation, particularly describing places, persons, or
2103 things to be seized.
2104 And when we saw the copy of this order from the FISA
2105 Court, all those assurances from my terms as a freshman went
2106 out the window because you have a judge, based on this before
2107 the FISA Court, who just says give all call detail records,
2108 telephony metadata. And then it defines telephony metadata
2109 basically as everything that you would desire about
2110 information and calls being made.
2111 I cannot find in that order any particularity or any
2112 specificity as at least appellate courts have always
2113 required. So this causes me great concerns without regard
2114 for discussion about Snowden, the fact that we had
2115 information provided to us that were misrepresentations of
2116 what was being done by this government.
2117 So let me also ask, since we have been told repeatedly
2118 how critical this FISA ability under 215 is, we have been
2119 told that all of these different plots have been foiled. And
2120 when it comes right down to it, it appears it was basically a
2121 subway bombing, and there are articles that indicate that,
2122 well, gee, they intercepted some information, so they went
2123 back and got all the phone logs for communication. But you
2124 do not need FISA Court, you do not need 215 when you have

2125 probable cause from a terrorist, a known terrorist, calling
2126 an American citizen. You would be able to get a warrant for
2127 that, would you not? I ask all of you.
2128 Mr. JAMES COLE. Well, I think there are a couple of
2129 issues there.
2130 Mr. GOHMERT. Well, the question is, you would be able
2131 to get a warrant if you showed that a known foreign terrorist
2132 made calls to an American citizens. You could go in and get
2133 basically any court to grant a warrant to get those logs,
2134 could you not?
2135 Mr. JAMES COLE. It depends on whether you get it under
2136 FISA, in which case you would have to show that it was an
2137 agent of a foreign power or a terrorist or an intelligence
2138 --
2139 Mr. GOHMERT. That was part of my question, a known
2140 foreign terrorist.
2141 Mr. JAMES COLE. Right. You may well be able to do
2142 that.
2143 Mr. GOHMERT. Mr. Swire, do you think we could get that?
2144 Mr. SWIRE. Congressman, to date the courts have not
2145 held that that was a search, so they say there is not a 4th
2146 Amendment constitutional protection in the metadata. And we
2147 recommend --
2148 Mr. GOHMERT. In other words, you do not need 215 to get
2149 that, do you?

2150 Mr. SWIRE. Well, you need some statutory basis to
2151 require the companies to turn over the data, but it is not a
2152 constitutional protection. It is statutory right now.
2153 Chairman GOODLATTE. The time of the gentleman has
2154 expired.
2155 Mr. GOHMERT. If I could get an answer from our last
2156 witness.
2157 Mr. MEDINE. Again, we agree that under Supreme Court
2158 law there is not a constitutional 4th Amendment issue, but we
2159 also do believe this information could be obtained through
2160 other authorities or warrant, subpoena, or possibly national
2161 security --
2162 Mr. GOHMERT. Without 215?
2163 Mr. MEDINE. Yes.
2164 Mr. GOHMERT. Okay. Thank you very much.
2165 Mr. JAMES COLE. -- would only be required for the
2166 listening of the call, not for the data.
2167 Mr. GOHMERT. Thank you. I yield back.
2168 Chairman GOODLATTE. The chair recognizes the gentleman
2169 from Georgia, Mr. Johnson, for 5 minutes.
2170 Mr. JOHNSON. Thank you, Mr. Chairman. The revelation
2171 that U.S. intelligence agencies were collecting telephone and
2172 email metadata on foreign to domestic, domestic to foreign,
2173 as well as domestic to domestic communications caused an
2174 uproar. This disclosure has given rise to the suspicion that

2175 intel agencies have been spying on Americans. The intel
2176 community denies spying on Americans, and states that the
2177 purpose of the metadata collection is to protect Americans
2178 from terrorist attacks like 9/11.
2179 Now, in the wake of the death of Osama bin Laden, who
2180 was one of the 5 top leaders of Al-Qaeda, and, in fact, 4 of
2181 the 5 top leaders of Al-Qaeda, including Osama bin Laden, are
2182 no longer living. And Al-Qaeda has, thus, decentralized with
2183 affiliates worldwide acting independently to establish an
2184 Islamic state through violence. These groups all share a
2185 Salafi jihadist ideology, which is that violence is the only
2186 pathway to achieving a world governed by what Al-Qaeda calls
2187 true Islam. Those groups are working towards that goal.
2188 Given the nature of the Al-Qaeda threat, or actually the
2189 Salafi jihadist threat, given the nature of that threat, and
2190 also assuming that those organizations use cell phones, chat
2191 rooms, emails, Facebook, and Twitter to conduct their
2192 operations, do you believe that that the universal data
2193 collection by U.S. intel agencies has the potential to
2194 disrupt Al-Qaeda's operations throughout the world? And
2195 secondly, and I think we already have answers to this from
2196 two of you, is metadata actually private information, and, if
2197 so, who does the information belong to? Is it the customer
2198 or is the service provider? Starting with you, Mr. Cole.
2199 Mr. JAMES COLE. Congressman Johnson, I think that the

2200 215 program is a tool, and it is a tool that is helpful. It
2201 is not going to solve all the problems all on its own in
2202 finding terrorists. It is one piece of what we use as a
2203 number of tools to try and find terrorists before they attack
2204 the country. In and of itself, it has some utility, but I do
2205 not think we should overstate the utility of it, but it is
2206 helpful, and I think it is something that we have determined
2207 that we do not want to give up that capability because it is
2208 helpful.
2209 Mr. JOHNSON. All right. Let me go to --
2210 Mr. SWIRE. Congressman, yes. One of the major themes
2211 of our reports is that we have to use our communication
2212 system for multiple goals. We have to use it to capture
2213 dangerous people and find them. It is the same communication
2214 system we used for commerce and we use for free speech and
2215 all these other things.
2216 And so, our report tried to figure out ways to be really
2217 good at finding the threats and also protect these other
2218 goals. People are all struggling with how to build that, and
2219 it is a big challenge.
2220 Mr. MEDINE. Congressman, you raised the question about
2221 whether Americans were improperly being spied on. We did not
2222 find any evidence of that, but the mere fact that people
2223 believe that could affect their behavior, their association,
2224 their speech rights. And that is one of the major reasons we

2225 recommend, the majority of the board, to not continue the 215
2226 bulk collection program because there are other methods that
2227 are more particularized to gather this information without
2228 storing everyone's phone records.
2229 Mr. JOHNSON. How would that affect the ability of our
2230 intelligence agencies to protect Americans from a threat like
2231 9/11?
2232 Mr. MEDINE. The majority believes that the ability to
2233 collect this information could be transferred to the
2234 providers instead of maintained in a bulk collection and
2235 maintain the same level of efficiency.
2236 Mr. JOHNSON. Okay. What would cause the private
2237 providers to have adequate security as to who in their
2238 operations had access to the, for lack of a better term,
2239 private information, the private metadata? What are the
2240 consequences? What are the ramifications of that?
2241 Mr. MEDINE. Well, under current law, the Federal
2242 Communications Commission requires telephone providers to
2243 maintain those records for 18 months, and also maintain the
2244 security of that information. So that is current law, and
2245 that happens every day that the providers maintain that
2246 information. What we are saying is instead of having them
2247 dump all of their information into a government database, it
2248 should be kept with them and cleared with them on a case by
2249 case basis.

2250 Mr. JOHNSON. Anyone else?

2251 Mr. JAMES COLE. I think one important point, and it
2252 goes to a question Mr. Gohmert asked, is that there are lots
2253 of security protections in lots of different databases. You
2254 can get around them every now and again. You can get around
2255 them in a government database. You can get around them in a
2256 provider's database. People can hack in. We tried to put in
2257 protections and legal restrictions to prevent that from
2258 happening, but nothing is completely foolproof.

2259 Chairman GOODLATTE. The time of the gentleman has
2260 expired.

2261 Mr. JOHNSON. Thank you.

2262 Chairman GOODLATTE. The gentleman from Ohio, Mr.
2263 Jordan, is recognized for 5 minutes.

2264 Mr. JORDAN. Thank you, Mr. Chairman. Mr. Cole, are you
2265 familiar with the name Barbara Bosserman?

2266 Mr. JAMES COLE. I have heard that name, yes.

2267 Mr. JORDAN. Is she an attorney who works at the Justice
2268 Department?

2269 Mr. JAMES COLE. She is.

2270 Mr. JORDAN. And she is part of the team that is
2271 investigating the targeting of conservative groups by the
2272 Internal Revenue Service, is that correct?

2273 Mr. JAMES COLE. She is a member of that team.

2274 Mr. JORDAN. A member of that team. I would dispute

2275 that and say she is leading the team, but I will take your
2276 word for it. Now, in the last 5 days, Mr. Cole, you have
2277 sent me two letters, one January 30th, last week, one just
2278 yesterday, where we had invited Ms. Bosserman to come testify
2279 in front of the Oversight Committee, and you sent me two
2280 letters saying that she is not going to come. And I counted
2281 them up. In these two letters, I think it is 7 different
2282 times you say this is an ongoing investigation, and that is
2283 why Ms. Bosserman cannot come to our committee and testify.
2284 Do you recall those two letters you sent me, Mr. Cole?
2285 Mr. JAMES COLE. I do.
2286 Mr. JORDAN. Yes, and you signed both of them?
2287 Mr. JAMES COLE. I did.
2288 Mr. JORDAN. And you referenced many times ongoing an
2289 investigation?
2290 Mr. JAMES COLE. Yes, it is.
2291 Mr. JORDAN. So here is my question. How can the
2292 President of the United States go on TV on Superbowl Sunday
2293 and say that there is not a smidgen of corruption in this
2294 investigation, not a smidgen of corruption in the IRS with
2295 how they targeted conservative groups? How can he be so sure
2296 when it is an ongoing investigation, something you told me 7
2297 times in two letters in 5 days? How can the President make
2298 that statement?
2299 Mr. JAMES COLE. Congressman, I think you should

2300 probably address that question to the White House.

2301 Mr. JORDAN. Did you brief the President on the status

2302 of this investigation?

2303 Mr. JAMES COLE. I have not.

2304 Mr. JORDAN. Do you know if the Attorney General has

2305 briefed the President on the status of this investigation?

2306 Mr. JAMES COLE. Not that I am aware of.

2307 Mr. JORDAN. Do you know if Ms. Bosserman, part of this

2308 team, who is investigating the targeting of conservative

2309 groups, do you know if she has talked to the President?

2310 Mr. JAMES COLE. Generally, the Justice Department does

2311 not brief the White House on --

2312 Mr. JORDAN. So how is the President so sure?

2313 Mr. JAMES COLE. Congressman, I am not in a position to

2314 answer --

2315 Mr. JORDAN. He did not say I do not think there is,

2316 there probably is not, nothing seems to point that way. He

2317 said there is not a smidgen of corruption. He was emphatic.

2318 He was dogmatic. He knew for certain. And no one has

2319 briefed him?

2320 Mr. JAMES COLE. No one I am aware of, Congressman.

2321 Mr. JORDAN. So you know what I think, Mr. Cole? I

2322 mean, you know, just a country boy from Ohio. You know what

2323 I think? I think the President is so emphatic and he knows

2324 for certain because his person is running the investigation,

2325 because Ms. Bosserman gave $6,750 to the Obama campaign and
2326 to the Democratic National Committee, and she is heading up
2327 the investigation. I think the President is so confident
2328 because he knows who is leading the investigation. And that
2329 is a concern not just for me, and members of this committee,
2330 and members of the Oversight Committee, but, more
2331 importantly, the American people who have to deal with the
2332 IRS every single year. Does that raise any concerns with
2333 you, Mr. Cole?
2334 Mr. JAMES COLE. Congressman, Ms. Bosserman is a member
2335 of the team. She is not leading this investigation.
2336 Mr. JORDAN. How was the team picked?
2337 Mr. JAMES COLE. The team was assigned in normal course
2338 by career prosecutors. It includes the FBI, the IG for the
2339 --
2340 Mr. JORDAN. How many members are on the team? This is
2341 something the FBI has refused to answer for the last year
2342 because I have been asking the question. They have refused
2343 to meet with us. They initially said they were going to meet
2344 with us. Then they talked with lawyers of the Justice
2345 Department and they said, no, we are going to rescind that
2346 offer, Mr. Jordan. We are not going to come meet with you.
2347 So how was the team put together, and how many members are on
2348 the team?
2349 Mr. JAMES COLE. Congressman, off the top of my head, I

2350 have no idea how many members are on that team. And
2351 generally, we do not brief elected officials on ongoing
2352 investigations. That is a standard --
2353 Mr. JORDAN. But again, we are not asking for a full
2354 briefing. We understand it is ongoing. We would just like
2355 to know who is heading it up. How many agents have you
2356 assigned? How many lawyers have you assigned? Who is
2357 heading it up? If it is not Ms. Bosserman as I think it is,
2358 who actually does head it up?
2359 Mr. JOHNSON. Mr. Chairman, parliamentary inquiry,
2360 please?
2361 Chairman GOODLATTE. The gentleman will state his
2362 parliamentary inquiry.
2363 Mr. JOHNSON. Is it proper for a member of the committee
2364 to question a witness about a matter that is not relevant to
2365 the matter that the hearing has been noted for?
2366 Chairman GOODLATTE. It is proper, and it has been done
2367 many times before in this hearing, this committee.
2368 Mr. JORDAN. I would just point out --
2369 Chairman GOODLATTE. The gentleman will continue.
2370 Mr. JORDAN. Mr. Cole sent me two letters in the last 5
2371 days. It is a pretty important issue. And when you appoint
2372 someone or you assign someone who gave $6,750 to the very
2373 person who -- the President could be a potential target in
2374 this investigation, and yet the person leading the

2375 investigation gave $6,000 to his campaign? She has got a
2376 financial stake in an outcome, a specific outcome. And Mr.
2377 Cole says "normal course of duty." We have got 10,000
2378 lawyers at the Justice Department, and, oh, it just happened
2379 to work out that Ms. Bosserman heads up the team. Really?
2380 Mr. JAMES COLE. She is not heading up the team,
2381 Congressman. There are many people --
2382 Mr. JORDAN. It is not what the witnesses we have talked
2383 to have said. Mr. Cole said she asked all the questions when
2384 they have been interviewed.
2385 Mr. JAMES COLE. She is not the head of the team, and
2386 there are many people who will be making the decision as to
2387 what to do with this case based on the evidence, the facts,
2388 and the law, just like every single investigation the
2389 Department of Justice does.
2390 Mr. JORDAN. Okay. All I know is the President said --
2391 Mr. JAMES COLE. And including FBI agents --
2392 Mr. JORDAN. All I know is the President said there is
2393 not a smidgen of corruption.
2394 Mr. JAMES COLE. -- including eight --
2395 Mr. JORDAN. The President has already reached a
2396 decision.
2397 Mr. JAMES COLE. -- and the Inspector General's office.
2398 Mr. JORDAN. Mr. Chairman, if I could real quickly. I
2399 sent my letters to Ms. Bosserman. She did not write me back.

2400 You did, Mr. James Cole. Did you talk to her about coming
2401 to testify? Did you tell her not to come testify?
2402 Mr. JAMES COLE. I did not tell her not to testify.
2403 Mr. JORDAN. Did you have any conversation with Ms.
2404 Bosserman about the request I gave her to come testify in
2405 front of our committee?
2406 Mr. JAMES COLE. Congressman, there is a standard --
2407 Mr. JORDAN. No, no, I did not ask that. I said did you
2408 talk to Ms. Bosserman about that specific request I sent to
2409 her. My letter was to her, and I got responses back from
2410 you.
2411 Mr. JAMES COLE. And I am answering your question,
2412 Congressman. There is a very long-held policy in the
2413 Department of Justice that line attorneys are not subjected
2414 to the questioning by members of Congress.
2415 Mr. JORDAN. Did you ask her if she wanted to testify?
2416 Mr. JAMES COLE. If I may finish, Congressman, they are
2417 not subjected to questioning --
2418 Mr. JOHNSON. Regular order, Mr. Chairman.
2419 Mr. JAMES COLE. -- by members of Congress, and we do
2420 not send people up here to talk about ongoing investigations.
2421 We have done that in every Administration.
2422 Mr. JAMES COLE. But you are not answering my question.
2423 Answer my question.
2424 Chairman GOODLATTE. The time of the gentleman has

2425 expired. The gentleman may answer the question.

2426 Mr. JAMES COLE. I think I have answered it.

2427 Mr. JORDAN. I do not think you have.

2428 Chairman GOODLATTE. The chair recognizes the

2429 gentlewoman from California, Ms. Chu, for 5 minutes.

2430 Ms. CHU. Mr. Medine, the PCLOB's report urges Congress

2431 to enact legislation that would allow the FISA Court to seek

2432 independent views from the special advocates. These

2433 advocates would step in where there are matters involving

2434 interpretation of the scope of surveillance authorities or

2435 when broad collection programs are involved.

2436 The report stresses that the Court should have

2437 discretion as to when these advocates step in. But is it

2438 advisable for the Courts to have that discretion? Is it

2439 possible that the Courts may leave the advocates out of the

2440 process when such important questions are before them?

2441 Mr. MEDINE. First, we do think it is important for

2442 advocates to be involved in issues of new technology and new

2443 legal developments. In terms of how they get involved, our

2444 feeling was that there are cases where they should certainly

2445 obviously be involved in a novel program that is being

2446 proposed. But there may be other cases which may not seem as

2447 novel on its face, but the judge is aware of the facts and

2448 circumstances, and wants to bring them in as well.

2449 So we felt it was appropriate to give the judge

2450 discretion as to when to involve the advocate, but we also
2451 called for reporting. And under the Court rules, Rule 11,
2452 the government is required to indicate to the Court if it is
2453 making an application that involves a new technology or a new
2454 legal issue. And so, what we have asked is that there be
2455 reporting of every Rule 11 case and how many of those
2456 instances has a special advocate been appointed, and that way
2457 there can be oversight of the court process of appointment.
2458 But we do, again, think that it is appropriate for the
2459 judges to maintain some discretion.
2460 Ms. CHU. Would that report also include times when
2461 special advocates were not included, though?
2462 Mr. MEDINE. Right. How many times has Rule 11
2463 application been forwarded, and how many of those instances
2464 has an advocate been appointed or not appointed? So again,
2465 if it is a significant case, one would assume it is likely
2466 that they would be, but there will be accountability to the
2467 public by the Court as to when they make those appointments.
2468 Ms. CHU. Now, you also advocate for the ability of the
2469 special advocates to request appellate review of court
2470 rulings. Why did you recommend this, and how would this
2471 strengthen privacy protections?
2472 Mr. MEDINE. In our American judicial system, we have a
2473 process by which district judges get reviewed by appellate
2474 bodies and ultimately the Supreme Court. We think that works

2475 effectively to have a dispassionate review of 3 judges at the
2476 appellate level and the 9 justices at the Supreme Court. And
2477 we think that the FISA Court process would be improved by
2478 encouraging that development.
2479 And so, we would like to empower the advocate to bring
2480 to the FISA Court of Review, which is their appellate body,
2481 adverse decisions to the advocate and in favor of the
2482 government so that there could be greater review. Again,
2483 much as there would be in any case in the District Court
2484 system.
2485 Ms. CHU. Mr. Swire, many of us think that, of course,
2486 the language in the statute in which the Section 215 bulk
2487 collection of metadata is broad, but that the government's
2488 interpretation of the relevant standard is even broader. The
2489 review group proposed a standard that the Court may only
2490 issue a 215 order if the government has reasonable grounds to
2491 believe that the particular information sought is relevant to
2492 an authorized investigation. And like a subpoena, the order
2493 has reasonable and focused scope and breadth.
2494 Can you tell us how this standard would narrow the
2495 government's inquiry so we could protect the American public
2496 in terms of its privacy interests? And how is this standard
2497 an improvement?
2498 Mr. SWIRE. Well, one change is that it would be a judge
2499 involved, and that is something that President Obama has

2500 recently said they are going to work with the FISA Court to
2501 do. A next change is to try to have these narrowing of
2502 scopes so that the bulk collection by the government prior to
2503 judicial looking at it would not occur. So it would be a
2504 narrowing in that respect as well.

2505 Ms. CHU. Also, the review group recognizes that
2506 intelligence programs, some, should remain secret. But you
2507 are also proposing that a program should be kept secret from
2508 the American public only if the program serves a compelling
2509 governmental interest, and if the efficacy of the program
2510 would be substantially impaired if our enemies were to know
2511 of its existence.

2512 If this proposed standard were in existence today, would
2513 the government have been compelled to disclose Section 215
2514 bulk collection program? How is your standard an improvement
2515 over what we have today?

2516 Mr. SWIRE. Right. Well, our recommendation 11 talks
2517 about a compelling government interest, and there would be a
2518 process within the government. When that process happens, we
2519 emphasized having not only intelligence perspectives, but,
2520 for instance, economic perspectives, civil liberties
2521 perspectives, as part of a sort of comprehensive review.

2522 And I also note that on bulk collection, the President
2523 has asked John Podesta to lead a process for private and
2524 public sector bulk data which is supposed to come back with

2525 additional recommendations about bulk data within, I think,
2526 60 days.
2527 Ms. CHU. Thank you. I yield back.
2528 Chairman GOODLATTE. The time of the gentlewoman has
2529 expired. The chair recognizes the gentleman from Texas, Mr.
2530 Poe, for 5 minutes.
2531 Mr. POE. Thank you, Mr. Chairman. I have great
2532 concerns about this whole process. This is reminiscent to me
2533 of the old-fashioned star chamber where courts met in secret,
2534 issued their verdicts and edicts in secret. No one knew what
2535 happened until the sentence was carried out.
2536 I also spent some time in the Soviet Union when it was
2537 the Soviet Union. Everything I did and all the citizens did
2538 was spied on by the Soviets. And here we are in 2014 trying
2539 to justify what I think is spying on American citizens.
2540 Mr. Cole, I have a question for you, but I want to quote
2541 Mr. Medine in his testimony. He said, "Based on the
2542 information provided to the Board, including classified
2543 briefings and documentation, we have not identified a single
2544 instance involving a threat to the United States in which the
2545 program made a concrete difference in the outcome of a
2546 counterterrorism investigation." Mr. Cole, name one criminal
2547 case that has been filed based upon this vast surveillance
2548 and metadata collection.
2549 Mr. JAMES COLE. Congressman, I think there was one

2550 which was a material support case that was filed based on the
2551 215 metadata where we were able to identify someone. And
2552 again, as I have said, this is not --
2553 Mr. POE. Reclaiming my time, as you know our time is
2554 limited. So how many criminal cases have been filed based
2555 upon this massive seizure?
2556 Mr. JAMES COLE. Well, the criminal support statute is a
2557 criminal --
2558 Mr. POE. I understand. My question is how many.
2559 Mr. JAMES COLE. I do not know off the top of my head,
2560 Congressman.
2561 Mr. POE. There is one.
2562 Mr. JAMES COLE. There may be one.
2563 Mr. POE. There may be one. So we have this vast
2564 metadata collection on Americans, and the reason is, oh, we
2565 have to seize this information or we are going to all die
2566 because of terrorists. And you are telling me as a former
2567 prosecutor -- I am a former judge and prosecutor -- all this
2568 information has collected one criminal case, is that what you
2569 are saying, that you know of?
2570 Mr. JAMES COLE. Well, Congressman, the point of this is
2571 not necessarily to make criminal cases.
2572 Mr. POE. I am not asking you --
2573 Mr. JAMES COLE. The point of it is to gather
2574 intelligence.

2575 Mr. POE. Reclaiming my time. My question is, one
2576 criminal case. That is all you can show for criminal cases
2577 being filed against individuals, right?
2578 Mr. JAMES COLE. I think that is the correct number, but
2579 I would have to go back and check to be sure.
2580 Mr. POE. It may not even be one.
2581 Mr. JAMES COLE. The point of the statute is not to do
2582 criminal investigations. The point of the statute is to do
2583 foreign intelligence investigations.
2584 Mr. POE. But the collection is on American citizens.
2585 When a warrant is signed -- I signed a lot of warrants, 4th
2586 Amendment. You know, I actually believe in the 4th
2587 Amendment. A warrant is served. Police officers go out and
2588 investigate. They return the warrant, and it is filed as a
2589 public document in State courts and in Federal courts. But
2590 when collection on American citizens of their information,
2591 this is not made public to them. They never know that this
2592 information was seized from them, do they?
2593 Mr. JAMES COLE. Well, as I think even the PCLOB and the
2594 President's review group have noted, the 4th Amendment does
2595 not cover the collection of metadata under the current law.
2596 So it would not have those requirements.
2597 Mr. POE. I know that is the current law, but that is
2598 not my question. My question is, the information is seized
2599 from them. They do not know that their personal information

2600 was seized by the Federal government. They do not know that.
2601 They are not protected under our current statute under the
2602 Patriot Act. Is that correct or not?
2603 Mr. JAMES COLE. The information does not come from
2604 them. It comes from the companies that they have phone
2605 service with. And, no, they are not informed directly that
2606 that metadata from those phone companies has been collected.
2607 Mr. POE. Do you have a problem with that information
2608 being seized on Americans through a third party and Americans
2609 never know that that they are the subject to this metadata
2610 collection? I mean, do you have a personal problem with
2611 that, or do you think that is okay, the government ought to
2612 do that?
2613 Mr. JAMES COLE. These are the issues we grapple with
2614 every day, Congressman, as far as trying to do national
2615 security investigations and trying to protect people's civil
2616 liberties. And we take leads from the Court as to the scope
2617 of the 4th Amendment and where people's reasonable
2618 expectations of privacy are. And these are difficult lines
2619 to deal with, and just what we are doing right now is trying
2620 to find where that right line is.
2621 Mr. POE. Well, I think it is an invasion of personal
2622 privacy, and it is justified on the idea that we have got to
2623 capture these terrorists. And the evidence, based on what
2624 you have told me, is all of this collection has resulted in

2625 one bad guy having criminal charges filed him. I think that
2626 is a bit over reaching to justify this massive collection on
2627 individuals' personal privacy. That is just my opinion. I
2628 yield back to the chair.
2629 Chairman GOODLATTE. The chair thanks the gentleman, and
2630 recognizes the gentleman from Florida, Mr. Deutch, for 5
2631 minutes.
2632 Mr. DEUTCH. Thank you, Mr. Chairman. General Cole, I
2633 am going to come at the judge's line of questioning from a
2634 slightly different angle, but I think trying to get at the
2635 same point. In a September letter to NSA employees, General
2636 Alexander wrote that "The Agency has contributed to keeping
2637 the U.S. and its allies safe from 54 terrorist plots," and
2638 that 54 terrorist plots has been repeated on several
2639 occasions.
2640 Last week in testimony before the Senate, there were
2641 some officials from the Administration who suggested that
2642 terrorist plots thwarted is not the appropriate metric for
2643 evaluating the effectiveness of the program. And I would
2644 just like to understand has the argument changed, and if it
2645 has, why should we now apply a different metric to determine
2646 the success of this program if it is not criminal
2647 prosecutions and if it is not terrorist plots thwarted?
2648 Mr. JAMES COLE. A couple of things, Congressman. The
2649 54 number, as I recalled it, was both 702 and 215. And the

2650 bulk of it, frankly, was 702 coverage. And that is a very,
2651 very valuable program, and, frankly, probably more valuable
2652 than 215.
2653 215 has a use, and it has a number of different uses.
2654 They are not as dramatic as 702, but they provide pieces of a
2655 puzzle. They provide tips and leads that allow us to then go
2656 and investigate and then gather other information. And that
2657 is really the value of 215.
2658 Mr. DEUTCH. But even if that 54 number that had been
2659 used does not apply primarily to the 215 program, you are
2660 telling me that the notion of terrorist plots thwarted even
2661 as it applies to this program is not the metric we should be
2662 using.
2663 Mr. JAMES COLE. It is not the only metric. Certainly
2664 it is a great metric, but I do not think it is the only
2665 metric we should be using. I think if we are gaining
2666 evidence that is valuable to us in doing investigations that
2667 help keep the country safe, that is a valuable metric.
2668 Mr. DEUTCH. Right. And Mr. Medine had told us earlier
2669 in his testimony, their first recommendation was to end the
2670 215 program, and said that whatever successes you are
2671 referring to could have been replicated in other ways. Mr.
2672 Medine, is that right? And how could that have been
2673 accomplished?
2674 Mr. MEDINE. Well, there are other authorities -- grand

2675 jury subpoenas, search warrants, national security letters
2676 -- that allow for access to the information without the need
2677 to collect bulk records.
2678 Mr. DEUTCH. And would have accomplished all of the same
2679 things that the 215 program does successfully.
2680 Mr. MEDINE. Substantially. Even the material support
2681 we talked about, but in many other cases. We looked at a lot
2682 of different metrics and based our recommendations on that.
2683 Mr. DEUTCH. Right. And when we talked about the
2684 suggestions going forward, the idea of moving this
2685 information away from the government, Mr. Swire, you had said
2686 that when we are talking about metadata held by or the
2687 suggestion of metadata to be held by private providers or
2688 private third parties instead of by the government. And, Mr.
2689 Cole, I think you said people are thinking outside the box
2690 about how to store this information.
2691 My question is this. The metadata that is being
2692 collected that you are comfortable moving to the private
2693 parties puts that metadata, does it not, and here is what I
2694 am concerned about. It puts the metadata that Mr. Medine and
2695 others believes is unnecessary to gather because it does not
2696 accomplish what is necessary. We can do it in other ways
2697 without intruding on people's civil liberties. But if it is
2698 stored by private contractors, private parties, it is at risk
2699 then, is it not, of being stored with all of the other data,

2700 dramatically more intrusive personal data, that we turn over
2701 to private parties regularly when we go on the internet,
2702 regularly.
2703 It puts it in the same place with all of the information
2704 that we have been assured time and time again today this
2705 program does not do in terms of intruding on the specifics of
2706 our emails and the specifics of what we do on the internet,
2707 et cetera. It puts it all together. Why should that not be
2708 a concern of ours?
2709 Mr. SWIRE. Congressman, I think part of the question is
2710 are we creating extra risk as we shift things around --
2711 Mr. DEUTCH. Exactly right.
2712 Mr. SWIRE. -- and find ways to shift things around.
2713 When it comes to phone company telephone records, as has been
2714 mentioned earlier, the Federal Communications Commission
2715 already requires it to be there for 18 months. Phone
2716 companies have been holding phone company data for an awfully
2717 long time.
2718 Mr. DEUTCH. Right, and, no, I understand, and that
2719 point has been made earlier. But there was another
2720 suggestion made. I think one of your suggestions was that we
2721 may need to have some other party. We may need to look
2722 outside of the box. My concern is that we are creating more
2723 risk than already exists in the program that we do not even
2724 need.

2725 Mr. SWIRE. Right. And what we said, and our entire
2726 report is prefaced by a transmittal letter saying this is our
2727 best effort in the time we had to come up with things. And
2728 one of the suggestions we had was in addition to possibly the
2729 phone companies, maybe a private sector entity could hold
2730 this with the right sorts of safeguards, and that we should
2731 look for ways to transition.
2732 We did not say we had the magic answer. Each one of
2733 these has downsized. But we thought getting it away from a
2734 huge government database was a better way to go.
2735 Mr. DEUTCH. Right, to a private database where risks
2736 could be even greater than they already are. I appreciate
2737 it, and I appreciate all the witnesses being here. I yield
2738 back. Thank you.
2739 Chairman GOODLATTE. The chair thanks the gentleman, and
2740 recognizes the gentleman from Arizona, Mr. Franks, for 5
2741 minutes.
2742 Mr. FRANKS. Well, thank you, Mr. Chairman, and thank
2743 all of you for being here. You know, it occurs to me that
2744 this committee, the Judiciary Committee, has a unique role in
2745 Congress in the sense that it sort of epitomizes the entire
2746 purpose of government. Our job is to protect the lives and
2747 the constitutional rights of Americans. And sometimes it is
2748 difficult to make that balance work out right.
2749 You know, everyone on this committee, I believe, wants

2750 to try to do everything that we can to protect the national
2751 security, to protect the lives of American people. But we
2752 also want to protect their constitutional rights in that
2753 process, and that requires us to make a clear distinction on
2754 how we go about that to where we maximize both.
2755 And I just have to suggest to you, without trying to
2756 sound argumentative, that this Administration has made it
2757 very difficult for us, because as Mr. Deutch has said and
2758 others, we feel that we have been blatantly deceived on what
2759 some of these programs have done and what they did. And
2760 consequently, it is hard for us sometimes to come up with the
2761 kind of architecture for any policy because we simply do not
2762 trust the Administration to be forthright with American
2763 people or us. And at the same time, I want to do the right
2764 thing here.
2765 So let me just ask you this question, Deputy Attorney
2766 General Cole. The President has made several recommendations
2767 for changing these data collection programs, including ending
2768 outright the bulk collection program. And then the last time
2769 the authorities were up for renewal, then the Administration,
2770 after they had said this, came before us and asked us to
2771 renew them completely. Now, help me understand that. Help
2772 me understand the contradiction there.
2773 Mr. JAMES COLE. I do not believe it is a contradiction,
2774 Congressman. I think it is just an evolution as people come

2775 to the debate and try to figure out the best way to do it, as
2776 we get the recommendations from the PCLOB and the President's
2777 review group, as we look at the value of what we get from
2778 these programs. And I think what the President has said is
2779 he does believe that the 215 program is valuable, but he is
2780 trying to find ways and has charged us with trying to find
2781 ways to accomplish as much and most of what that gives in
2782 other ways that will cause less concern for the American
2783 people, legitimate concern that they have about what is being
2784 done.

2785 Despite all of the court restrictions that are put on,
2786 despite the fact that as both groups found, there has been no
2787 intentional abuse of any of this, it has been well regulated
2788 and well minded, and it has been reported to the courts and
2789 Congress and the executive branch. There is still a faith
2790 that we want to keep with the American people about making
2791 sure that they are satisfied we are doing everything we can
2792 do. So that is where we are. It is an evolution more than a
2793 contradiction.

2794 Mr. FRANKS. Attorney General Cole, I appreciate that.
2795 I just would suggest to you that the American people are
2796 clearly at odds with that understanding. They feel that they
2797 have been deceived, and I certainly cannot possibly come back
2798 to them and tell them they have not.

2799 But if I could shift gears and ask you, Mr. Medine, a

2800 question regarding 2315 that the Attorney General brought up.
2801 How can a bulk collection that potentially violates the 1st
2802 and 4th Amendments be potentially unconstitutional, but
2803 individual collection is not? Help me understand the
2804 dichotomy there. I mean, if as, you know, the majority
2805 suggests here that the bulk collection of telephony metadata
2806 under Section 215 is constitutionally unsound, would the same
2807 not be true for individual 215 orders?
2808 Mr. MEDINE. First, the board did not say that the bulk
2809 collection was unconstitutional. What we did say is there is
2810 a Supreme Court precedent, Smith v. Maryland, that says that
2811 records held by third parties are not entitled to 4th
2812 Amendment protection. But we have also looked at the Jones
2813 case involving GPS tracking and seen a potential trend,
2814 especially the voices of five justices, suggesting that this
2815 type of information was entitled to constitutional protection
2816 because of the breadth of its collection.
2817 So collecting information on hundreds of millions of
2818 Americans over an extended period of time is very different
2819 from collecting information on one person who may be a
2820 suspect for a short period of time. So we did not reach
2821 constitutional conclusion on that, but I think there is a
2822 distinction between those two scenarios.
2823 Mr. FRANKS. All right. Well, quickly, Judge Bates, who
2824 formerly sat on the FISC, recently wrote a letter objecting

2825 to the creation of a public advocate position, like Mr. Obama
2826 has suggested. He wrote that, "Given the nature of FISA
2827 proceedings, the participation of an advocate would neither
2828 create a truly adversarial process nor constructively assist
2829 the courts in assessing the facts."
2830 Attorney General Cole, I will ask you, do you agree with
2831 Judge Bates' conclusion and tell me why.
2832 Mr. JAMES COLE. Well, I think the history of the Court
2833 has been that it has functioned quite well, and that the
2834 judges have been very earnest about trying to look at both
2835 sides. But I think, again, as we have started to think
2836 through this, there may be instances where the Court could
2837 benefit from another point of view, not in every instance.
2838 And the instances may be quite infrequent. But there are
2839 those where we think that another perspective may be helpful
2840 to the Court in reaching its conclusions.
2841 Mr. FRANKS. Mr. Chairman, I am out of time. Thank you,
2842 sir.
2843 Chairman GOODLATTE. The chair thanks the gentleman, and
2844 recognizes the gentlewoman from Washington, Ms. DelBene, for
2845 5 minutes.
2846 Ms. DELBENE. Thank you, Mr. Chair, and thanks to all of
2847 you for being here today. Mr. Medine, I would like to talk
2848 about transparency and the impact of the Administration's
2849 step to allow technology companies to be able to provide

2850 greater disclosure about the number of government requests
2851 they receive.
2852 Just yesterday many companies took advantage of the
2853 agreement reached with the DoJ and have provided new
2854 information to the public, which I think is a welcomed
2855 development. Do you think legislation that allows companies
2856 to provide more details to the public would be helpful? In
2857 particular, can you talk about the distinction between what
2858 the agreement last week allows and what you believe should
2859 happen? I am also a co-sponsor of the USA Freedom Act, and
2860 we also outline recommendations there. And I would love your
2861 opinion on that.
2862 Mr. MEDINE. Our board's report recommends a number of
2863 areas where transparency could be greater so that there could
2864 be more public confidence in our intelligence programs, and
2865 so transparency with regard to the government's request to
2866 companies is certainly a part of that.
2867 What our board recommended is that companies be given an
2868 opportunity, in some cases a greater opportunity, to disclose
2869 government requests consistent with national security. And
2870 so, we have not had a chance to evaluate the arrangement that
2871 was struck with the Justice Department, but certainly it is a
2872 move in the right direction to allow the companies to make it
2873 clear what is collected and also to disabuse people,
2874 particularly overseas, that there is less collection going on

2875 than they think, which I think will actually help American
2876 businesses down the road. So we are very supportive in
2877 principle of doing this, but we have not examined the
2878 specifics of it.
2879 In terms of whether there is a need for legislation, I
2880 think we could evaluate how well the government struck its
2881 balance. But there are important national security concerns
2882 in reviewing information, and it is important to do it in the
2883 right way.
2884 Ms. DELBENE. Okay. We would be interested in your
2885 opinion on that after you have had a chance to look at it in
2886 more detail.
2887 Mr. Cole, you stated last week the Administration had
2888 determined that the public interest in disclosing this
2889 information now outweighs the national security concerns that
2890 required its classification. And, you know, my position is
2891 that even greater disclosure is warranted in order to restore
2892 the credibility and trust of the American in our government.
2893 But I want to focus one particular element of the
2894 transparency agreement announced last week. In the letter
2895 you shared with companies' general counsels last week
2896 outlining the terms of the agreement, you state that the
2897 government is able to designate a service or designate a new
2898 capability order, and thereby delay reporting on that service
2899 for 2 years. And I wondered what the criteria was that you

2900 would be using in making the decision of what a new
2901 capability would encompass.
2902 Mr. JAMES COLE. Well, I think the criteria is set out
2903 in the letter. It is a new platform or a service or a
2904 capability that we have not had before that would indeed be
2905 something new and that we would be, I think, going to the
2906 court and having it incorporated in the order. And so, it
2907 would be something where we have gained a new capability to
2908 intercept communications that we have not had before, so that
2909 if people are relying on our inability to be able to
2910 intercept that information -- terrorists and people like that
2911 -- that they will not all of a sudden see a spike if we come
2912 to adopt that view or that capability, and, no oh, I better
2913 get off this platform.
2914 Ms. DELBENE. But given that that is a rather vague
2915 definition of what a new capability is, because of a new
2916 version of what you are doing right now, how do we know that
2917 that is not going to be used in such a broad way that
2918 basically ends up preventing disclosure of a lot of
2919 information that otherwise is covered in the agreement?
2920 Mr. JAMES COLE. I believe there is an avenue for the
2921 companies to go to the Court and challenge that, and
2922 certainly come to the Justice Department and challenge that,
2923 and say it, in fact, is not a new capability. And we can try
2924 and work that through, and the Court could find that it is

2925 not.

2926 Ms. DELBENE. And why do you believe that there has to

2927 be such a caveat in the agreement at all?

2928 Mr. JAMES COLE. From a national security standpoint so

2929 that people who are comfortable communicating over a certain

2930 type of capability do not all of a sudden realize that we can

2931 now intercept that capability.

2932 Ms. DELBENE. But do have a specific example in mind

2933 from what --

2934 Mr. JAMES COLE. Nothing that I would want to talk about

2935 in an open hearing.

2936 Ms. DELBENE. Thank you, and I will yield back, Mr.

2937 Chair.

2938 Chairman GOODLATTE. The chair thanks the gentlewoman,

2939 and recognizes the gentleman from South Carolina, Mr. Gowdy,

2940 for 5 minutes.

2941 Mr. GOWDY. Thank you, Mr. Chairman. Mr. Chairman, I

2942 was going to pursue a line of questioning related to the

2943 balancing of constitutional principles, and two of them are

2944 at play here, national security and privacy. And then I was

2945 going to pursue a line of questioning related to the

2946 expectation of privacy and whether or not it can change with

2947 culture and technology. But two things happened, Mr.

2948 Chairman, on the long, arduous walk from your chair to mine.

2949 One was something my friend from Tennessee said,

2950 suggesting a link between appointing judges and how they
2951 rule. In fact, Mr. Chairman, our colleague from Tennessee
2952 said everything is politics, justices are politics. So I
2953 want to ask Mr. Swire, I am going to read you a list of
2954 names, and everybody on this list has at least two things in
2955 common, and I want you to see if you can guess what those two
2956 things are, okay?
2957 Mr. SWIRE. It is arduous for us, too, Congressman, but
2958 go ahead.
2959 Mr. GOWDY. David Souter, John Paul Stevens, Harry
2960 Blackmun, William Brennan, Earl Warren, and Anthony Kennedy.
2961 What do all of those justices have in common?
2962 Mr. SWIRE. I suspect you are pointing to the fact that
2963 they are Supreme Court justices nominated by Republican
2964 presidents.
2965 Mr. GOWDY. That is exactly what I am referring to. And
2966 what would be the second thing they have in common? Would
2967 you agree that they wildly underperformed if they were put
2968 there to pursue a conservative agenda?
2969 Mr. SWIRE. I am hesitant to say all these justices
2970 wildly underperformed on any criteria.
2971 Mr. GOWDY. You do not think Brennan wildly
2972 underperformed if we put him there to pursue a conservative
2973 agenda?
2974 Mr. SWIRE. I am sorry, which --

2975 Mr. GOWDY. Blackmun, Brennan. They cannot get you in
2976 trouble anymore.
2977 [Laughter.]
2978 Mr. GOWDY. Judges cannot take up for themselves, Mr.
2979 Chairman. They either cannot or will not. I just do not
2980 think it is appropriate to try to make links between who put
2981 somebody on the bench and how they are going to turn out
2982 because I just pointed to a half dozen that did not turn out
2983 the way we though they were going to turn out.
2984 The second thing that happened, Mr. Chairman, was Mr.
2985 Jordan's line of questions. Mr. Cole, I am not going to ask
2986 you about the IRS targeting scandal for two reasons. Number
2987 one, you cannot comment on it, and I know you cannot comment
2988 on it, so I am not going to put you in a position of having
2989 to repeatedly say you cannot comment on it. The second thing
2990 you cannot do is explain to us why the President said what he
2991 said Sunday. So because you cannot explain it any more than
2992 anyone can explain it, I am not going to ask you about it.
2993 I am going to ask you to do one thing, and you do not
2994 have to comment on it. I am just going to ask you to do one
2995 thing, prosecutor to prosecutor. I am going to ask you to
2996 consider, in my judgment, how seriously the President
2997 undermined the integrity of that investigation by what he
2998 said, "not a smidgen." Lay aside that is not a legal term,
2999 "not a smidgen" or scintilla of evidence to support

3000 corruption or criminality.

3001 This investigation is ongoing. I assume no conclusions
3002 have been reached, hence the word "ongoing." And for him to
3003 conclude that there is no evidence of criminality whatsoever
3004 in the midst of an investigation I think undermines the hard
3005 work that the men and woman of your Department do. And I do
3006 not expect you to comment. I do not want you to comment,
3007 other than I would ask you to consider anew appointing
3008 special counsel under the regulations. The special counsel
3009 of regulation say it is appropriate in extraordinary
3010 circumstances.

3011 What we have been discussing all day today is the
3012 extraordinary circumstance of whether can you target under
3013 the 4th Amendment. The IRS case is whether government has
3014 targeted people for the exercise of their 1st Amendment
3015 rights. So I do not think anyone would argue it is not
3016 extraordinary if there is an allegation that government is
3017 targeting someone.

3018 And the second part of the regulation speaks to the
3019 public interest. So I would just ask you to please
3020 respectfully reconsider in light of what was said Sunday
3021 night, which was there is nothing here, not a smidgen of
3022 criminality in the midst of an investigation that matters
3023 greatly to lots of people. The Chief Executive said move on.
3024 For no other reason than to protect the integrity of the

3025 justice system, which I know you care about and I care about,
3026 I would ask you respectfully to consider appointing someone
3027 as special counsel in light of what the President said Sunday
3028 night, because he seriously undermined the integrity, in my
3029 judgment, of what is an ongoing investigation. And with
3030 that, I will yield, Mr. Chair.
3031 Chairman GOODLATTE. The chair thanks the gentleman, and
3032 recognizes the gentleman from New York, Mr. Jeffries, for 5
3033 minutes.
3034 Mr. JEFFRIES. I thank the chair as well as the
3035 witnesses for your participation in today's hearing.
3036 Mr. Cole, I want to go over a few questions related to
3037 the relevancy standard. I recognize this may have been
3038 ground covered earlier in the hearing, but if you would just
3039 indulge me. They will be pretty brief.
3040 Since the passage of the Patriot Act, which I believe
3041 was done in late 2001, how many actual terrorist plots have
3042 been thwarted connected to the new tools made available to
3043 law enforcement pursuant to this act?
3044 Mr. JAMES COLE. Well, I do not think that 215 was
3045 around in the original version of the Patriot Act. That came
3046 some time later. I do not know the exact number.
3047 Mr. JEFFRIES. Right. I am asking about the overall
3048 Patriot Act.
3049 Mr. JAMES COLE. I do not know the exact number.

3050 Mr. JEFFRIES. Okay. Now, as it relates to the bulk
3051 collection of metadata allegedly authorized by 216 that came
3052 subsequent to the initial creation of the Patriot Act, how
3053 many terrorist plots can be directly linked to this bulk
3054 collection? Am I correct that the answer is zero?
3055 Mr. JAMES COLE. I think the question is directly
3056 linked. There are tips and there are leads that come from
3057 the 215 metadata as I have said a number of --
3058 Mr. JEFFRIES. Can you provide us with one example where
3059 a tip or a link actually led to the thwarting of a terrorist
3060 plot connected to this bulk collection?
3061 Mr. JAMES COLE. Well, alleged charges. It does not
3062 mean that there were not other tips and leads that led to
3063 further investigations that were valuable and helpful to the
3064 government.
3065 Mr. JEFFRIES. But it is fair to say there is no
3066 substantial connection between this bulk collection and the
3067 resolution or thwarting of any terrorist plot related to this
3068 particular authorization under 215, correct?
3069 Mr. JAMES COLE. I think that may be correct, but I
3070 think that that is not always the only standard that is used.
3071 Mr. JEFFRIES. Right. Now, you referenced that earlier
3072 in your testimony. Can you give an example to the American
3073 people to justify this bulk collection outside of its alleged
3074 relevance, given that there has been no evidence, not a

3075 scintilla of evidence, presented that it has been relevant to
3076 any terrorist investigation?
3077 Mr. JAMES COLE. Well, I think it is relevant in a
3078 couple of ways. One is to be able to rule out that there are
3079 connections within the United States from terrorist plots
3080 that may be starting outside the United States. So it is
3081 very valuable to be able to know that so we can direct our
3082 resources very much at the core of what we are trying to look
3083 for.
3084 Mr. JEFFRIES. Now, do you think that the current
3085 relevance standard is a robust one?
3086 Mr. JAMES COLE. I think the current relevance standard
3087 is one that is used in both criminal and civil law, and it is
3088 a very broad standard.
3089 Mr. JEFFRIES. It is a very permissive standard in terms
3090 of what the government has been able to get access to,
3091 correct?
3092 Mr. JAMES COLE. It is not unfettered. It has to be
3093 done in a way that is necessary. We cannot just take
3094 whatever we want any time we want for any purpose. We have
3095 to go to a court and justify the fact that we need this
3096 volume of records in order to find the specific things we are
3097 looking for under very restricted circumstances. And then
3098 the court has to say you have permission to do this.
3099 Mr. JEFFRIES. Right, but what is very troubling, and I

3100 would like to talk to Mr. Swire about this, it is my
3101 understanding that once that bulk collection has been
3102 obtained, that the standard of reasonable articulable
3103 suspicion as it currently exists is a decision made by a NSA
3104 supervisor, not by an independent member of the judiciary,
3105 correct?
3106 Mr. SWIRE. In the first instance, it is made by the
3107 analyst, and it is reviewed by a supervisor.
3108 Mr. JEFFRIES. Now, how is the Review Board proposing to
3109 change the absence of judicial consideration?
3110 Mr. SWIRE. As was true in 2009 when there were some
3111 difficulties with compliance, we recommended that it go to
3112 the FISA Court in individual instances for a judge to review.
3113 Mr. JEFFRIES. Are you saying in the first instance in
3114 terms of the authorization of bulk collection or subsequent
3115 collection to search the data there must be a judicial
3116 determination made?
3117 Mr. SWIRE. In this case, there is collection, and then
3118 there is reasonable articulable suspicion about some phone
3119 number. And at that point you would go to the judge and say,
3120 judge, here is our RAS, and here is why we think we should
3121 look at it.
3122 Mr. JEFFRIES. Okay. Now, as it relates to collection,
3123 there has been discussion and debate about which entity would
3124 be most appropriate, putting aside the question as to whether

3125 it is even proper for this information to be collected, and I
3126 think the jury is still out on that, and the balance of facts
3127 suggest that it is not. But assuming that this information
3128 is collected, I guess the proposals have included the private
3129 sector, telephone companies, and an independent third party
3130 yet to be identified. Has there been any consideration given
3131 to the judicial branch as a separate, but co-equal, branch of
3132 government independent from the executive creating the
3133 mechanism to retain this data given the fact that a judicial
3134 determination at some point is going to be made as to whether
3135 it should be searched?

3136 Mr. SWIRE. Yes. I am not aware of the judicial branch
3137 holding databases and running those except for their own
3138 court records. So that would be quite a different function
3139 than I think what we have seen previously

3140 Mr. JEFFRIES. Okay, thank you. I yield back.

3141 Chairman GOODLATTE. The chair thanks the gentleman, and
3142 recognizes the gentleman from Texas, Mr. Farenthold, for 5
3143 minutes.

3144 Mr. FARENTHOLD. Thank you, Mr. Chairman. Mr. Medine,
3145 you talked a little bit earlier in response to some questions
3146 about limited 4th Amendment protections for information held
3147 by third parties. I think a lot of that is what Section 215
3148 kind of bootstraps on. It gives the government broad
3149 authority to get a hold of that information.

3150 Just so the folks watching this and everybody
3151 understands, there is a difference between, like, if I have a
3152 file on my computer or if I have a file on something on a
3153 cloud storage. I have more privacy, correct, in what is on my
3154 computer, more protection.
3155 Mr. MEDINE. Under current Supreme Court law, that is
3156 right.
3157 Mr. FARENTHOLD. And the same would be true for
3158 something sent by postal mail. I would have more privacy
3159 than something sent by email. That is kind of more
3160 traditional. And I would assume that, you know, a canceled
3161 check that I have in my drawer is more protected than the
3162 bank record. Is that something you think most Americans
3163 understand the difference in this day and age about
3164 information that is held electronically or held by third
3165 parties? Do you think most Americans understand that it is
3166 basically fair game?
3167 Mr. MEDINE. I suspect that they do not, but I think the
3168 key thing here is that, as you say, technology has changed
3169 dramatically since the Supreme Court's decision in Smith v.
3170 Maryland, which is collecting a limited amount of information
3171 for one person over a short period of time as opposed to --
3172 Mr. FARENTHOLD. Our ability to gather information has
3173 changed. So the courts could revisit this, but is it also
3174 not appropriate that Congress could revisit this and say you

3175 actually do have a reasonable expectation of privacy in
3176 certain things?
3177 Mr. MEDINE. That is exactly what the majority of our
3178 board has recommended is that based upon our legal analysis
3179 of Section 215, our constitutional analysis, which we say is
3180 heading in the direction of adding protections, and also our
3181 balancing national security with privacy and civil liberties,
3182 we saw a great impact of this program on --
3183 Mr. FARENTHOLD. So let me just ask Mr. Cole, and I
3184 suspect I know the answer to this question. So if any of my
3185 information is held by a third party, do you see any
3186 substantial limitation on what Section 215 allows you guys to
3187 get?
3188 Mr. JAMES COLE. Yes, I see very significant limitations
3189 on what we could get being held by a third party.
3190 Mr. FARENTHOLD. All right. Let us just talk about some
3191 things that are probably held in bulk. We talked a lot about
3192 the metadata on telephone calls. Could geolocation data that
3193 is routinely reported back from cell phones be gathered?
3194 Mr. JAMES COLE. If there is a need, it may or it may
3195 not.
3196 Mr. FARENTHOLD. Bank records, credit card transactions,
3197 things like that?
3198 Mr. JAMES COLE. They may not be. It depends on whether
3199 there would be a need to show the connections where you would

3200 need the whole group --

3201 Mr. FARENTHOLD. But under the rationale that you get
3202 all telephone records, could that not be extended to say, all
3203 right, we need all credit card transaction records, or all
3204 geolocation data so we can go back and mine it after the
3205 fact, from what we hear from the folks to your left, is a
3206 very limitedly effective program.

3207 Mr. JAMES COLE. Well, we are not mining the data,
3208 Congressman. That is not something --

3209 Mr. FARENTHOLD. Or go back and searching it, I guess.

3210 Mr. JAMES COLE. Well, and we are searching only in a
3211 very limited way.

3212 Mr. FARENTHOLD. Right, but the same argument that says
3213 you can collect all the phone data, could the exact same
3214 argument not be used for any other sorts of data that are
3215 collected by businesses in bulk?

3216 Mr. JAMES COLE. Not necessarily because the phone data
3217 connects two different people, and you have to look at those
3218 two different sets of information.

3219 Mr. FARENTHOLD. Right. So the geolocation data does
3220 the same thing. I go --

3221 Mr. JAMES COLE. Not necessarily because it only focuses
3222 on one person and not --

3223 Mr. FARENTHOLD. Right. But if you got the geolocation
3224 data, you could get everybody who is within 150 feet of me by

3225 rather than searching the person's phone, you could search
3226 the law and where they are, and you could tell everybody
3227 who's in this room right now.
3228 Mr. JAMES COLE. But there may be other ways to go about
3229 that without collecting all of the data for every single cell
3230 tower in the United States.
3231 Mr. FARENTHOLD. Okay. But do you believe that it would
3232 be legal for you all to do that?
3233 Mr. JAMES COLE. Only if there was a need. The Court's
3234 rulings have really focused on the fact that there is a need
3235 under the facts and circumstances --
3236 Mr. FARENTHOLD. All right. I see I am almost out of
3237 time, and I wanted to follow up on something that came up in
3238 the Oversight and Government Reform Committee last week. Can
3239 you tell us whether the NSA is playing any role in
3240 identifying, assessing, or classifying information about
3241 security threats or vulnerabilities associated with the
3242 healthcare.gov website? Are you aware of anything?
3243 Mr. JAMES COLE. I am not aware of anything,
3244 Congressman. Nothing that I am aware of.
3245 Mr. FARENTHOLD. Thank you very much. I yield back.
3246 Chairman GOODLATTE. The chair thanks the gentleman and
3247 recognizes the gentleman from Rhode Island, Mr. Cicilline,
3248 for 5 minutes.
3249 Mr. CICILLINE. Thank you, Mr. Chairman. I thank you

3250 and the Ranking Member for the warm welcome, and I look
3251 forward to the work of this committee. Thank the witnesses
3252 for being here and for your testimony.
3253 I am, too, a proud sponsor of the USA Freedom Act and
3254 really associate myself with the remarks of my colleague, Mr.
3255 Sensenbrenner, and hope the urgency of action is clear to all
3256 of the witnesses and hopefully to our colleagues in the
3257 Congress.
3258 I share the view of many people that it is very
3259 difficult for me to understand how the existing statute
3260 authorizes this massive data collection of all Americans, and
3261 I am struggling to understand how that authorization is
3262 provided in the statute. But I want to ask a couple of very
3263 specific questions.
3264 One is I think there has been testimony from all three
3265 witnesses that there is not a lot of evidence, if any, that
3266 this action, this metadata data collection, has led to the
3267 interruption of a terrorist attack, but it has been useful in
3268 a variety of different ways. And since the private industry
3269 holds these records for 18 months, has anyone looked at in
3270 the instances it has been useful what the time period has
3271 been? Has it been beyond the 18 months? If we were to
3272 change that to 24 months, would we cover all of the useful
3273 moments and not have to have the government collecting any of
3274 this data? Does anyone know the answer to that?

3275 Mr. JAMES COLE. I think that is one of the factors that
3276 we are trying to look at to see how long you need the data
3277 for. This was one of the issues when the President said, and
3278 we talked about cutting it down to 3 years instead of 5 years
3279 for holding it, is one step. And we may look further to see
3280 what the right amount of time is.
3281 Mr. CICILLINE. So with respect to the information we
3282 have currently, the benefits of in these instances where it
3283 has been useful, we do not know what that time period has
3284 been.
3285 Mr. JAMES COLE. We are looking into that.
3286 Mr. CICILLINE. Okay. The second thing I want to ask
3287 is, you know, we have this very deeply held belief in this
3288 country that the key parts to our justice system or two of
3289 the key parts are an independent neutral magistrate or judge.
3290 The current system allows the queries to be made by
3291 decisions made by someone other than a judge. And one of
3292 those reforms that has been recommended is that a FISA Court
3293 judge make that determination as a result of hopefully some
3294 adversarial process so that arguments can be made on both
3295 sides. That seems a very common sense reform.
3296 I would like to ask your thoughts about the national
3297 security letters because it seems to me the same kind of
3298 information can be collected through the national security
3299 letters that do not require a judicial determination. And it

3300 would seem to me that that would be a fairly easy reform to
3301 implement that says these letters can broadly collect lots of
3302 information without any judicial determination that it is
3303 necessary or appropriate. Why not impose the same
3304 requirement? And I know, you know, the argument always is,
3305 oh, it is too much, you know. It will require lots of extra
3306 hours.
3307 Setting aside the fact that it will be a lot of work for
3308 some folks and that we are prepared to fund that, does it not
3309 make sense that we ensure that there is a judicial
3310 determination as to the propriety of the information sought
3311 that can be quite broad? And I would like all three of you
3312 to comment on that.
3313 Mr. JAMES COLE. First of all, you have to understand
3314 national security letters are not as broad as other things,
3315 other kinds of subpoenas, grand jury subpoenas, even
3316 administrative subpoenas under the Controlled Substances Act
3317 or 215 authorities. It is more limited. That being said, it
3318 is much like an administrative subpoena or a grand jury
3319 subpoena, which does not involve any prior judicial approval
3320 before they are issues. Any judicial involvement comes on
3321 the back end if people do not comply with it.
3322 And they are very routine. They are used --
3323 Mr. CICILLINE. But those grand juries -- excuse me for
3324 interrupting -- those grand jury subpoenas require the

3325 participation of grand jurors, of citizens, to make a
3326 determination --
3327 Mr. JAMES COLE. They do not issue them themselves.
3328 There usually can be just a blanket authority from the grand
3329 jury to go issue --
3330 Mr. CICILLINE. But it requires action of citizens to
3331 authorize it. In this case, the national security letters,
3332 there is no participation of citizens. It can be a NSA
3333 official that makes that determination with no either citizen
3334 participation or judicial participation.
3335 Mr. JAMES COLE. Actually grand jurors usually do not
3336 participate in the decision to issue a subpoena. They
3337 receive the evidence that comes as a result of it and
3338 consider it, but they do not usually get involved in the
3339 issuance of the subpoena. That is usually done by the
3340 prosecutor.
3341 Mr. CICILLINE. So is it your position that having a
3342 judicial determination of the national security letter
3343 request is not appropriate? Would that not provide
3344 additional protection against an intrusion into the privacy
3345 rights of citizens with a de minimis kind of intervention by
3346 a judicial officer?
3347 Mr. JAMES COLE. I do not think it would provide any
3348 significant protection against privacy invasions for
3349 citizens. There are still administrative subpoenas, grand

3350 jury subpoenas, lots of things like that that go well beyond
3351 what a national security letter can do. I do not see the
3352 point of it.
3353 Mr. CICILLINE. Mr. Swire?
3354 Mr. SWIRE. Our report came out in a different place,
3355 and we did recommend a judge. And in terms of the comparison
3356 with a grand jury subpoena, here are two differences that are
3357 not always stressed. One is that the NSLs stay secret under
3358 current law probably for 50 years, and that is very
3359 different. And the second way from what happens in a
3360 criminal investigation where if there is a problem with the
3361 investigation, the criminal defendant and his or her lawyer
3362 find out about it quickly, and that is a check on over reach.
3363 With NSLs, the person who is being looked at does not
3364 get that kind of notice, so you do not have a built in check
3365 against using it too much.
3366 Mr. MEDINE. Our board unanimously recommended that the
3367 RAS determinations, reasonable articulable suspicion,
3368 immediately go to the Court after the fact for judicial
3369 oversight of that program.
3370 Going forward, the only thing I would say is because we
3371 have not studied national security letters on our board as
3372 yet is to consider that we not make it a higher standard to
3373 collect counterterrorism information than we do in ordinary
3374 criminal cases, to look more broadly at overall how are these

3375 programs operating.

3376 Mr. CICILLINE. Thank you. I thank you, and I yield

3377 back.

3378 Chairman GOODLATTE. The chair recognizes the gentleman

3379 from North Carolina, Mr. Holding, for 5 minutes.

3380 Mr. HOLDING. Thank you, Mr. Chairman. Mr. Swire, with

3381 private parties holding metadata, what kind of liability do

3382 those private parties have for any misuse of the metadata?

3383 Mr. SWIRE. So a phone company today, if it is hacked

3384 into or if they turn it over when they are not supposed to

3385 turn it over?

3386 Mr. HOLDING. First, you know, if they are hacked into,

3387 I guess there would be some determination as to whether they

3388 have taken adequate steps to protect the data. So what

3389 liability do they have there? What liability do they have if

3390 they turn it over to the government, and for some reason the

3391 government misuses it? Are there any immunities that these

3392 third parties have?

3393 Mr. SWIRE. So there is not an immunity if they lack

3394 reasonable security. Most of them have privacy policies

3395 where they said they are going to use reasonable security

3396 measures. The Federal Trade Commission or the Federal

3397 Communications Commission could bring a case against it.

3398 Private tort suits have not succeeded mostly, but the

3399 government could come in.

3400 When it comes to the second part, I think that comes up
3401 with the scope of the immunity that Congress included in the
3402 law the last time around. I do not know all the contours of
3403 that, but it is quite immunity is my understanding.
3404 Mr. HOLDING. And, of course, if we set it up so these
3405 third parties are retaining this information for a longer
3406 period of time, I assume that they would want additional
3407 assurances of immunities.
3408 Mr. SWIRE. I predict they would want that, yes.
3409 Mr. HOLDING. Mr. Cole, you would certainly agree that
3410 we live in a dangerous world.
3411 Mr. JAMES COLE. I am sorry?
3412 Mr. HOLDING. We live in a dangerous world.
3413 Mr. JAMES COLE. Yes, we do.
3414 Mr. HOLDING. And the dangers are overseas, and they are
3415 at home.
3416 Mr. JAMES COLE. That is correct.
3417 Mr. HOLDING. There are plenty of people who wish us
3418 great harm. And in the years subsequent to 9/11, the danger
3419 may have changed, but I do not think the danger has
3420 diminished.
3421 Mr. JAMES COLE. That is correct.
3422 Mr. HOLDING. In fact, it may have increased.
3423 Mr. JAMES COLE. It has become different, and it has
3424 become a lot more difficult to detect.

3425 Mr. HOLDING. And you have mentioned several times and
3426 the other members have mentioned several times about the use
3427 of the metadata in 215. And, you know, some people pointed
3428 out that, you know, no criminal case has been brought, you
3429 know, on the basis of metadata queries. But you pointed out
3430 that it is a part of a fabric of an investigation. I would
3431 like to think of it as a mosaic when you are putting together
3432 an investigation, whether it is public corruption, or a
3433 sophisticated drug conspiracy, or indeed, you know, a
3434 terrorism investigation.
3435 I want to give you a few minutes to spin a hypothetical
3436 based on your experience as a prosecutor and as, you know,
3437 someone who oversees a lot of investigations, a hypothetical
3438 where the Section 215 metadata is used as a piece of that
3439 mosaic. And to give some context to the conversations, you
3440 know, that we have had back and forth, and kind of what that
3441 mosaic looks like.
3442 Mr. JAMES COLE. Well, obviously there is any number of
3443 different ways it could play out. But one possible scenario
3444 is you have reasonable articulable suspicion that a certain
3445 phone number is connected with a certain terrorist group, and
3446 you then inquire about it, and you see calls to and --
3447 Mr. HOLDING. Now let us back up a little bit. And how
3448 would you come about one of these telephone numbers?
3449 Mr. JAMES COLE. Well, that could be from any number of

3450 other sources of intelligence, and without going into too
3451 much detail, there is a lot of information that feeds in that
3452 helps inform how we come to those conclusions if there is, in
3453 fact, reasonable articulable suspicions. But it has to be
3454 documented. It is not just something that is floating in the
3455 air. It has to actually be written down so somebody can read
3456 it, look at. A supervisor can determine that, in fact, it is
3457 reasonable articulable suspicion, and authorize the inquiry
3458 to be made.

3459 At that point, we just have the phone number. We then
3460 look at who that phone number ~~is~~ has called, and we may see that has
3461 there are a number of calls to another number. At that
3462 point, we do not know who that is, but we may then give that
3463 information to the FBI. They may then through a national
3464 security letter or something else determine who that number
3465 belongs to. They may then be able to look at other holdings
3466 that they have and other information they have that indicates
3467 that that other number is, in fact, somebody that they have
3468 been investigating for terrorism. And then they start
3469 putting that together, and the investigation starts to
3470 blossom from there. That is one of the ways that this could
3471 play out.

3472 Mr. HOLDING. So the metadata may not be the smoking
3473 gun, but it certainly puts not only a piece of the mosaic,
3474 but it might be like the cement that kind of puts the mosaic

3475 together, hooks it to another part.

3476 Mr. JAMES COLE. It is tip or a lead. It starts the

3477 process going.

3478 Mr. HOLDING. Thank you. Mr. Chairman, I yield back.

3479 Chairman GOODLATTE. I thank the gentleman, and the

3480 chair recognizes the gentleman from Georgia, Mr. Collins, for

3481 5 minutes.

3482 Mr. COLLINS. Thank you, Mr. Chairman. I appreciate the

3483 time. And I am probably not going to spend the whole time

3484 because one of the things that I want to focus on here is

3485 probably the question, is I think from the sense -- Mr. Cole,

3486 you have been here many times, and we have had these

3487 conversations. Others have been here as well. Today the

3488 committee, especially Judiciary, reminds me more of a P90X

3489 workout. One side you are going hard for 5 minutes, and then

3490 the next time, whew, I rest for 5 minutes.

3491 [Laughter.]

3492 Mr. COLLINS. Hard for 5 minutes, rest for 5 minutes.

3493 And what happens here is you see a unilateral sort of

3494 discussion and understanding that what we have that nobody is

3495 comfortable with. They are not. They do not want to put our

3496 national security at risk. Nobody on this panel, nobody in

3497 this Congress, and many people in the country, they do not

3498 want to put -- but they are also very uncomfortable with the

3499 collection. They are very uncomfortable with the way it has

3500 been dripped out of this is what is happening now, this is
3501 what is happening now, 2 weeks later here is what is
3502 happening. By the way, we are now angry birds, you know.
3503 Whatever it is, it is just dripping out.
3504 And so, every time we begin to maybe put a hold on it,
3505 it becomes a deeper problem with another revelation, and some
3506 of that was definitely not intended. Some of that was leaked
3507 maliciously, and I recognize all that. And from my part of
3508 Georgia, people understand national security. They
3509 understand patriotism. That is not the problem. What they
3510 do not understand is a loss of trust in the government,
3511 frankly a loss of trust in this Administration, a loss of
3512 trust.
3513 So what I really would like to focus on just for a
3514 moment, and if you have a lot you want to say, great. If you
3515 do not, then that is okay. But I think we have discussed a
3516 lot of specific recommendations. We have talked about have
3517 you found out, have you showed it. The mosaic, as my dear
3518 friend from North Carolina talked about, about
3519 investigations. But mine goes back to an essential question
3520 that this Congress will have to ask, and I believe it is the
3521 only reason that the President came out and said we need to
3522 change this, we need to look at this, is because, frankly,
3523 the poll numbers are bad. You have been looking at this for
3524 5 years. You knew it for 5 years. And now it is, well, this

3525 is getting bad, we need to get ahead of this, let us show
3526 leadership, the whole crowd is up there, let me run in front
3527 and lead. The problem is trust.
3528 So my question as we look at this, no matter what
3529 recommendations may come here, and I have associated with
3530 many on both sides of the aisle of the problems that we have,
3531 is in my district and in many others, NSA has become not a
3532 three-letter word, but a four-letter word. It has become
3533 something that they just do not understand and they do not
3534 trust anymore.
3535 So my question is, no matter what recommendations we
3536 give -- any of you want to talk about it -- for just a
3537 moment, how do we restore that? And that is the basic
3538 question here. How do we restore trust?
3539 Mr. JAMES COLE. Congressman, I think you raise a very,
3540 very important point, which is trust. We come to this
3541 through years of both Republican and Democratic
3542 Administrations where the intelligence community has
3543 determined that it is appropriate to classify a lot of thins
3544 information that we are now talking about in open hearings.
3545 And they had a good faith determination at the time that it
3546 should be classified for the national security and safety of
3547 our country.
3548 It is out, and we are talking about it. And the
3549 American people deserve to have answers, and they deserve to

3550 have a level of transparency that makes them comfortable
3551 about these things. And I think that this Administration,
3552 quite frankly, has taken the bull by the horns, and these are
3553 not easy issues. These are not easy resolutions. These are
3554 not easy balances to find. But this Administration has gone
3555 very far in trying to be transparent, in trying to bring
3556 these programs back into line, in trying to balance how far
3557 we can go, how transparent we can be, how many civil
3558 liberties and privacy interests we have to respect, and how
3559 much of the national security side we have to respect, and
3560 where that balance is. And these are tough balances.
3561 You are not going to do it overnight. You are not going
3562 to sit there and say, oh, that is easy. Let us just go over
3563 and disclose all of this, or let us just not collect this
3564 information. These are things that if you do not collect it
3565 and something blows up, people are going to be very angry.
3566 But these are also things that if you do over collect, and
3567 you do over classify, and you do inhibit people's civil
3568 liberties, they are going to be upset about that, too. So we
3569 have to find that balance, and I wish it were easier, but it
3570 is not.
3571 Mr. COLLINS. And, look, I respect that, and you have
3572 been up here, and you are an advocate of what the
3573 Administration is doing, and I get that. But I think the
3574 trust factor is the biggest issue, and I think it was not

3575 grabbing the bull by the horns. I think it was grabbing a
3576 microphone and saying I will make you feel better, and I
3577 understand that. But at the same point, it does not go to
3578 the heart of the question. It does not go to that trust
3579 issue on how we in this Congress can explain that, and how
3580 the Administration can make it look more instead of a public
3581 appearance and we are going to PR, how we actually solve
3582 this.

3583 Look, I respect everyone. Thank you for being here.
3584 But that goes back to the real issue. This is a trust issue.
3585 We can do the recommendations, but we have got to get back
3586 to trust, and we just do not have that trust right now.

3587 Mr. Chairman, I yield back.

3588 Chairman GOODLATTE. The chair thanks the gentleman, and
3589 the chair thanks all of our witnesses on this first panel.
3590 You have taken a large number of questions, and we appreciate
3591 the input to the committee.

3592 I want to ask unanimous consent to place the following
3593 documents into the record: Annex A of the PCLOB report,
3594 separate statement of board member Rachel Brand; Annex B of
3595 the PCLOB report, separate statement of board member
3596 Elizabeth Collins Cook; comments of the judiciary on
3597 proposals regarding FISA; a letter written by the Honorable
3598 John D. Bates, director of the Administrative Office of the
3599 United States Courts on January 10, 2014; Presidential Policy

3600 Directive Number 28, the President's directive regarding
3601 signals intelligence issued January 17, 2014.
3602 [The information follows:]

3603 ********** COMMITTEE INSERT **********

3604 Chairman GOODLATTE. I want to thank all the members of
3605 the panel, and you are excused. And we will --
3606 Mr. NADLER. Mr. Chairman?
3607 Chairman GOODLATTE. Yes?
3608 Mr. NADLER. May I ask unanimous consent that we admit
3609 into the record the entirety of the PCLOB report since the
3610 dissenting views are going be --
3611 Chairman GOODLATTE. Without objection, that will be
3612 made a part of the record as well.
3613 [The information follows:]

3614 ********** COMMITTEE INSERT **********

3615 Mr. NADLER. Thank you.

3616 Chairman GOODLATTE. And we thank all of our panelists.

3617 Mr. JAMES COLE. Thank you, Mr. Chairman.

3618 Chairman GOODLATTE. And we will move onto to the next
3619 panel. We are expecting a vote soon, but we want to keep
3620 moving.

3621 [Pause.]

3622 Chairman GOODLATTE. We welcome our second panel today,
3623 and if all of you would please rise, we will begin by
3624 swearing you in.

3625 [Witnesses sworn.]

3626 Chairman GOODLATTE. Thank you very much. Let the
3627 record reflect that all of the witnesses answered in the
3628 affirmative.

3629 Our first witness of the second panel of witnesses is
3630 Mr. Steven G. Bradbury, an attorney at Dechert, LLP, here in
3631 Washington, D.C. Formerly, Mr. Bradbury headed the Office of
3632 Legal Counsel in the U.S. Department of Justice during the
3633 administration of George W. Bush, handling legal issues
3634 relating to the FISA court and the authorities of the
3635 National Security Agency.

3636 He served as a law clerk for Justice Clarence Thomas on
3637 the Supreme Court of the United States and for Judge James L.
3638 Buckley of the United States Court of Appeals for the D.C.
3639 Circuit. Mr. Bradbury is an alumnus of Stanford University

3640 and graduated from Michigan Law School.

3641 Our second witness is Mr. Dean C. Garfield, president
3642 and CEO of the Information Technology Industry Council, a
3643 global trade association that is a voice advocate and thought
3644 leader for the information and communications technology
3645 sector. Previously, Mr. Garfield served as executive vice
3646 president and chief strategic officer for the Motion Picture
3647 Association of America.

3648 Mr. Garfield is a regular contributor to the Huffington
3649 Post and has been featured in several national and
3650 international publications representing the ICT industry.
3651 Mr. Garfield holds degrees from Princeton University and New
3652 York University School of Law.

3653 Our third witness is Mr. David Cole, a professor of law
3654 at Georgetown University Law Center. He is also the legal
3655 affairs correspondent for The Nation and a regular
3656 contributor to the New York Review of Books. He is the
3657 author of seven books.

3658 Mr. Cole previously worked as a staff attorney for the
3659 Center for Constitutional Rights from 1985 to 1990 and has
3660 continued to litigate as a professor. He has litigated many
3661 constitutional cases in the Supreme Court. Mr. Cole received
3662 his bachelor's degree and law degree from Yale University.
3663 Mr. Cole has also received two honorary degrees and numerous
3664 awards for his human rights work.

3665 I want to thank you all for being here today. We ask
3666 that each of you summarize your testimony in 5 minutes or
3667 less, and to help you stay within that time, there is a
3668 timing light on your table. When the light turns from green
3669 to yellow, you will have 1 minute to conclude your testimony.
3670 When the light turns red, it signals the witness' 5 minutes
3671 have expired, but I think you all know that.
3672 And I thank you all. And we begin with Mr. Bradbury.
3673 Welcome.

3674 TESTIMONY OF STEVEN G. BRADBURY, DECHERT, LLP; DAVID D. COLE,
3675 GEORGETOWN UNIVERSITY LAW CENTER; AND DEAN GARFIELD,
3676 INFORMATION TECHNOLOGY INDUSTRY COUNCIL

3677 TESTIMONY OF STEVEN G. BRADBURY

3678 Mr. BRADBURY. Thank you, Mr. Chairman.
3679 The independent judges of the FISA court have repeatedly
3680 upheld the legality of the NSA programs, and the President
3681 has strongly affirmed that they remain necessary to protect
3682 the United States from foreign attack. While I welcomed the
3683 President's defense of the programs in his recent speech, I'm
3684 disappointed that he decided, evidently at the last minute,
3685 to pursue changes in the telephone metadata program
3686 recommended by his review group.
3687 The President wants to move the metadata into private
3688 hands. I don't believe that's workable, not without
3689 seriously affecting the operation of the program and creating
3690 new data privacy concerns.
3691 The current program allows NSA to combine data from
3692 multiple companies into a single, efficiently searchable
3693 database and preserve it for historical analysis. This
3694 database is among the most effective tools we have for

3695 detecting new connections with foreign terrorist
3696 organizations. Moving this database outside NSA would
3697 require ceding control to a private contractor, since no
3698 single phone company has the capacity to manage all the data.
3699 Putting a private contractor between NSA and the data
3700 would compromise the utility and responsiveness of this
3701 asset. It would also reduce the security of the data.
3702 Today, the database is kept locked down at Fort Mead, with
3703 access strictly limited by court order and stringent
3704 oversight. If it were outsourced to a contractor, the data
3705 would likely reside in a suburban office park on much less
3706 secure servers.
3707 It would be vulnerable to privacy breaches and cyber
3708 incursions from foreign governments and terrorist groups. It
3709 could be exposed to court-ordered discovery by litigants in
3710 civil lawsuits, and the contractor's employees would be much
3711 less subject to direct oversight by the executive branch, the
3712 FISA court, and Congress. Those are not desirable outcomes.
3713 The President also intends to require FISA court
3714 approval of the reasonable suspicion determinations before
3715 NSA could query the database. This change moves us back
3716 toward the pre-9/11 approach. It will inevitably hamper the
3717 speed and flexibility of the program, particularly if it
3718 requires separate court approval of each query, and it will
3719 place a substantial new burden on the FISA court. Requiring

3720 the involvement of lawyers and court filings will impose a
3721 legalistic bureaucracy on a judgment call more appropriately
3722 made in real time by intelligence analysts.
3723 Finally, the President ordered NSA not to analyze
3724 calling records out to the third hop from the seed number,
3725 something the NSA only does when there's a specific
3726 intelligence reason. Why should we needlessly forego these
3727 potentially important intelligence leads?
3728 Beyond the changes endorsed by the President, I urge
3729 this committee to reject most of the other major proposals
3730 for curtailing FISA. The most sweeping proposal would
3731 restrict the use of Section 215 to individual business
3732 records directly pertaining to a specific person.
3733 A similar proposal would limit NSA to conducting queries
3734 of the telephone calling records only while the data is
3735 retained by the companies in the ordinary course of business.
3736 These restrictions would kill the metadata program by
3737 denying NSA the broad field of data needed to conduct the
3738 necessary analysis.
3739 At the same time, denying NSA the ability to access
3740 metadata in bulk would preclude the historical analysis of
3741 terrorists' calling connections, which is among the most
3742 valuable capabilities of the 215 program. Any requirement to
3743 shorten the data retention period would degrade our ability
3744 to discover important historical connections.

3745 One further proposal would attempt to convert FISA into
3746 an adversary process by establishing some form of public
3747 advocate. This proposal would raise significant
3748 constitutional concerns, both if the President is required to
3749 share sensitive national security secrets with an adversary
3750 and if the public advocate were given the power to oppose
3751 each FISA application and to appeal a decision of the FISA
3752 court.

3753 Such an officer would lack the Article III standing
3754 necessary to initiate an appeal and would occupy a gray zone
3755 outside the three branch framework established in the
3756 Constitution.

3757 Instead of creating a formal office of public advocate,
3758 the President wants to set up a panel of pre-cleared outside
3759 advocates who could be called upon by the FISA judges to
3760 submit amicus briefs on significant questions. This proposal
3761 is less objectionable if it leaves to the FISA judges the
3762 decision to call for amicus input and preserves the
3763 President's discretion to decide whether the amicus gets
3764 access to classified information.

3765 Of course, any requirement that an outsider be granted
3766 access to the intelligence information available to the court
3767 will chill the executive branch's willingness to disclose the
3768 most sensitive details relevant to FISA applications. As the
3769 FISA judges recently pointed out, this disincentive would

3770 threaten the relationship of trust between the Justice
3771 Department and the FISA court, something this committee
3772 should strive to avoid.
3773 Many of these reforms, Mr. Chairman, run the risk of
3774 re-creating the type of cumbersome, overlawyered FISA regime
3775 that proved so inadequate in the wake of 9/11. If our Nation
3776 were attacked again, I am concerned that a future President
3777 may feel the need to fall back on Article III authority to
3778 conduct the surveillance necessary to protect the country,
3779 and I don't think any of us would like that outcome.
3780 Thank you very much.
3781 [The statement of Mr. Bradbury follows:]

3782 ********** INSERT 4 **********

3783 Chairman GOODLATTE. Thank you, Mr. Bradbury.
3784 Mr. Cole, welcome.

3785 TESTIMONY OF DAVID D. COLE

3786 Mr. DAVID COLE. Thank you, Mr. Chairman, Ranking
3787 Member, for inviting me here to testify.
3788 I want to make three brief points in my opening remarks.
3789 First, that technological advances employed by the NSA raise
3790 substantial privacy and liberty concerns and demand new legal
3791 responses if we are not going to forfeit our privacy by
3792 technological default. Second, that Congress is particularly
3793 well situated to adopt rules to protect Americans' privacy in
3794 the digital age. And third, that the USA FREEDOM Act,
3795 sponsored by Representative Sensenbrenner and Senator Leahy,
3796 is an excellent start toward restoring the privacy and the
3797 accountability that has been infringed by NSA practices.
3798 First, the NSA metadata program illustrates the profound
3799 threat to our privacy and to our associational freedoms
3800 brought on by the capabilities of the digital age. At the
3801 time of the framing or even 50 years ago, if the Government
3802 wanted to know what we read, what we listened to, who we
3803 spoke and associated with in the privacy of our home, they
3804 would have to get a warrant based upon probable cause.

3805 Today, virtually everything we do in the home and out,
3806 including what we read, with whom we associate, where we go,
3807 and even what we are thinking about leaves a digital trace
3808 that reveals the most personal details of our lives.
3809 According to the administration's interpretation of
3810 Section 215, there is no limit on the Government getting
3811 these digital details of our lives, whether they be phone
3812 records or email records or Internet browsing data records or
3813 business or bank records. There is no limit on their ability
3814 to get them because they might at some point be useful to
3815 search through for a connection to terrorism.
3816 According to the Government's reading of the Fourth
3817 Amendment, the Fourth Amendment provides no constitutional
3818 limit on the Government's ability to get all of this data
3819 about all of us because, by sharing it with Google or AT&T or
3820 Verizon, we have forfeited our -- any interest in privacy
3821 that we might have.
3822 But many people who have looked at this problem,
3823 including President Obama, including the President's review
3824 group, including the Privacy and Civil Liberties Oversight
3825 Board, including Justice Alito, including Justice Sotomayor,
3826 and including Justice Scalia, have said and acknowledged that
3827 when technology advances in this way, it is critical that we
3828 adapt our laws to ensure that we retain the privacy that we
3829 had at the time of the framing.

3830 We're in a brave new world. And unless we adapt our
3831 laws to reflect that fact, we will effectively forfeit the
3832 privacy that is so critical to our own human relations and to
3833 a free and open democracy.
3834 Second, Congress is well situated to act. As Justice
3835 Alito said in the Jones case, a legislative body is well
3836 situated to gauge changing public attitudes, to draw detailed
3837 lines, and to balance privacy and public safety in a
3838 comprehensive way. When it comes to adjusting law to deal
3839 with advances in technology, Congress has historically done
3840 so, and it has historically done so where the Supreme Court
3841 has either declined to protect Americans' privacy or failed
3842 to address sufficiently Americans' privacy.
3843 So when the Supreme Court said the Fourth Amendment does
3844 not protect the privacy rights of people vis-a-vis pen
3845 registers, Congress responded by enacted statutory limits on
3846 the Government's use of pen registers. When the Supreme
3847 Court said we have no privacy rights in our bank records,
3848 Congress responded by enacting the Right to Financial Privacy
3849 Act. FISA itself imposes restrictions on the Government's
3850 ability to gather information that the court has not yet said
3851 is constitutionally protected.
3852 That intervention is necessary here because the
3853 administration has essentially interpreted Congress' prior
3854 law to give it carte blanche. I was around when we debated

3855 the changes on the PATRIOT Act, and I am absolutely certain
3856 that had the administration come to Congress and said we'd
3857 like to amend the business records law, which at that time
3858 allowed the Government to get records on specific targets,
3859 and we'd like to amend it by giving us the authority to get
3860 records, phone records and other business records on
3861 literally every American and amass them in a single database
3862 and keep them for 5 years, there is no way that this
3863 committee would have approved of that. There is no way that
3864 this Congress would have approved of that.
3865 And yet that's the interpretation that the
3866 administration has put on this law in secret. And therefore,
3867 I think it's critical that Congress respond, and I think the
3868 USA FREEDOM Act, by ending dragnet collection and requiring a
3869 nexus between business records sought and terrorism
3870 investigations, is the best way to go.
3871 Thank you very much.
3872 [The statement of Mr. David Cole follows:]

3873 ********** INSERT 5 **********

3874 Chairman GOODLATTE. Thank you, Mr. Cole.

3875 Mr. Garfield, I don't know how the introductions and the
3876 seating got reversed there. Our apologies to you, but you
3877 get the last word of the testimony. Then we are going to
3878 take a recess to go vote, and we will come back and ask
3879 questions of all members of the panel.

3880 TESTIMONY OF DEAN GARFIELD

3881 Mr. GARFIELD. Thank you, Chairman Goodlatte, Ranking
3882 Member Conyers.

3883 On behalf of some of the most dynamic and innovative
3884 companies in the world, we thank you for hosting this hearing
3885 and for inviting us to testify.

3886 My testimony today will be infused with a healthy dose
3887 of humility because we recognize that the phrase, "We don't
3888 know what we don't know," is particularly apt in the area of
3889 national security. That being said, given the multinational
3890 and multisectoral nature of the tech sector and our business,
3891 we know we have something important to contribute to this
3892 conversation.

3893 As you instructed, rather than repeating my written
3894 testimony, which has been submitted for the record, I'll
3895 focus on the economic impact; second, the societal

3896 implications; and then, third, offer some solutions.

3897 With regard to the first, the economic impact is
3898 significant and ongoing. We live in a world where
3899 innovations that were previously the province of your
3900 imagination or solely the movies are now found in technology
3901 that positively impact all of our everyday lives.

3902 Those innovations are not just cool and potentially
3903 lifesaving. They have positive economic benefit, with the
3904 United States benefiting significantly.

3905 By way of example, the data solutions industry, which is
3906 fast growing, is expected to create over 4 million new jobs
3907 in the next 3 years. Nearly a third of those jobs are
3908 expected to be created in the United States, which we all
3909 benefit from.

3910 Unfortunately, because of the NSA disclosures, "made in
3911 the USA" is no longer a badge of honor, but a basis for
3912 questioning the integrity and the independence of U.S.-made
3913 technology. In fact, a number of industry experts have
3914 projected that the losses from the NSA disclosures in the
3915 cloud computing space alone will be in the tens of billions
3916 of dollars.

3917 Second, with regard to the societal implications, the
3918 impact is significant there as well. Many countries are
3919 using the NSA's disclosures as a basis for accelerating their
3920 policies around force localization and protectionism. We've

3921 all read about what's happening in Brazil and their efforts
3922 to create a walled garden around their data.
3923 Brazil is not alone. Some of our other allies,
3924 including Europe, are questioning the safe harbor that
3925 enables cross-border data flows. As well, many European
3926 countries are advocating the creation of country-specific
3927 clouds.
3928 If that is able to proceed and turns into a contagion,
3929 we run the real risk of going down the path of a Smoot-Hawley
3930 like protectionist downward spiral that dramatically impacts
3931 U.S. businesses and actually impacts businesses all around
3932 the world and transfer what is an open, global Internet
3933 instead into a closed, siloed Internet, which is not
3934 something that none of us would like to see.
3935 Congress is in a great position to avoid that, and so
3936 I'll turn to solutions. I offer 3 sets of solutions that
3937 build on 8 principles that we released 2 weeks ago.
3938 First, we think that additional transparency is
3939 critical. The previous panel spoke to some of the steps that
3940 have recently been taken by the Justice Department to enable
3941 greater disclosures. We view those steps as a positive step
3942 forward but still think that legislation is necessary to
3943 cement those gains and to build on them.
3944 Second, we think greater oversight is also very
3945 important, and developing a framework that enables a civil

3946 liberty advocate to be a part of the FISC court process --
3947 I'm sorry, the FISA court process is also important.
3948 The last round of questions for the first panel revolved
3949 around trust, and we think that rebuilding trust is also
3950 critically important. And there are a number of steps we can
3951 take in that regard.
3952 One is around the standard-setting processes around
3953 encryption. The NSA disclosures have significantly
3954 undermined the encryption standard-setting process, and the
3955 President in his speech passed on the opportunity to affirm
3956 the integrity of those processes. We think that it's
3957 critically important that that occur.
3958 Second, and finally, the issue that's been much debated
3959 in the first panel around Section 215. We think the work
3960 that you're doing today and, hopefully, will do in the future
3961 around examining and reexamining 215 is critically important.
3962 In addition to considering national security, we would
3963 advocate considering other factors, including economic
3964 security, civil liberties, cost, as well as the impact on our
3965 standing with U.S. citizens and around the world.
3966 Those same factors are equally apt as we consider
3967 whether that data should be stored by a third party.
3968 Again, I thank you for this opportunity and look forward
3969 to your questions.
3970 [The statement of Mr. Garfield follows:]

3971 ********** INSERT 6 **********

3972 Chairman GOODLATTE. Thank you, Mr. Garfield.

3973 The committee will stand in recess, and we will return

3974 as soon as these votes are over to begin the questioning.

3975 [Recess.]

3976 Chairman GOODLATTE. The committee will reconvene. We

3977 are missing one of our witnesses. We will go ahead and start

3978 with you, Mr. Bradbury, and I am sure we will be joined by

3979 Mr. Garfield shortly. There he is. You were safe. We were

3980 starting with Mr. Bradbury anyway.

3981 Do you see any legitimacy in Justice Sotomayor's concern

3982 that there is a cumulative effect to the data collected?

3983 Does the evolution of technology necessitate a reevaluation

3984 of the concept of a legitimate expectation of privacy?

3985 Mr. BRADBURY. Well, first, Justice Sotomayor in the

3986 Jones case was not addressing anything like the telephone

3987 metadata program. There was a criminal investigation

3988 targeted at a specific individual where they were tracking

3989 him around, and they put a device on his car, and they were

3990 collecting data about everywhere he went and everything he

3991 did. It was focused on a dragnet, if you will, on that

3992 particular individual. And there is nothing like that here.

3993 The only focus in this program in this program is on

3994 terrorist groups and their connections.

3995 Number two --

3996 Chairman GOODLATTE. Well, let me just interject there

3997 because I understand that concern, but I think the concern
3998 that a lot of Americans have is that while that is the
3999 purpose and intent of this, the collection of data, which as
4000 we know technology today allows us to do pretty incredible
4001 things, and not just the government, but it is certainly done
4002 in the private sector. It is done in presidential elections,
4003 for example, to mix data and come up with very, very
4004 informative facts from the advanced use of technology. And
4005 the long-term storage of that data at the same time is, I
4006 think, whether it is what she is concerned about or what many
4007 of us are concerned about.

4008 Nonetheless, I know it is a concern of many of my
4009 constituents that when you put those two things together,
4010 there has to be a much greater degree of trust in what
4011 government is going to do with that data over an extended
4012 period of time.

4013 Mr. BRADBURY. Certainly that is true, and I think it is
4014 important for Congress and an appropriate role for Congress
4015 to study if statutory changes are appropriate with regard to
4016 developments and the use of data and the creation of data and
4017 data records.

4018 But the same concern, which I think is a hypothetical
4019 concern about the potential for abuse, would apply to broad
4020 data collections that are all done by all manner of Federal
4021 regulatory agencies under subpoena authorities,

4022 administrative subpoena powers, that are based on the exact
4023 same language of this statute, but that do not involve --
4024 Chairman GOODLATTE. But let me point out one
4025 difference, and it really goes to my next question. And that
4026 is, do you believe it is possible that because the FISC
4027 operates in secrecy and all those other agencies you cite,
4028 and you are correct about that, they do not operate in
4029 secrecy. Is it possible for the evolution of the law in that
4030 court to become so ossified or to go off track because it
4031 does not get challenged in the same way that regular Federal
4032 courts, or Federal regulatory process for that matter, are
4033 challenged? And if so, what would be the damage in having a
4034 panel of experts, maybe like yourself, available to argue a
4035 counterpoint to make sure that the FISC has all points of
4036 view?
4037 Mr. BRADBURY. Well, I do think that there is nothing
4038 wrong or objectionable, as I have indicated, with a panel of
4039 experts that could be called upon as amicus to provide views
4040 on a difficult question, provided the constitutional issues I
4041 identify could be addressed.
4042 But the other agencies I mentioned do not have to go
4043 through a court, so there are no court decisions unless the
4044 subject of an administrative subpoena challenges it in court,
4045 which is rare because this standard is so generous to those
4046 agencies. So the Securities Exchange Commission, Federal

4047 Trade Commission, Consumer Financial Protection Bureau, they
4048 get vast amounts of data about transactions affecting private
4049 interests of Americans in vast quantities.
4050 Now, I am not saying it is the same quantity as here,
4051 true. But here, the interests are very different. They are
4052 the protection of the Nation from foreign attack. That is
4053 the paramount mission of the National Security Agency. The
4054 reason for the secrecy in the FISA process is because it
4055 involves the most sensitive national security secrets and
4056 threats to the country. It simply cannot be exposed.
4057 Chairman GOODLATTE. I understand that, but there is an
4058 element of trust here that will ultimately cause this to fail
4059 unless the American people believe that what the protections
4060 are available to them are actually being asserted and
4061 exercised in the judicial process. And they do not get to
4062 see that like they do in other proceedings. And your point
4063 is well taken about those other agencies. Maybe we should be
4064 looking at what they do with their data as well.
4065 But finally, let me ask you, do you believe that the
4066 government acquisition of third party data should be
4067 permitted indefinitely, or should there be some limit on how
4068 much of this data should be permitted?
4069 Mr. BRADBURY. Well, in terms of time limit, the
4070 government does impose a time limit if the court order
4071 includes a time limit that requires all this data to be

4072 deleted, purged, after 5 years. The reason they chose 5
4073 years, it is a standard time in the NSA programs because it
4074 is an important period to look back and do historical
4075 analysis. We know there was a cell operating in a particular
4076 operation 3 years ago. We see a new number now. It is
4077 important to know if it --

4078 Chairman GOODLATTE. There is always an example of, you
4079 know, if you saved it further. I think it declines, however,
4080 exponentially, for example, the example of the Boston
4081 bombing. The data that was used to determine whether he had
4082 phone contacts with people that might be engaged in a
4083 conspiracy that we are going to launch another attack, which
4084 his certainly a concern that law enforcement and the general
4085 public would have, would not need to have storage for 5
4086 years.

4087 But let me just also suggest that it is not just about
4088 the length of time. The gentlewoman from California asked
4089 the question of the first panel related to what is the limit
4090 on what kind of data can be gathered. It is not just
4091 telephone data. It is not just financial services data. It
4092 could be almost anything. And, therefore, when you put
4093 together that wide array of data over an extended period of
4094 time, there becomes a great deal of mistrust about how this
4095 system could be abused.

4096 Mr. BRADBURY. Yes, and I think once the disclosures

4097 were made and this became the subject of public debate -- I
4098 think it is a healthy debate -- I think it was incumbent on
4099 the President to come out early and often to explain to the
4100 American people the nature of the program, the limitations,
4101 the lack of abuse, and to defend the program. I was happy to
4102 see that he did that in his speech on the 17th. I think that
4103 came a little late in the day, and unfortunately it was
4104 combined with a decision to change the program in material
4105 respects.

4106 So I think it is first the role of the President to
4107 defend these programs. And second, I think the chairs and
4108 ranking members of the intelligence committees that oversee
4109 the programs have an important role in terms of explaining
4110 and defending the programs.

4111 Chairman GOODLATTE. Thank you. I am going to ask one
4112 more question, and that is directed to you, Mr. Garfield.
4113 Can you list for us the problems that your member companies
4114 anticipate they will face if they are required to store all
4115 the data the NSA is currently storing?

4116 Mr. GARFIELD. It would probably be a long list, but we
4117 have talked about many of them. Some of them include having
4118 to keep data that goes beyond the business purpose of that
4119 data, the time period for keeping it that extends beyond the
4120 time period, security concerns, cost concerns, as well as the
4121 broader concern around trust, which is a critical component

4122 of how we operate in the tech sector.

4123 Chairman GOODLATTE. Thank you. The chair recognizes
4124 the gentleman from Michigan, Mr. Conyers, for 5 minutes.

4125 Mr. CONYERS. Thank you, Mr. Chair. In her concurrence
4126 in U.S. v. Jones, Justice Sotomayor wrote this: "It may be
4127 necessary to reconsider the premise that an individual has no
4128 reasonable expectation of privacy in information voluntarily
4129 disclosed to third parties." Well, here is where that leads
4130 us: your phone number, the website address, the email
4131 address, the correspondence with the internet service
4132 providers, the books, groceries, medications, the purchase
4133 online retailers, and so forth and so on.

4134 How should we, Professor David Cole, how we should we
4135 rethink the right to privacy in what Justice Sotomayor called
4136 the digital age?

4137 Mr. DAVID COLE. Thank you, Representative Conyers. I
4138 think that Justice Sotomayor is onto something. I think
4139 Justice Alito said much the same thing. He did not speak
4140 specifically to the third party disclosure rule, but he did
4141 speak specifically to the risks to our privacy that are posed
4142 by the fact that the government has technology today that
4143 allows it to learn information about all of us without going
4144 through the steps that were required at the time that the
4145 Constitution was adopted. And historically, the 4th
4146 Amendment has been adapted to deal with those kinds of

4147 technological advances, whether it is the phone, or the use
4148 of the beeper, or the use of a GPS, or the use of a thermal
4149 imaging device.
4150 So I think the Supreme Court can and should recognize
4151 that in the modern era, there is a difference between my
4152 voluntarily sharing information with, say, Mr. Bradbury and,
4153 therefore, voluntarily assuming the risk that he will turn
4154 around and provide that information to the government. That
4155 is a voluntary risk that assume.
4156 There is a difference between that and the fact that to
4157 live in the modern age today you necessarily have to share
4158 information with businesses. Every place you walk, you are
4159 sharing with the cell phone company where you are. Every
4160 time you make a search on the internet, you are sharing with
4161 Google what you are thinking about. Every time you send an
4162 email, you are sharing with Google or your internet service
4163 provider who your friends are, who you are addressing.
4164 And the notion that we somehow as Americans have
4165 voluntarily surrendered our privacy and all that incredibly
4166 intimate detail is probably telling about what we think and
4167 what we do than anyone who knows us knows about us. I mean,
4168 I do not think my wife knows as much about me as my computer
4169 knows about me, and yet if you adopt a third party disclosure
4170 rule without any change to recognize the advance in
4171 technology, you have just forfeited privacy.

4172 But that is for the Supreme Court. I think even if the
4173 Supreme Court does not change the rules, this Congress can
4174 recognize that Americans demand more privacy than that. And
4175 as I said in my opening and as I say in my written statement,
4176 Congress has frequently done that. And I think this is an
4177 appropriate time to do that yet again to protect the privacy
4178 that all Americans deserve.

4179 Mr. CONYERS. What do you think of the USA Freedom Act
4180 that I worked with both our U.S. Senator Leahy and with our
4181 former chairman, Jim Sensenbrenner? Do you think that --

4182 Mr. DAVID COLE. I think that is precisely the type of
4183 response I think that is needed and that is justified because
4184 what it does is it says we are going to end the notion that
4185 the government, simply by calling something business records
4186 and claiming that at some point in the future they may want
4187 to look through those business records, the government can
4188 collect everybody's records. Instead, what the USA Freedom
4189 Act says is the NSA, the FBI, they can collect records if
4190 they demonstrate that those records have a nexus either to a
4191 target of an investigation -- a suspected terrorist or a
4192 foreign agent -- or to a person known to or associated with
4193 that target.

4194 That seems to me a perfectly reasonable and tailored
4195 response. Indeed, I think that is how the Administration
4196 sold what they were asking Congress to do when Section 215

4197 was amended with the Patriot Act. And again, as I said in
4198 the opening, I do not think anybody in Congress thought when
4199 they said we are going to allow you to get relevant records
4200 that are relevant to an authorized investigation. I do not
4201 think a single member of Congress thought what we meant by
4202 that is there are no limits on the business records that you
4203 can get. You can get records on every American, every phone
4204 call without any showing of any connection to terrorism.
4205 That is clearly unacceptable in terms of protecting the
4206 privacy of Americans.

4207 The USA Freedom Act protects that privacy. It ensures
4208 that security interests are balanced by giving the government
4209 the ability to get those records where it has a basis for
4210 suspecting that a person has that nexus.

4211 Mr. CONYERS. Thank you so much. I have got a question
4212 for Mr. Dean Garfield, but I am going to give it to him and
4213 ask him to submit it in writing so it will go in the record.

4214 Thank you, Mr. Chairman.

4215 Chairman GOODLATTE. Thank the gentleman, and the chair
4216 recognizes the gentleman from Alabama, Mr. Bachus, for 5
4217 minutes.

4218 Mr. BACHUS. Thank you. First, Professor Cole, I am a
4219 part of a bipartisan group that is looking at sentencing
4220 reform, which is a different area. We are not dealing with
4221 that today, but I know you have been very active in

4222 advocating for changes in our criminal justice system, and I
4223 applaud you for that.
4224 Mr. DAVID COLE. Thank you.
4225 Mr. BACHUS. And I will ask the first question to you.
4226 It is not just the technology that has changed over the last
4227 30 or 40 years. It is really the amount of information out
4228 there. We share so much information on Facebook, Tweeter, or
4229 Twitter, InstaGram. You know, that information is there in
4230 the public realm. I think Smith v. Maryland, those cases
4231 that were decided in the 70s and 80s on privacy and our
4232 expectations on privacy. How does the fact that there is so
4233 much more information out there, and we are sharing so much
4234 more information, how does that affect our expectation of
4235 right to privacy or how should it?
4236 Mr. DAVID COLE. Well, I think that is the key question,
4237 and I think the answer may lie in the decision of Justice
4238 Alito in the Jones case where he says that there is a
4239 difference between following a car from point A to point B in
4240 public. You do not have an expectation of privacy with
4241 respect to your going from point A to point B in a car in
4242 public. There is a difference between that and using a GPS
4243 to follow that car from point A to point B to point C to
4244 point D to point E to point F all the way to point Z, 24/7
4245 for 28 days. You are still in public, but the notion that
4246 the government could have followed you 24/7 for 28 days

4247 without the technology, it just could not have. It would
4248 have cost remarkable resources they would not have. And
4249 Justice Alito says, therefore, people had a reasonable
4250 expectation of privacy with respect to that information
4251 because it was just onerous for the government to collect it.
4252 The same thing is true with all this information. You
4253 know, we generate all this information, but what has changed
4254 is that now every time we make a decision and take an action,
4255 it generates a digital record. And now we have computers
4256 that have the ability to collect and amass all of that data
4257 and to examine it for connections and ties, which tells
4258 whoever is looking, whether it be the NSA, or the FBI, or the
4259 IRS, whoever is looking, tells them a whole lot more about an
4260 individual than they ever possibly could have known before
4261 the advent of this technology and before the blossoming of
4262 these digital traces.
4263 And, you know, it seems to me that both the
4264 Constitution, the 4th Amendment doctrine, and the statutory
4265 law of this Congress needs to be adapted to recognize that
4266 fact. Otherwise, as Justice Scalia said in the Kyllo case
4267 involving thermal imaging devices, we will simply forfeit our
4268 privacy to advances in technology.
4269 We have a choice, and the choice is whether we want to
4270 preserve our privacy or not. It does not go automatically.
4271 It goes if we let it go. And Congress has the power to stop

4272 it.

4273 Mr. BACHUS. Okay. Mr. Bradbury, would you like to

4274 comment?

4275 Mr. BRADBURY. Well, I think there is a big difference

4276 between what has been referred to as the third party

4277 doctrine, records being held by a third party, and the notion

4278 that metadata, which is transactional data, simply data about

4279 communications, not the content of the communications, is not

4280 a search because there is not a reasonable expectation of

4281 privacy. That is data created by a company to conduct its

4282 business. And the people involved in the communications as

4283 subscribers know the company is creating that record, that

4284 data. It is not your personal record. It is not something

4285 that includes the content4 of the communication.

4286 There may be a communication that is stored in a cloud

4287 some place and somebody might try to argue that is held by a

4288 third party and it is not subject to protections. But this

4289 Congress has given it protections under the Electronic

4290 Communications Privacy Act and the Stored Communications Act.

4291 And I think there is an argument that the Court would

4292 recognize it as protected because it still includes the

4293 substance and private communications. So I think there is a

4294 big difference between that pure transactional metadata and

4295 every other kind of third party stored data.

4296 The last thing I would comment on, Congressman, is with

4297 respect to the Jones case and what has been called the mosaic
4298 theory is that at a certain point when you put enough
4299 information about an individual together in an investigation,
4300 voila, that becomes a search suddenly, I think that Court has
4301 not gone there yet. There is a lot of scholarship about it
4302 and discussion. But if the Court goes there, that could
4303 really seriously interfere with criminal investigations of
4304 all kinds.

4305 I mean, think about organized crime investigations where
4306 the prosecutors who are investigating or the FBI puts up on
4307 the wall an organization chart with the pictures of the
4308 members of the organization and collects all kinds of public
4309 data about the goings-on of those particular members of the
4310 organization. Does that constitute a search that would
4311 require a warrant to put that kind of profile together from
4312 all manner of public available information? No, it cannot.
4313 If it does, then criminal investigations would come to a
4314 halt.

4315 Mr. BACHUS. Thank you.

4316 Chairman GOODLATTE. The chair recognizes the gentleman
4317 from New York, Mr. Nadler, for 5 minutes.

4318 Mr. NADLER. I thank the Chairman. Let me first observe
4319 that because of the evolving technology, people may, in fact,
4320 if they think about it, realize that the metadata on their
4321 phones is in the possession of somebody, but still have an

4322 expectation of privacy when they are using the phone because
4323 you do not think about it in everyday terms. And if you did
4324 and you said, gee, I do not want this in the public domain
4325 because it might go into the public domain because the phone
4326 company is keeping it for billing records and maybe because
4327 of something else, you would have no privacy at all. So I
4328 think our law has to change. Maybe for 40 or 50 years the
4329 expectation of privacy theory was valid, you know, and was
4330 sufficient, but no longer as privacy becomes more invaded.
4331 But let me ask you the following, Professor Cole. You
4332 wrote in your testimony, "The bill would" -- the bill, that
4333 is to say, the USA Freedom Act -- "would restore an approach
4334 to privacy that is governed in this country since its
4335 founding, namely the notion that the government should only
4336 invade privacy where it has some individualized objective
4337 basis for suspicion," which, of course, is not the bulk
4338 collection of information under Section 215.
4339 But you are describing exactly what we always wanted to
4340 do to avoid the general warrant. The 4th Amendment was
4341 written specifically to say no general warrants. You have to
4342 describe the thing to be searched. We do not want the king's
4343 officer to be able to come and say show me everything based
4344 on nothing except that you live in Boston.
4345 What we have now, is this not the type of general
4346 warrant that Section 215, the way it has been interpreted,

4347 precisely the general warrant that the 4th Amendment was
4348 enacted to prevent?
4349 Mr. DAVID COLE. I think it is. I think that when you
4350 have an order that says go out and collect literally every
4351 American's every phone call record, how is that different
4352 from a general warrant? It is not targeted. It is not
4353 predicated on individualized suspicion. It is as expansive
4354 as a general warrant, and that is precisely the concern that
4355 was raised.
4356 Now, Mr. Bradbury says, well, but it is only getting
4357 metadata, not content. I think that is a very evanescent --
4358 Mr. NADLER. Because you can learn a lot from metadata.
4359 Mr. DAVID COLE. Well, and here is what Stewart Baker,
4360 who is general counsel of the NSA, said about that. He said,
4361 "Metadata absolutely tells you everything about somebody's
4362 life. If you have enough metadata, you do not really need
4363 content. It is sort of embarrassing how predictable we are
4364 as human beings."
4365 Mr. NADLER. Okay. I thought the moment I heard about
4366 it, I thought it was precisely the general warrant. And we
4367 certainly had no intention of authorizing Section 215. And
4368 the FISA Court, if it were not the kind of kangaroo court it
4369 is because it only gets one side, and it is done in secret,
4370 probably would not have decided it that way.
4371 But let me ask you a second question. The review board

4372 established by the President recommended, among other things,
4373 that we harmonize the standards for national security letters
4374 for Section 215 collection. This makes sense to me,
4375 particularly as many of the standards for NSL's minimization
4376 of initial approval process are less rigorous. What is your
4377 opinion? Should we harmonize the standards by requiring that
4378 NSL meet the same and presumably amended standards since it
4379 will fix the problem that now exists with the Administration
4380 and FISA Court's interpretation of what is relevant?
4381 In other words, should we make the NSLs match 215, and,
4382 for that matter, if we do, why bother having NSLs at all
4383 anymore?
4384 Mr. DAVID COLE. Right. Well, yes, I think they should
4385 be harmonized. The USA Freedom Act would harmonize them and
4386 would employ the same standard to define the nexus required
4387 to get business records generally and the nexus required to
4388 get NSLs.
4389 Right now, NSLs in Section 215 have the same standards.
4390 It's just that it is this relevance standard which the
4391 government has read to be meaningless. So the USA Freedom
4392 Act would keep parity between --
4393 Mr. NADLER. It would harmonize them?
4394 Mr. DAVID COLE. Huh?
4395 Mr. NADLER. It would harmonize them.
4396 Mr. DAVID COLE. Right.

4397 Mr. NADLER. Good.

4398 Mr. DAVID COLE. It is harmonized, yes. But I think it
4399 needs to be harmonized and elevated to --

4400 Mr. NADLER. Harmonized up, not down.

4401 Mr. DAVID COLE. Yes.

4402 Mr. NADLER. Mr. Garfield, in the few seconds I have,
4403 last week the government agreed to allow to Facebook,
4404 Microsoft, Google, Yahoo, Apple, and other tech companies to
4405 make information available to the public about the
4406 government's request for email and other internet data. Are
4407 these new disclosure rules sufficient? Should Congress take
4408 additional steps? And assuming that the NSA continues to
4409 collect telephone metadata under Section 215, will the
4410 government reach a similar deal with telephone companies for
4411 disclosures about call record requests?

4412 Mr. GARFIELD. I will answer the first two questions,
4413 which I am in a good position to answer.

4414 Mr. NADLER. That is why I asked you.

4415 Mr. GARFIELD. The agreement last week I think is a
4416 positive step in allowing greater transparency, which is
4417 something we strongly believe in.

4418 The answer to your second question as to whether
4419 legislation would be helpful is yes. It goes part way, but
4420 not far enough. For example, it is important that the
4421 private sector have transparency reports and disclosures, but

4422 it is also important that the public sector do as well. And
4423 so, in that respect, among others, I think having legislation
4424 would be very helpful.
4425 Mr. NADLER. Thank you. My time has expired. Thank
4426 you.
4427 Chairman GOODLATTE. The chair recognizes the
4428 gentlewoman from California, Ms. Lofgren, for 5 minutes.
4429 Ms. LOFGREN. Thank you, Mr. Chairman, and thanks for
4430 this hearing. You know, Mr. Conyers read the exact quote
4431 from Justice Sotomayor's opinion that I had been looking at.
4432 And I have been thinking a lot about we have the role of
4433 writing the statutes, but behind that is, you know, what the
4434 Constitution requires. And I think that it is not just the
4435 Court that needs to examine that. I think the Congress has
4436 an obligation to do that as well.
4437 And as I have been thinking about this, I have been
4438 thinking about two longstanding doctrines, one, the third
4439 party data, there is no expectation of privacy, as well the
4440 plain sight doctrine. And just as you have said, I mean, 30
4441 years ago, if I walked out my front door, I knew that my
4442 neighbors could see me. I did not expect that my picture
4443 would be taken every place I walked and compiled, and using
4444 facial recognition technology someone could say where I was
4445 every moment of every day.
4446 Yes, if I went in and checked into a hotel, I knew that

4447 that was not private information, but I did not expect that
4448 every email I send, every website, that if I went on my
4449 Constitution document that somebody could track how often I
4450 read the 4th Amendment. That was not part of the third party
4451 doctrine.

4452 So I think Congress needs to not delegate this to the
4453 Court, but to head on take on these issues because I think if
4454 you look at where the Court is going, you know, I do not know
4455 how long it is going to take them to get there. You know, we
4456 cannot discuss what we are told in closed sessions, but I
4457 will just read the news reports that we had a few days ago,
4458 reports that that the NSA is spying using leaky mobile apps;
4459 a few days before that the NSA collected over 200 million
4460 text messages; that in late December that cookies were being
4461 used to track people; that there were 5 billion records of
4462 mobile phone location data collected daily; that there was
4463 collection of pornographic website visits used to blackmail
4464 potential so-called terrorists; that money transfers were
4465 being tracked. And it goes on and on.

4466 So I guess, you know, one of the questions I have,
4467 Professor Cole, is if the Congress should step forward to
4468 interpret the 4th Amendment in light of big data, how would
4469 we do that, statute by statute? And I am a co-sponsor of Mr.
4470 Sensenbrenner's bill, but that really relates to just a
4471 portion of this question. Do you have thoughts on that?

4472 Mr. DAVID COLE. Well, I think it is a great question.
4473 I think it is the defining question of privacy for the next
4474 generation, which is how do we preserve privacy in the face
4475 of these advances in technology, which make it possible for
4476 the government to learn everything about us.
4477 And I think, you know, it is absolutely critical that
4478 Congress play a role, that Congress has historically played a
4479 role, not waited for the Supreme Court to act, in some
4480 instances acting before the Supreme Court does so, FISA for
4481 example. In other areas when the Supreme Court has said
4482 there is no expectation of privacy, Congress has come on the
4483 heels of that and said, wait a minute, the American people
4484 disagree with you. We want our privacy. And so, I think
4485 that is what you did with respect to bank records, video
4486 rental records, PIN registers, and the like.
4487 So there is a real history of Congress stepping up here
4488 and doing so. And I am not sure you can do it in a global
4489 way, but the USA Freedom Act, as I suggested earlier, is a
4490 useful start because it puts in place the principle of
4491 individualized suspicion, rejecting this general warrant
4492 notion.
4493 Ms. LOFGREN. I am going to follow up with you and I am
4494 going to ask one additional question of Mr. Garfield. On the
4495 technology issues, one of the very distressing reports was
4496 that the government, rather than alert people to zero day

4497 events, simply exploited them. I am worried about the
4498 balkanization of the internet. We see what Brazil is doing,
4499 certain authoritarian regimes insisting that servers be
4500 placed in their country. I am worried about governance and
4501 whether ICON will be able to continue to be the governing
4502 body, or whether efforts to dismantle that will be enhanced
4503 by these revelations.

4504 I am wondering if we should make obligations to the
4505 government to proactively take steps to preserve the global
4506 internet both through mandates not to weaken encryption,
4507 mandates as to assisting in zero day events, and if you have
4508 thoughts on that.

4509 Mr. GARFIELD. Yes, I absolutely do. We worry as well
4510 about the potential balkanization and what the NSA
4511 disclosures mean for internet governance. I think it is very
4512 important for Congress to act in this area. I think the
4513 President missed an opportunity by not speaking to the
4514 encryption standards issue and the need to bolster the
4515 integrity of encryption standards. And so, to the extent
4516 that Congress has the ability to do that, we would encourage
4517 it.

4518 Ms. LOFGREN. My time has expired. Thank you, Mr.
4519 Chairman.

4520 Chairman GOODLATTE. The chair thanks the gentlewoman,
4521 and recognizes the gentleman from Virginia, Mr. Scott, for 5

4522 minutes.

4523 Mr. SCOTT. Thank you, Mr. Chairman. Mr. Garfield, can
4524 you just say another word about the effect of global
4525 competitiveness on this issue and how American companies are
4526 actually pretty much at a disadvantage if we do not get this
4527 straight?

4528 Mr. GARFIELD. No, absolutely. So trust, integrity,
4529 security are key components of technology and doing well in
4530 technology and developing your business in that area. The
4531 United States has played a significant leadership role around
4532 the world. And to the point in my testimony, rather than
4533 continuing to be a badge of honor, today because of the NSA
4534 disclosures, countries and customers around the world are
4535 questioning the integrity and independence of U.S. technology
4536 companies, which puts us at a competitive disadvantage
4537 overseas, but also here where the American people also have
4538 those same trust concerns.

4539 Mr. SCOTT. And do you have a choice in vendors in a lot
4540 of products, whether it is an American company or a foreign
4541 company?

4542 Mr. GARFIELD. I am sorry?

4543 Mr. SCOTT. Is there a choice in vendors in products?

4544 Mr. GARFIELD. Almost always, I mean, but the tech
4545 sector is highly competitive. We represent both domestic and
4546 international companies. The impact, interestingly enough,

4547 is global because to the extent that innovations that are
4548 being led by the United States do not occur, the whole world
4549 is disadvantaged because we all benefit from those
4550 innovations. And so, it creates a global problem, but one
4551 that is particularly acute for U.S. companies.
4552 Mr. SCOTT. Does your council have a position on where
4553 information should be stored if the decision is made to
4554 collect and store this data where it ought to be stored at
4555 NSA or some, say, department store or something like that?
4556 Mr. GARFIELD. Yes. Our view is that the same
4557 considerations that we offer in evaluating 215 are apt in
4558 considering where that data is stored. For example, if the
4559 goal is to rebuild trust, it is not clear how having that
4560 data stored in a third party addresses the trust concern. If
4561 it is around data integrity and security, it is not clear how
4562 having it stored in a third party addresses that data
4563 integrity or security question.
4564 And so, in the examination, we think it is important to
4565 come up with certain principles and have those principles
4566 guide the examination both of 215 as well as where the data
4567 is stored.
4568 Mr. SCOTT. So are you suggesting it could be stored at
4569 the NSA as long as they separate it down the hall, across the
4570 street, but have NSA control it rather than the private
4571 sector?

4572 Mr. GARFIELD. I am not suggesting that at all.

4573 Mr. SCOTT. Well, where would it be?

4574 Mr. GARFIELD. The beginning comment that I made, which
4575 is that there is a lot that I am not privy to for a whole
4576 host of reasoning, including security clearance. And so, I
4577 do not feel I am in a position to give advice to the U.S.
4578 government on national security. What I feel that I have the
4579 confidence to do is to make sure that certain important
4580 factors, in addition to national security, are considered.
4581 Economic security, privacy, civil liberties, as well as our
4582 standing in the world, are some of the factors that we think
4583 should be considered.

4584 Mr. SCOTT. Thank you. Mr. Cole, the Administration has
4585 offered a lot of administrative changes. What would be the
4586 shortcomings if those changes are not codified?

4587 Mr. DAVID COLE. If those changes are not codified?

4588 Mr. SCOTT. Right.

4589 Mr. DAVID COLE. Well, I think those changes are
4590 important ones, in particular the notion that the NSA cannot
4591 search through the bulk collection without first getting
4592 approval from a court. That seems to me an important
4593 modification. The notion that there would be an independent
4594 advocate in the FISC seems to be important. And one
4595 implication of not doing that, I think as we see, we see
4596 repeated instances of what we have now learned about, right?

4597 So Mr. Bradbury said 15 judges of the FISA Court
4598 approved of the use of Section 215 to get all of our phone
4599 data. What he did not say is that when that program was
4600 first approved by the first judge in May 2006, he did not
4601 even write an opinion. He did not address the constitutional
4602 questions. He did not say why he thought the limitation on
4603 relevance was somehow met by giving the NSA access to
4604 everybody's information. No opinion.
4605 Every 90 days thereafter, a different Federal judge, and
4606 this is how he gets to 15, signed an order that extended the
4607 program. No analysis of the constitutional question, no
4608 analysis of the statutory question. It was not until Edward
4609 Snowden disclosed it to the public that the FISC finally
4610 wrote an opinion 7 years after the program had been up and
4611 running explaining retroactively why they thought what they
4612 had been doing for 7 years was okay. And it is, as the
4613 privacy board has shown in its analysis, a very, very
4614 doubtful construction of the statute, one that, as
4615 Representative Sensenbrenner has, was not in anybody's mind
4616 who adopted the statute.
4617 So I think the Administration's proposals are important,
4618 but I think they do not go far enough. And particularly the
4619 key way in which they do not far enough is that they do not
4620 end bulk collection. They do not end dragnet collection.
4621 They just put it somewhere else. I think with the USA

4622 Freedom Act would do is end it, and that is a much better
4623 response.
4624 Mr. SCOTT. You were not here when Mr. Cole answered the
4625 question about retroactive immunity. I asked the question
4626 that you keep hearing that the collection of the data was
4627 helpful. It was an illegal collection, finding that it was
4628 helpful does not give you immunity for the collection. Do
4629 you have a comment on what relevance it is that people keep
4630 saying we need because it is helpful as a justification for
4631 getting the data?
4632 Mr. DAVID COLE. Yes, absolutely. I mean, it would be
4633 helpful if the police could, without a warrant, search every
4634 one of our homes on a daily basis without any basis for
4635 suspicion. That would be helpful because they might find
4636 some bad guys who are hiding behind the privacy that we all
4637 expect from our home. But that does not make it right.
4638 But number two, I think when they say it is helpful, you
4639 have got to look behind that, as the privacy board did, met
4640 with them in classified sessions, looked at classified
4641 materials, looked at the "success stories," and found, and
4642 here I am quoting from them on page 146, "We have not
4643 identified a single instance involving a threat to the United
4644 States in which the telephone records program made a concrete
4645 difference in the outcome of a counterterrorism
4646 investigation. Moreover, we are aware of no instance in

4647 which the program directly contributed to the discovery of a
4648 previously unknown terrorist plot or the disruption of a
4649 terrorist attack."
4650 Mr. SCOTT. Well, to justify the program because it was
4651 helpful, it just adds insult to injury. It was not even
4652 helpful. But even if it had been helpful, it would not
4653 retroactively make the collection legal, would it?
4654 Mr. DAVID COLE. That is right.
4655 Mr. BACHUS. [Presiding] Mr. Scott, your time has
4656 expired.
4657 Mr. SCOTT. Thank you, Mr. Chairman.
4658 Mr. BACHUS. Thank you. Mr. Chaffetz.
4659 Mr. CHAFFETZ. Thank you. I appreciate the hearing. I
4660 know it has been a long one, and I appreciate your patience
4661 here.
4662 Mr. Garfield, one of the terms that has been thrown out
4663 there is this so-called balkanization of the internet or
4664 internet balkanization. I would like you to expand on that.
4665 You have talked about bits and parts of it. You know, there
4666 have been some concerns about what is going on in Brazil, the
4667 European Union. They have announced some policies that would
4668 disadvantage the United States based companies. Can you kind
4669 of expand your thoughts on that?
4670 Mr. GARFIELD. Yes. I know this is not just
4671 theoretical, it is actually real, so you point to Brazil

4672 where the government of Brazil is moving forward with
4673 policies that would essentially create a wall garden around
4674 data that is developed in Brazil. They have already said
4675 that the email systems being used by the government can only
4676 be stored or developed by Brazilian companies. So as a
4677 result, U.S. companies that have previously held a leadership
4678 position in the technology innovation in that space are being
4679 dispossessed.

4680 It is an economic issue, but it also a broader internet
4681 governance issue. If it turns out that the open internet
4682 that we have all gotten used to becomes a balkanized series
4683 of walled gardens, then a lot of the innovation, a lot of the
4684 societal benefits that we have experienced will be limited.

4685 Mr. CHAFFETZ. Thank you. In your written testimony you
4686 state the need to rebuild trust regarding the National
4687 Institute of Standards and Technologies, or NIST, and their
4688 commitment to cryptographic standards developed and vetted by
4689 experts globally. Could you explain the importance of this
4690 in your opinion?

4691 Mr. GARFIELD. Yes. The reason why technologies work
4692 across geographic boundaries is you get off the plane and
4693 your phone will work in Europe as well as the United States,
4694 is because of standards that are driven through consensus and
4695 multi stakeholder voluntary processes. Some of the
4696 disclosures have suggested that the United States has

4697 exploited vulnerabilities in cryptography, which erodes
4698 trust. And so, in order to ensure that our technology will
4699 work across borders, it is critical to rebuild that trust.
4700 The President missed an opportunity in his speech to
4701 speak to this issue. We hope that he will, but Congress has
4702 the opportunity to correct that error.
4703 Mr. CHAFFETZ. Thank you. I think you have touched on
4704 two of the concerns that globally the communication that we
4705 enjoy. These things are so important. So I appreciate all
4706 of your expertise being here today. I appreciate this
4707 committee talking about such an important issue.
4708 Mr. Chairman, I think you wanted me to yield you some
4709 time if that is correct? I will yield back or yield to you,
4710 whatever you choose.
4711 Mr. BACHUS. Yes, yield to me, if you will.
4712 Mr. CHAFFETZ. Yes.
4713 Mr. BACHUS. And let me say this. I am going to pursue
4714 that same line. I had intended to. And, Mr. Garfield, are
4715 there other countries that are demanding information from
4716 your member companies about their citizens or foreign
4717 citizens?
4718 Mr. GARFIELD. It happens in a number of countries. And
4719 so, as we think about internet governance and jurisdiction
4720 issues, we are always careful about the salutary impact. And
4721 so, the rules that we live by in one market set a precedent

4722 for how we operate globally, and that is in part why in our
4723 recommendations we strongly encourage more multilateral
4724 dialogue around these surveillance and security issues so we
4725 can get greater harmonization around the rules that are
4726 created.
4727 Mr. BACHUS. Right. And are other countries tapping
4728 into your member company systems for spying purposes?
4729 Mr. GARFIELD. The question presumes that that is
4730 happening anywhere, including here in the United States.
4731 Mr. BACHUS. Well, say, in other countries.
4732 Mr. GARFIELD. No. So our companies are always working
4733 hard to make sure that cryptography and security measures are
4734 robust.
4735 Mr. BACHUS. But what I am talking about is, you know,
4736 they have databases, and they maintain those in other
4737 countries. Can they come and use that platform to access
4738 information for spying purposes?
4739 Mr. GARFIELD. We work hard to make sure that is not, in
4740 fact, the case. I mean, the previous panel made the point
4741 that we live in a world in which cyber warfare and efforts on
4742 undermining cyber security are quite aggressive, including by
4743 companies as well as nations. We are always working because
4744 it is a first priority of ours to maintain the data integrity
4745 to fight against that.
4746 Mr. BACHUS. Well, let me say this. If you are required

4747 to store some of this data, say, even the U.S. government,
4748 then it could be subject to requests in civil proceedings,
4749 divorce proceedings, once you maintain it. So you may want
4750 to consider to start maintaining that data.

4751 Mr. GARFIELD. Exactly, and there are two issues. One
4752 is data stored by private companies at the request of the
4753 U.S. government, and then data stored at a third party. We
4754 are unequivocally opposed to data being stored by the private
4755 sector, us, beyond the need for business purposes for the
4756 very reason you highlight, which is the data integrity issue.
4757 It creates additional vulnerabilities. We are always
4758 fighting against that, but we do not want to create more
4759 targets.

4760 Mr. BACHUS. Thank you. The gentlelady from Texas is
4761 recognized for 5 minutes.

4762 Ms. JACKSON LEE. Let me thank you again, and let me
4763 take note that this is a long hearing, and we thank you very
4764 much for your participation here.

4765 I was, Professor Cole, reading the old 215, and I guess
4766 I continue to be baffled, having been here when we crafted
4767 the Patriot Act in the waning hours, months, and days after
4768 9/11. And everyone was in a perplexed state, and the idea
4769 was, of course, to protect our citizens. But I notice 215 in
4770 Section 501 particularly pointed out, they listed books,
4771 records, papers, documents, and other items. There goes the

4772 mega data. But they also said protect against international
4773 terrorism or clandestine intelligence activities. Further
4774 down, it goes onto again emphasize that we should specify
4775 that there is an effort to protect against international
4776 terrorism, clandestine intelligence.
4777 And I only raise that because it looks to me that we
4778 have firewalls, but what resulted is this massive
4779 acknowledgement of the gathering of telephone records of
4780 every single American. And I want to find a way to politely
4781 push back on Justice Sotomayor's reflection, and I think it
4782 is a reflection, and I think it is one in the reality of
4783 today, which is maybe we can have privacy, and have you muse,
4784 if you will, on the new legislation that we have introduced
4785 where we enunciate a whole list of reasons. And I do not
4786 know if you have been able to look at that number 1 section
4787 that we have here that goes on to as relevant material,
4788 obtain foreign intelligence not concerning a United States
4789 person, protect against international terrorism. It sort of
4790 lays it out.
4791 And I ask you, can we comfortably find a way to answer
4792 Justice Sotomayor and say, yes, we can? I might use that.
4793 And is there something else we should add in the legislation
4794 that I have co-sponsored enthusiastically, and we will be
4795 looking forward to it moving forward. Can we add something
4796 else because as I look at 215, Section 501, it looks as if we

4797 had all that we need to have to say, you know what? I do not
4798 think they wanted you to get the mega data. Are we where we
4799 need to be in this new legislation?
4800 Mr. DAVID COLE. Thank you for that question. You know,
4801 I agree that Section 215, if you read it with its ordinary
4802 meaning, sought to put constraints on the types of records
4803 and the amounts of records that the government could obtain
4804 because it did not say you are hereby authorized to obtain
4805 all business records on all Americans. It said you are
4806 authorized to obtain business records that are relevant to an
4807 authorized investigation.
4808 And as the privacy board's report shows in exhaustive
4809 detail, very powerful analysis, no court in any other setting
4810 has ever read a relevance limitation as expansively as saying
4811 you can pick up every American's every record. No court, not
4812 in a grand jury context, not in a civil discovery context.
4813 So Congress did seek to put in limited language.
4814 Ms. JACKSON LEE. We did.
4815 Mr. DAVID COLE. But the Administration essentially took
4816 it out. So I think what Congress needs to do is to push
4817 precisely as Justice Sotomayor suggests, and I think that the
4818 key is to identify when it is obviously justified to sweep up
4819 the kinds of records that disclose so much about our intimate
4820 and personal lives. And I think the USA Freedom Act does a
4821 good job because it says you can do so when those records

4822 pertain to a foreign agent or a suspected terrorist, when
4823 they pertain to an individual in contact with or known to a
4824 suspected agent of a foreign power or a terrorist who is a
4825 subject of an investigation.

4826 So that says you can get records on the target. You can
4827 get records on people connected to the target. But, no, you
4828 cannot get records on every single American because Americans
4829 want security, but they also want privacy, and they want to
4830 use their phones. And we should not have to give up any one
4831 of those three. I think the USA Freedom Act ensures that we
4832 have all three.

4833 Ms. JACKSON LEE. And diligence is part of that. Mr.
4834 Gardner, let me ask you this. I know you may have been asked
4835 and answered over and over again. What will be the burden of
4836 the private sector hold onto this vast amount of data if it
4837 was to be crafted in that way? What would be the cost? What
4838 would be the problems?

4839 Mr. GARFIELD. It is hard to put a precise number on it.
4840 I think it suffices to say the burden would significant, not
4841 only in cost, but the impression that it creates. One of the
4842 challenges we face as a result of the NSA disclosures is
4843 there is a question around the integrity as well as the
4844 independence of U.S.-based companies. If we are to store
4845 that data, that would call into question whether we are, in
4846 fact, independent. And so, there are financial costs as well

4847 as broader costs as well.

4848 Mr. BACHUS. Thank you.

4849 Ms. JACKSON LEE. Mr. Chairman, if you would just

4850 indulge me for 30 seconds, a group question.

4851 Mr. BACHUS. A brute question? But a very short

4852 response.

4853 Mr. GARFIELD. Okay.

4854 Ms. JACKSON LEE. Thank you very much. I will not

4855 follow up. I just want to get Mr. Bradbury and Mr. Cole in

4856 again, and I will group my question together. Mr. Gardner

4857 makes a valid point on the perception issue. Why is it not

4858 better that we have a monitored holding of the data of

4859 whatever it may be, and the fact that we have now laid out a

4860 framework by the Federal government instead of the private

4861 sector.

4862 And then just an aside with respect to how we do our

4863 intelligence. Do you think it is time that we haul in all of

4864 the outside contracting and do a better job of vetting and

4865 doing this in house dealing with our intelligence access? If

4866 I can get a quick answer. I think I put two questions in at

4867 once. Mr. Bradbury?

4868 Mr. BRADBURY. Thank you, Congresswoman. I do think

4869 there are risks with outside contractors, and I think putting

4870 the data in private hands would raise those risks. I think

4871 it would increase privacy concerns and make the program less

4872 effective.

4873 So I think it is monitored now while it is being held by
4874 the NSA, closely overseen. I do not think it is an excess or
4875 abuse of the relevant standard. I think if this committee
4876 changes the relevance standard, it should not single out the
4877 NSA and the intelligence community. It should consider
4878 applying the same narrowing standard to all Federal
4879 regulatory agencies, which collect vast amounts of records
4880 and data for their own investigatory purposes. They do not
4881 just limit themselves to those narrow individual records that
4882 are directly pertaining to their investigation. They get
4883 databases so that they can search it for relevant queries.

4884 And so, if the same standards applied across the board,
4885 I think it would really inhibit the functioning of
4886 government. I do not think the NSA should be singled out
4887 when its mission is the most important.

4888 Ms. JACKSON LEE. Thank you. Mr. Cole, can you --

4889 Mr. DAVID COLE. I think if you adopt the USA Freedom
4890 Act, which I think you should, then the problem of where to
4891 store the bulk collection is solved because there is no bulk
4892 collection, right? If you say the NSA can only collect data
4893 where it is actually connected to a terror suspect or someone
4894 who is connected to a terror suspect, there is no bulk
4895 collection, and there is not the problem of storage. The
4896 problem of storage arises only if you continue to permit bulk

4897 collection. I do not think that should continue to be
4898 permitted.
4899 Ms. JACKSON LEE. I thank you, Mr. Chairman. I think we
4900 have got strong support for the H.R. 3361, and I look forward
4901 to moving forward on such legislation. With that, I yield
4902 back.
4903 Mr. BACHUS. This concludes today's hearing. The
4904 chairman thanks all of our witnesses for attending.
4905 Without objection, all members will have 5 legislative
4906 days to submit additional written questions for the witnesses
4907 or additional materials for the record.
4908 [The information follows:]

4909 ********** COMMITTEE INSERT **********

4910 Mr. BACHUS. This hearing is adjourned. Thank you.

4911 [Whereupon, at 3:09 p.m., the committee was adjourned.]

****
SPEAKER LISTING
****

****
CONTENTS
****

****
INDEX OF INSERTS
****

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 19, 2014

The Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find the corrected transcript of the testimony of James Cole, Deputy Attorney General, at the hearing held before the Committee on February 4, 2014, entitled "Recommendations to Reform Foreign Intelligence Programs."

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Principal Deputy Assistant Attorney General

Enclosure