S. HRG. 113–879

CONTINUED OVERSIGHT OF U.S. GOVERNMENT SURVEILLANCE AUTHORITIES

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

DECEMBER 11, 2013

Serial No. J–113–42

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE
28–113 PDF WASHINGTON : 2018

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California	CHUCK GRASSLEY, Iowa, *Ranking Member*
CHUCK SCHUMER, New York	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	JEFF FLAKE, Arizona
MAZIE HIRONO, Hawaii	

KRISTINE LUCIUS, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

CONTENTS

DECEMBER 11, 2013, 2:02 P.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

ANSWERS

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

CONTINUED OVERSIGHT OF U.S. GOVERNMENT SURVEILLANCE AUTHORITIES

WEDNESDAY, DECEMBER 11, 2013

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to notice, at 2:02 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Whitehouse, Klobuchar, Franken, Blumenthal, and Grassley.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Okay. We can get started because I know with all the other things going on on the Hill, it is going to be a tad busy today. But I appreciate General Alexander, Mr. Cole, and Mr. Litt being here.

We are going to be renewing our examination of Government surveillance activities, and it seems every time we have these, there has been a series of new revelations. The latest disclosures raise some significant questions about the scope and wisdom of our surveillance activities both at home and abroad. So it is clear that we have a lot more oversight work to do.

In the last week, there have been press reports that the NSA is collecting billions of records a day of cell phone locations around the world and can track individuals and map their relationships. There have also been reports that the NSA is monitoring online video games, which just in the press reports raises a question: Because we can do something, does it really make sense to do it?

Especially last month, the administration released a set of documents revealing details about yet another massive dragnet collection program in addition to the phone records program. And this time the NSA was gathering in bulk an enormous amount of Internet metadata under the pen register and trap and trace device authority in FISA. Now, I would just note that, just like Section 215, there is nothing in the pen register statute that expressly authorizes the dragnet collection of data on this scale.

Although the Internet metadata collection program we are told is not currently operational, it resulted in a series of major compliance problems—just like the Section 215 program. According to the FISA Court, the NSA exceeded the scope of authorized acquisition

not just once or twice, but "continuously" during many of the years the program was in operation. Again, another reason why we should have a lot more oversight and a lot more open oversight than we do have.

The problems were so severe that the FISA Court ultimately suspended the program entirely for a period of time before approving its renewal. But once renewed, the Government asserted that this bulk collection was an important foreign intelligence tool—which is the claim it makes now about the Section 215 phone records. But then in 2011 the Government ended this "valuable tool," as they called it, this Internet metadata program because, as Director Clapper explained, it was no longer meeting "operational expectations."

It is important to note that the administration does not believe that there is any legal impediment to re-starting this bulk Internet data collection program if it—or a future administration—wanted to do so. The legal justification for this Internet metadata collection is troubling. As with the Section 215 program, the Internet metadata program was based on a "relevance" standard. And as with the Section 215 program, there is no adequate limiting principle to this legal rationale. The American people have been told that all of their phone records are relevant to counterterrorism investigations. Now they are told that all Internet metadata is also relevant and apparently fair game for the NSA to collect.

In any country, this legal interpretation would be extraordinary. It goes beyond extraordinary in the United States. And it is going to have serious privacy and business implications in the future, particularly as new communications and data technologies are developed.

So it should come as no surprise that the American technology industry is greatly concerned about these issues. I have heard from a number of companies who worry that their global competitiveness has been weakened and undermined. They say that American businesses stand to lose tens of billions of dollars in the coming years, and we need to make substantial reforms to our surveillance laws to rebuild confidence in the U.S. technology industry. This confidence can be thrown away very easily, and it is more difficult to get it back.

Earlier this week, eight major technology companies—including Microsoft, Google, Apple, Facebook, and Yahoo—released a set of five principles for surveillance reform. Citing the "urgent need to reform Government surveillance practices worldwide," the companies call for greater oversight and transparency, but they also advocate for limits that would require the Government to rely on targeted searches about specific individuals rather than the bulk collection of Internet communications from all of us.

I have introduced the USA FREEDOM Act with Senator Lee here in the Senate, and our bill takes many of these steps. So I appreciate the support we have received from the technology industry, and I look forward to hearing their perspective on the second panel.

Without objection, I will place in the record the open letter and reform principles from the technology companies, an earlier letter from technology companies applauding the USA FREEDOM Act,

and a supportive letter from a coalition of civil society organizations, companies, trade associations and investors. And without objection, they will be part of the record.

[The letters appear as submissions for the record.]

Chairman LEAHY. Support from the technology industry is representative of the broad-based, bipartisan support for our legislation. Organizations across the spectrum have endorsed the bill, from the ACLU to the NRA. I want to thank Senator Lee, Senator Durbin, Senator Blumenthal, and Senator Hirono for their cosponsorship.

This is bipartisan, it is also bicameral legislation. It is a commonsense bill that makes real and necessary reforms. So I want input on the legislation, and I look forward to working on this in the coming months. I do want to thank our witnesses for being here today, especially after we had the unexpected cancellation in November.

[The prepared statement of Chairman Leahy appears as a submission for the record.]

Senator Grassley, I know you have half a dozen conflicts on your schedule. I thank you for being here.

OPENING STATEMENT OF HON. CHUCK GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Thank you. Of course, this is a very important hearing, and you are doing the right thing by having the hearing because this is a subject of ongoing media attention and a lot of constituent interest.

We last held a hearing in early October. Since then, reports have continued to surface in the media about possible overreach on the part of Government. Some of the reports may be more accurate than others, but I continue to believe that many of them call into serious question whether the law and other safeguards currently in place strike the right balance between protecting our civil liberties and our national security. And that balance is a very important balance, but it is a balance that, for personal liberty as well as national security, both have constitutional implications. You cannot forget one or the other.

This is especially so concerning the public revelation that under Section 215 of the PATRIOT Act, the Government is collecting Americans' phone metadata in bulk.

Why are many Americans so concerned? Well, it is not hard to find an example of what can happen to Americans' personal information when the Government overreaches, mismanages, and fails the American people.

It has been 2 months since the administration tried to bring the Obamacare website online, and the American people are suffering under that issue. Many are finding they cannot keep the insurance plans they liked. Their premiums are rising, and uncertainty is growing about which parts of the law the President will decide to uphold.

But in just these few months, we have already seen reports of incidents where Obamacare has not adequately protected Americans' personal data. In one reported instance in Minnesota, an insurance broker was accidentally provided the personal information

of 2,400 people. Moreover, there are many unanswered questions about the website's ability to protect privacy going forward.

Now, I expect—in fact, I understand that the standards of the dedicated professionals in our intelligence community do not compare to those of the contractors who failed to set up the website that I have referred to. But it is easy to see why many Americans tend to be skeptical then that the Government can adequately maintain their privacy when it collects vast amounts of information.

The President's disengagement on these important matters does not help. He claims he was unaware of the problems with the Obamacare website before it was launched. Now reports say he was unaware of the reported surveillance of many world leaders.

As I did back in October, I call on the President to lead. Many of these programs are critical to our national security. The President needs to contribute to the national debate by publicly explaining and defending them. For instance, a visit to Fort Meade would help the morale a great deal.

It is good that there are numerous reform proposals that this Committee will have the opportunity to consider going forward. I am convinced there is a role for greater transparency, oversight, and accountability in the FISA process. The public trust in our intelligence community must be rebuilt. And, of course, we must ensure that intelligence authorities are exercised in a manner consistent with our laws and the Constitution.

These proposals should be subject to the same rigorous and critical examination to which we are subjecting the surveillance programs themselves.

These proposals should address the specific concerns that have been brought to light, not relitigate old and irrelevant legislative battles.

These proposals should not provide a terrorist abroad with rights similar to those of a U.S. citizen here at home.

These proposals should not make it more burdensome for authorities to investigate a terrorist than it is to investigate a common criminal.

And these proposals should not return us to a pre-September 11th posture. Then we did not adequately weigh the dedication, intelligence, and lethality of our foreign enemies, who are undoubtedly watching the debate very closely.

The balance between protecting individual liberties and our national security is a delicate one, and reasonable people can disagree about precisely where that balance must be struck, and that is our responsibility here in the Congress of the United States.

Our witnesses on both panels today represent a wide range of views, and I look forward to hearing their point of view. And before you start, Mr. Chairman, I would like to explain further something you brought up that I had a conflict. At 2:30, Secretaries Kerry and Lew are briefing Senators about the classified details of the controversial nuclear agreement the Obama administration has made with Iran. I am skeptical of that agreement, but I have a responsibility to learn more about it. But I have to weigh going to that hearing to be here because I also, as leader of the Republicans,

know the importance of FISA and whatever work is done there for our national security as well.

The Chairman did accommodate us to some extent by moving this ahead by a half-hour. I am going to stay beyond that half-hour anyway to ask questions, at least of the first panel. I had asked the meeting to be rescheduled, and it is the Chairman's prerogative to lead this Committee as he sees the necessity to do it. But I think it is too bad that this could not be worked out so that Senators could attend both of these matters together.

Thank you, Mr. Chairman.

Chairman LEAHY. Well, thank you, and I wish I could be at the other hearing, too, but we have had to reschedule this once already, and everybody has agreed to be here today, and I did not think it was fair to our witnesses to reschedule again. Besides, a lot of these classified briefings, like the one you just referred to, I have had to miss in the past because of conflicts, but I find I can usually read almost all of what was said there in the paper the next day anyway, usually in more detail.

Senator GRASSLEY. I agree with you on that point. But also it kind of makes a mockery of what they call "secured."

Chairman LEAHY. Well, it depends upon whose ox is being gored, I guess. It is more of a question of who can get it out quickest. I do recall one of these very highly classified matters that we had, and the very first thing that came up marked top secret was a photograph of the cover of one of that week's news magazines, and it went downhill from there.

Our first witness is General Keith Alexander, Director of the National Security Agency and head of U.S. Cyber Command. He began his service at the U.S. Military Academy at West Point, previously served as the commanding general of the U.S. Army Intelligence and Security Command, and Director of Intelligence, U.S. Central Command. And, of course, one, General, I thank you for being here. Your full statement will be made part of the record, but in the time you have, please feel free to hit any points you want or summarize in any way you would like.

STATEMENT OF HON. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, FORT MEADE, MARYLAND

General ALEXANDER. Chairman, thank you, and I will keep my opening remarks short, but I would like to hit a few key things.

First, NSA is a foreign intelligence agency. Those action tools that we do are to connect what we know about foreign intelligence to what is going on here in the United States. We need tools to bring that together. I want to talk briefly about some of those tools.

Some of those tools, like Section 215, in my opinion and I think in the Court's, our community, were authorized by Congress. They are legal, they are necessary, and they have been effective.

From my perspective, the threats are growing. When we look at what is going on in Iraq today, what is going on in Syria, the amount of people killed from 1 September to 3 December is over 5,000 from terrorist-related acts in Iraq, Syria, and several other countries around the world.

In Iraq alone, in 2012 the total number killed were 2,400. From 1 September to 3 December, that has risen to 2,200-plus in a 3-

month period. It is on the verge of a sectarian conflict. The crisis in the Middle East is growing, and the threat to us from terrorist activities, their safe havens, and those being radicalized are growing.

What we found out in 9/11—and I go back, Senator Grassley, to your comments—we cannot go back to a pre-9/11 moment. Sir, I absolutely agree with that. So we have to find out what is the right way for our Nation to defend ourselves and our allies and protect civil liberties and privacy. I think the way we are doing Section 215 is actually a good model, not just for our country but for the rest of the world. It has the courts, Congress, and the administration all involved.

Why do I say that? The reason is if you look at all the information that is out there, the billions and billions of books of information that are out there, there is no viable way to go through that information if you do not use metadata. In this case, metadata is a way of knowing where those books are in the library and a way of focusing our collection, the same that our allies do, to look at where are the bad books.

From our perspective, from the National Security Agency's perspective, what we do is get great insights into the bad actors overseas. Armed with that information, we can take the information, the to-from—and what I did is I put that on a little card. It says the from number, the to number, the date, time group of the call, and the duration. That is the elements of information we use in the 215. There is no content. There are no names, no email addresses.

From my perspective, that is the least intrusive way that we can do this. If we could come up with a better way, we ought to put it on the table and argue our way through it.

The issue that I see right now is there is not a better way. What we have come up with is can we change one.

But, Senator Grassley, you brought out a great point: 9/11, we could not connect the dots because we did not have this capability to say someone outside the United States is trying to talk to someone inside the United States.

Chairman LEAHY. We also had people in the administration that refused to listen to FBI agents who had picked up on what was happening here in the United States when they were told it was not important, even though anybody with a brain in their head would have known it was. But go ahead. I understand your point. And let us stick to the facts. We are not talking about a library. I had my first library card when I was 4 years old. I understand libraries. Let us talk about the NSA.

General ALEXANDER. Well, I think the important part for us, Mr. Chairman, is: How do you bring information that you know from outside the country to that which we have inside? How do you connect the dots? And that is the issue with the metadata program. There is no other way that we know of to connect the dots.

And so that gets us back to, do we not do that at all. Given that the threat is growing, I believe that is, an unacceptable risk to our country. So what we have to do is can we do more on the oversight and compliance? And there are things that are being looked at. But taking these programs off the table from my perspective is absolutely not the thing to do.

I do agree with this discussion with industry, as well, that you brought up, Chairman. Industry ought to be a player in here. They have been hurt by this, and I think unfairly hurt. We ought to put this on the table from two perspectives. Industry has some technical capabilities that may be better than what we have. If they have ideas of what we could do better to protect this Nation and our civil liberties and privacy, we should put it on the table. And I think we should have a way of bringing Government and industry together for the good of the Nation, and we ought to take those steps.

So, Mr. Chairman, I just want to end with this statement: We are a foreign intelligence agency. Our job is to figure out what is going on outside the United States and to provide that level of information to the FBI and others who are operating inside the United States. To date, we have not been able to come up with a better way of doing it.

I am not wed, I do not think anybody at NSA or the administration is wed to a specific program, but we do need something to help connect the dots, something that could help defend this country. And I think these programs have been effective.

That is all I have, Mr. Chairman.

Mr. COLE. Thank you, Chairman Leahy, Ranking Member Grassley——

Chairman LEAHY. I should have done an introduction. I apologize.

Mr. COLE. Quite all right.

Chairman LEAHY. James Cole first joined the Department of Justice in 1979, served for 13 years in the Criminal Division. He later became Deputy Chief of the Division's Public Integrity Section. Before entering private practice, he was sworn in as the Deputy Attorney General on January 3, 2011.

Please go ahead, Mr. Cole.

STATEMENT OF HON. JAMES M. COLE, DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. COLE. Thank you, Chairman Leahy, Ranking Member Grassley, and distinguished Members of the Committee, for inviting us here to talk about the Foreign Intelligence Surveillance Act. I am going to focus my opening remarks just on the 215 program.

As has been mentioned, it involves the collection of metadata from telephone calls, including the number that was dialed, the date, and the time of the call and the length of the call. It does not include the content of any phone calls, any names, addresses, or financial information of any party to the call. And under 215 it does not include any cell site location information.

The Government can search this data only if it has a reasonable, articulable suspicion that the phone number being searched is associated with certain terrorist organizations. Only a small number of analysts can make that determination, and that determination must be documented so it can be reviewed by a supervisor and later reviewed for compliance purposes. And only a small portion of these records actually end up being searched.

This program is conducted pursuant to authorization by the FISA Court. Since the Court originally authorized this program

back in 2006, it has been reapproved on 35 separate occasions by 15 individual Article III judges on the FISA Court.

Oversight of the 215 program involves all three branches of Government. Within the executive branch, numerous entities in NSA, the Department of Justice, and the Office of the Director of National Intelligence are involved in assessing compliance. We report any compliance incidents to the FISA Court immediately. With respect to Congress, we have reported any significant compliance problems, such as those uncovered in 2009, to the Intelligence and Judiciary Committees of both Houses. Documents related to those 2009 problems have since been declassified and have been released by the DNI.

Over the past several months, we have also gone to great lengths to better explain publicly why the program is lawful. Under Section 215, there must be reasonable grounds to believe that the records that are collected are relevant to an authorized investigation to protect against international terrorism.

As both the FISA Court's opinions and our own 22-page white paper explain, "relevant" is a very broad term. In its ordinary sense, information is relevant to an investigation if it bears upon or is pertinent to that investigation. Courts have held that large repositories of information can satisfy a relevance standard where the search of the whole repository is necessary in order to identify the critical documents. This is precisely the rationale that underlies the 215 collection program, and it was recognized by the FISA Court.

The Court found that the entire collection of bulk metadata is relevant to an authorized international terrorism investigation because it is necessary, a necessary part of the process to allow NSA to identify phone calls between terrorists and other persons.

As Judge Eagan's recent opinion reauthorizing the program recognized, and I quote, "Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced but can only be found after the production is aggregated and then queried using identifiers determined to be associated with the identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity."

In addition to complying with 215, NSA's program must also comply with the Fourth Amendment of the Constitution. Here the Supreme Court's decision in *Smith v. Maryland* is directly on point.

In *Smith*, the Court held that telephone users who convey information to phone companies for the purpose of routing their calls have no reasonable expectation of privacy in that information.

Now, the *Smith* case was a number of years ago, and some have questioned the applicability of it because it did not concern a situation where the Government collected and retained the bulk metadata and aggregated it all in one place. However, a recent opinion of the FISA Court addressed this specific issue, and it noted, "Where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly situated individuals cannot result in the Fourth Amendment interest springing into existence."

I understand that there is interest in legislating reforms to the 215 program and other aspects of FISA, including the nature of the

Court process itself. We welcome this public debate and this public discussion about whether the current version of 215 and other provisions of FISA strike the right balance between our national security and the privacy of our citizens, both of which are important and have to be honored. We look forward to working with the Committee to address these issues and to find the right balance.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you. Thank you very much, Mr. Cole.

And our last witness on this panel will be Robert Litt, confirmed by the Senate in 2009 to serve as General Counsel of the Office of the Director of National Intelligence. Prior to joining the ODNI, he was a partner with the law firm of Arnold and Porter, worked at the Department of Justice, and has testified before this Committee before. Welcome back, Mr. Litt.

STATEMENT OF HON. ROBERT S. LITT, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, WASHINGTON, DC

Mr. LITT. Thank you, Mr. Chairman, Ranking Member Grassley, Members of the Committee. We do appreciate the opportunity to appear today to continue our discussions about the intelligence activities that are conducted pursuant to the Foreign Intelligence Surveillance Act.

It is critical to assume that the public dialogue on this topic is grounded in fact rather than in misconceptions, and we, therefore, understand the importance of helping the public to understand how the intelligence community actually uses the legal authorities provided by Congress to gather foreign intelligence and the extent to which there is vigorous oversight of those activities to ensure that they comply with the law.

As you know, the President directed the intelligence community to make as much information as possible available about certain intelligence programs that were the subject of unauthorized disclosure, consistent with protecting national security and sensitive sources and methods. Since that time, the Director of National Intelligence has declassified and released thousands of pages of documents about these programs, including court orders and a variety of other documents. We are continuing to do so. These documents demonstrate both that the programs were authorized by law and that they were subject to vigorous oversight, as General Alexander said, by all three branches of Government.

It is important to emphasize that this information was properly classified. It has been declassified only because in the present circumstances the public interest in declassification outweighs the national security concerns that originally prompted classification.

In addition to declassifying documents, we have taken significant steps to allow the public to understand the extent to which we use the authorities in FISA going forward. Specifically, as we describe in more detail in the written statement that we submitted for the record, the Government will release on an annual basis the total number of orders issued under various FISA authorities and the total number of targets affected by those orders. Moreover, we recognize that it is important for companies to be able to reassure their customers about how often or, more precisely, how rarely the

companies provide information to the Government. And so we have agreed to allow the companies to report the total number of law enforcement and national security legal demands they receive each year and the number of accounts affected by those orders. We believe that these steps strike the proper balance between providing the public relevant information about the use of these legal authorities while at the same time protecting important collection capabilities.

A number of bills that have been introduced in Congress, including the USA FREEDOM Act, which you have sponsored, Mr. Chairman, contain provisions that would require or authorize additional disclosures. We share the goals that these laws and bills provide of providing the public with greater insight into the Government's use of FISA authorities. However, we are concerned that some of the specific proposals raise significant practical or operational concerns.

In particular, we need to make sure that any disclosures are operationally feasible with a reasonable degree of effort, and that they would provide meaningful information to the public. We also need to make sure that the disclosures do not compromise significant intelligence collection capabilities by providing our adversaries information that they can use to avoid surveillance.

But, Mr. Chairman, I do want to emphasize our commitment to work with this Committee and others to ensure the maximum possible transparency about our intelligence activities consistent with national security. We are open to considering any proposals so long as they are feasible and do not compromise our ability to collect the information we need to protect our Nation and its allies. And we have been in discussion with the staff of this Committee and the Intelligence Committee on some proposals and some alternate means of trying to provide greater transparency while protecting our critical sources and methods.

We look forward to continuing to work with you in this regard. Thank you.

[The prepared joint statement of General Alexander, Mr. Cole, and Mr. Litt appears as a submission for the record.]

Chairman LEAHY. Thank you, Mr. Litt.

Normally I would ask questions at this point, but I am going to yield first to Senator Grassley, who does want to make the other briefing. Senator Grassley.

Senator GRASSLEY. Yes, and I appreciate very much that accommodation.

Mr. Cole, back on October 2nd, I wrote a letter to the Attorney General requesting information about cases of willful and intentional abuse of authority by NSA employees. Some of them were referred to the Justice Department for prosecution. I would like to know whether these cases were prosecuted and, if not, why not. I asked for a response by December 1st. Do you know the answers to these questions? And if not, when would I be able to expect an answer?

Mr. COLE. I do not know the specific answers on each of the ones you cited, Senator Grassley, but we are in the process of collecting that information. A number of them were not prosecuted. A number of them involved the risk of further damaging the national se-

curity by having to release more information. Other sanctions were found that were adequate in those cases. But we are trying to put together that information so that we can give you an assessment of what happened in those cases.

Senator GRASSLEY. I thank you for that courtesy.

Mr. Cole, I want to make sure that I understand the administration's positions on the USA FREEDOM Act. In your prepared testimony that bill is not specifically mentioned, but in your testimony you state that the administration "does not support legislation that would have the effect of ending the . . . 215 program" because the administration maintained that it is lawful and valuable to protect national security. The answer may be obvious, but I want to be clear for the record. Do you understand the USA FREEDOM Act to be "legislation that would have the effect of ending the Section 215 program" that you described in your testimony?

Mr. COLE. Senator, you have kind of asked me a legal question. I am going to have to give you a bit of a lawyer's answer. It is going to depend on how the court—if the USA FREEDOM Act becomes law, it is going to depend on how the court interprets any number of the provisions that are in it and any number of the additional requirements that are contained in it over what is here and now. I think it will have an impact on what is currently done under 215, but 215 covers more than just bulk data collection. It covers individualized Business Records acquisition. And depending on what kinds of records are being sought, what the facts and circumstances are, will depend on the nature and extent of the FREEDOM Act's impact on it.

On the bulk data, I think it is going to be a question of the court's interpretation. Right now the interpretation of the word "relevant" is a broad interpretation. Adding "pertinent" to a foreign agent or somebody in contact with a foreign agent could be another way of talking about relevance as it is right now. We would have to see how broadly the court interprets that, or how narrowly.

Senator GRASSLEY. I appreciate your legal view. Just from the standpoint of how our process of legislation works and since the President is Commander-in-Chief, the number one person in charge of our national security, I would hope that we would have a firm statement from the administration of whether or not this legislation is harmful or not, and it would be better to know that before courts get a decision, which would be years down the road, than it would be now. And I think that the administration owes that to all of us, both proponents and opponents, of what that situation is.

My other question to you as well, other than 215, the USA FREEDOM Act would also make other significant changes to the tools used to investigate terrorism and espionage cases. For example, the bill would raise the legal standard to issue national security letters to require that the information sought be both relevant and material as well as the information pertained directly or indirectly to a foreign power or an agent of that power. This is a change from the current standard, which is mere relevance.

Question: What operational effect, if any, will these changes have on the ability of your Department and the FBI to protect the Nation from terrorist attacks?

Mr. COLE. Senator Grassley, probably the largest effect that it would have on the NSL situation is the addition of the requirement that it be relevant to or there is information that it is connected to a foreign power. Many times NSLs are used in a very preliminary stage of an investigation in order to determine if the person who is being looked at is, in fact, a foreign power or an agent of a foreign power. And so the question is sometimes being answered through the use of national security letters. If you must answer that question before you can get a national security letter, it would reduce the availability of that tool in terrorism investigations.

Senator GRASSLEY. Thank you, Mr. Chairman. And I have two questions that I will submit for answer in writing—can I ask one more?

Chairman LEAHY. Certainly.

Senator GRASSLEY. Mr. Litt, one of the issues this Committee has been looking at is whether or how to add more of an adversarial element in the FISA Court process. The Chairman invited a former FISA Court judge to be a witness at our hearing in July. Judge James Carr explained in his answers to questions for the record that he did "not believe that having independent counsel review all Government applications before the FISC would be necessary or desirable." This appears to be an approach reflected in the legislation that was passed by the Senate Intelligence Committee. In contrast, as I understand it, the FREEDOM Act requires the Government to provide every application to the advocate.

Question: Between the different advocates proposals in the USA FREEDOM Act and the Senate Intelligence Committee bill, which do you believe is a better approach to making the FISA Court process more adversarial? And why?

Mr. LITT. So, Senator Grassley, since the Department of Justice is the agency that really conducts the litigation before the FISA Court, I am going to defer the answer to that to Deputy Attorney General Cole, although I will say that there has been a lot of interagency discussion about the appropriate approach there, which I think he can lay out.

Senator GRASSLEY. Okay.

Mr. COLE. Senator Grassley, as I think we have said on a number of occasions, we find that there is a use and a value to having an independent legal representative in the FISA Court process in the appropriate circumstances. We would not advocate or recommend having one for all of the procedures that go on there. Many of them, like in normal criminal cases, are routinely done in an ex parte basis. They are done usually with a fair degree of expediency and efficiency, and we think a permanent public advocate might impede that process some of it is applying to every single thing that is there. There would also be, I think, some constitutional issues of standing for a public advocate on every single issue.

We would propose that it be an amicus appointed by the Court. When the Court feels that they have the need for another perspective and another point of view, when it is a significant issue involving privacy issues, civil liberty issues that the Court would like to have another view on, that would be a good example of a time. Something like the bulk data collection programs where somebody

may want to have a view of what the law is other than the Government's view, we think that would be a good area.

But I think the Court is in the best position to determine when and where it is going to need those kinds of things and do it only for those issues.

Senator GRASSLEY. General Alexander, it will take you 5 seconds to answer this question. At our hearing in July, your Deputy Director testified that the NSA was conducting an investigation into how so highly classified information was compromised by a single contractor. He stated the NSA would report back to Congress about individual and systemic responsibilities of what occurred. When can we expect that report?

General ALEXANDER. We will send that up right away. We have actually taken 41 different actions, and we will get you a report on what those are.

Chairman LEAHY. What is "right away"?

General ALEXANDER. Over the next week.

Chairman LEAHY. Okay. So we will have it by Wednesday.

Senator GRASSLEY. Thank you, Mr. Chairman.

General ALEXANDER. Next Wednesday.

Chairman LEAHY. By then. Thank you.

Senator GRASSLEY. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Going back to the penultimate question about 215 phone records and FISA Courts or FISC courts and so on, it has been said these have always been authorized, and they have never been up on appeal. We have never had an appellate court rule on them. The bill that I have does not require an advocate in every FISA Court case. It would be only when the Court agreed that it might be helpful.

We also have statements from judges that, if that was the case, there may be more credibility with the courts, or at least more of a willingness on the part of the public to accept courts that operate in secret.

Would you agree with that, Mr. Cole?

Mr. COLE. I think that that would help the public have better confidence. I think the Court does run well. I think there is a great deal of independence from my experience with the Court in its rulings. It is not by any means a rubber stamp. But I think there is a value with the public to having some other person, some other advocate in the appropriate kinds of cases, and I think there is a value to that, Senator, Mr. Chairman. So I think that is a good idea as long as we keep it in the right matters. So I would agree with that.

Chairman LEAHY. And Senator Klobuchar will submit her questions for the record, and I would ask them to be answered as quickly as possible.

[The questions of Senator Klobuchar appears as a submission for the record.]

Chairman LEAHY. Now, we get in these press accounts that the NSA is collecting billions of cell phone location records every day and is reportedly gathering information or communications information from online gaming sites. The stories suggest the activities are directed abroad. We know the NSA was making plans to obtain cell site location information under Section 215. We also know that

the NSA engaged in bulk collection of Internet metadata under the FISA pen register statute. So it suggests to me that under that kind of a legal interpretation of FISA, the NSA could collect the same massive amounts of information domestically that these recent stories suggest they are collecting abroad.

So, Mr. Litt, maybe I should direct this first at you. I know the program authorized the bulk collection of email and other Internet metadata was shut down in 2011 because it was not operationally useful. But under current law, would the NSA be able to restart the bulk collection of Internet data?

Mr. LITT. I think that if the NSA and the Department of Justice were able to make a showing to the FISA Court that the collection of Internet metadata in bulk, which, of course, is a category of information that is not protected by the Fourth Amendment, that if it were relevant to an authorized investigation and could convince the FISA Court of that, then, yes, it would be authorized.

Chairman LEAHY. It was shut down before because of not being operationally useful. Would you have to go to the Court?

Mr. LITT. I believe we would have to——

Chairman LEAHY. To restart the bulk collection of Internet data, would you have to go to the Court?

Mr. LITT. I believe we would.

Chairman LEAHY. Mr. Cole?

Mr. COLE. Yes, Mr. Chairman. Under the FISA statute, I think you would have to get Court authority, just like you would under 215, to be able to do that, and that would only last for a period of time and have to be renewed periodically. So there is no active authority for it right now.

Chairman LEAHY. Thank you. And setting aside any technological limitations, would the FISA pen register statute authorize you to obtain all Internet metadata, not just email metadata?

Mr. COLE. I think that is correct, but, again, it would be limited to the metadata in that regard.

Mr. LITT. And if I could just add on that——

Chairman LEAHY. If I can just make sure I understand Mr. Cole's answer. So the only limitation would be that it be metadata?

Mr. COLE. It cannot be content. It cannot be—and the latest order of the FISA Court under 215, it specifically excluded cell site location as well.

Chairman LEAHY. Thank you.

Mr. LITT. I was going to add only that you would have to show that the category of metadata that you are seeking was, in fact, relevant to the authorized investigation.

Chairman LEAHY. Okay. Well, Mr. Cole, you talked about the legislation that Senator Lee and I have talked about to update the Electronic Communications Privacy Act. We want to require in criminal matters—I am talking about just criminal matters now—that the Government obtain a probable cause warrant to gain access to the contents of electronic communications that are stored by a third-party provider. Section 215 of the USA PATRIOT Act requires the Government to show only relevance to an authorized intelligence investigation in order to obtain records. I am not talking about bulk collection but the more standard usage of 215.

Has Section 215 ever been relied upon to obtain the contents of stored communications from a third-party provider?

Mr. COLE. Not that I am aware of, Mr. Chairman.

Chairman LEAHY. Mr. Litt?

Mr. LITT. I am hesitant to give an answer to that just because it is not a question I have ever asked. I would prefer to get back to you on that, sir. I just do not know the answer sitting here.

Chairman LEAHY. Can you get back to me by the end of the week?

Mr. LITT. I will try.

Chairman LEAHY. If they have not, as a legal matter, could Section 215 be used to obtain the contents of communication?

Mr. COLE. I would have to think about that, considering that it is limited to the types of information you can get with a grand jury subpoena. I would have to look—because of the aspects of stored communication and things of that nature, I would have to check. But I am not sure—I would have to go back and look at that. So without a check of the legal authorities, I will get back to you on that, Mr. Chairman.

Chairman LEAHY. And I appreciate you checking those. I think you understand by the question I——

Mr. COLE. Yes.

Chairman LEAHY. There are some serious legal ramifications to your answer.

Mr. COLE. I agree.

Chairman LEAHY. Well, good.

Chairman LEAHY. I am going to yield to Senator Franken, but, General Alexander, you talked about using—and I will get to you in my next round—about going to the private sector looking for best practices from them. You can imagine I am going to ask if those best practices had been used, would a 29-year-old subcontractor have been able to walk away with all your secrets like Mr. Snowden did.

Senator Franken.

Senator FRANKEN. You are going to ask that in the next round?

Chairman LEAHY. Sure, but——

Senator FRANKEN [continuing]. Do you want it answered now?

Chairman LEAHY. No. That is okay. I do not want to take—you have been waiting patiently. I will wait my turn.

Senator FRANKEN. Well, okay. General, you will have plenty of time to think about that, except I have a question for you, so we will see if you can do both at the same time.

I have a bill, too, called the Surveillance Transportation Act that I think you are all familiar with. Among other things, General Alexander, the bill would require NSA to tell the American people how many of them have had their communications collected by the NSA. Do you think that the American people have the right to know roughly how many of them have had their information collected by the NSA?

General ALEXANDER. I do, Senator. I think the issue is how do you describe that. Those that are under a court order—so under FISA, as you know, to collect the content of a communication, we have to get a warrant. The issue would be almost in the Title III court. Do you tell someone, a U.S. person, who may not be a U.S.

citizen, that we are tracking them here in the United States or that we have identified that?

Senator FRANKEN. I am not suggesting that you have to tell people they are being surveilled, that they personally are a suspect. What I am saying is, do the American people have a right to know how many American people have had their information collected? That is a different question. I was not suggesting we tip people off that are suspects.

General ALEXANDER. Yes. So I think in broad terms, absolutely, and let me give you an example.

Senator FRANKEN. In broad terms?

General ALEXANDER. Yes. So, for example, under 215 today, less than 200 numbers are approved for reasonable, articulable suspicion, are being searched in that data base.

Senator FRANKEN. Two hundred.

General ALEXANDER. Numbers.

Senator FRANKEN. People—that is 200 orders or 200 people?

General ALEXANDER. Two hundred numbers. Some of those numbers may be multiple numbers per person. Those numbers could be both foreign and domestic. In fact, they are. But that is the total number for that category for Section 215 today under that program.

The other one that I think—and I think the Deputy Attorney General mentioned, is we can also put out more about what we are doing under the FAA 702 program, that we have compelled industry to do in a more transparent manner. The issue is how do we do that without revealing some of our own capabilities. And we are working through the interagency to get resolution on that.

Senator FRANKEN. Okay. I am being told by staff that that is actually the number of people that have had their phone numbers searched, not collected. Right?

General ALEXANDER. So under 215, all the data is going into a repository.

Senator FRANKEN. Metadata.

General ALEXANDER. Metadata. So, if, for example, I am talking to a foreign terrorist, my number would automatically hit that link. In fact, you probably would want to know that.

Senator FRANKEN. Right.

General ALEXANDER. I know the White House would.

Senator FRANKEN. We need to know that.

General ALEXANDER. That is right. So the issue would be how many of those. What we would do is we would look at those and, based on our analysis, give those numbers that are appropriate to the FBI for them to then go through their appropriate process to look at those numbers.

Senator FRANKEN. Okay. There is a difference between collected and searched, but that is—okay. But let us talk about 702. That is supposed to target non-Americans, right? Foreign persons?

General ALEXANDER. Reasonably believed to be outside the United States.

Senator FRANKEN. Right. Are Americans—shouldn't the American people know how many Americans have gotten caught up in that?

General ALEXANDER. That again is—and I do not mean to hedge. Let me just tell you the difficulty. If a terrorist that we are going after is talking to another person, in that communication there is nothing that says, "I am an American, and here is my Social Security number." So the fact is when we are tracking a terrorist, if they are talking to five people and one of those is American, chances of us knowing that are very small.

If we find out that it is an American, then there are procedures that the Attorney General and the courts have given us that we have to do to minimize that data on that American.

Senator FRANKEN. Okay. Well, I guess my question is that my bill calls for the NSA to report how many Americans' information has been searched, has been looked at by agents. And I am not talking about necessarily a precise number, but 702 says that it can only look at non-Americans. And, look, my feeling is this: that the American people are skeptical of executive power.

General ALEXANDER. Right.

Senator FRANKEN. That when there is a lack of transparency, they tend to suspect that something—they tend to be very skeptical and suspect abuse. And part of the reason to have transparency is for people to be able to make their decisions based on some real information about whether or not this power is being abused or not.

Now, I believe that you gentlemen have our national security at interest—that is your interest. That is your interest. But I also believe that—you know, you keep saying there are three—there is oversight from all three branches of Government. We are one of the branches, and we are doing the oversight. Okay?

General ALEXANDER. We are feeling it.

Senator FRANKEN. And my feeling doing the oversight is that I would be more comfortable and that the American people would be more comfortable and feel that they can decide for themselves, if they knew how many Americans were being caught up in a program like 702 that is designed by law not to target Americans.

General ALEXANDER. So I think, Senator, absolutely. But I would just put into this that what we are going to do is, if asked to do that, we are going to give you faithfully and truthfully that which we know. And my concern would be, 2 days later, we find out that was also an American, so we could report that later, but we are not going to—do you see what I mean?

Senator FRANKEN. Because what I am talking about in my legislation is not a precise number. It is a range.

General ALEXANDER. Yes.

Senator FRANKEN. And what I have been told by ODNI is that producing this estimate would be very difficult. But I do not think it would be that difficult.

General ALEXANDER. So it may be. I would just offer, Senator, to have you come up and we could sit down and show you this and then come up with perhaps a reasoned way to do that, because I do think—actually, I agree with you. I think this is the right thing to do, because the number is not that big. And I think if we could explain it to the American people, and you as one of our three elements of our Government could say, "Here is what we see, and here is what the administration sees, and here is what the courts

and all three of us together see, that is the best number we can come up with." When you see that, when the American people understand that, they will know we are doing this right. So I agree with you.

Senator FRANKEN. I see Mr. Litt, whom I know quite well—we have discussed this a lot—sort of jumping out of his seat.

Mr. LITT. No. I am firmly planted, sir.

Senator FRANKEN. Okay. Well, eager to answer, and that is why I am afraid I have run out of—no, I am sorry. Go ahead.

[Laughter.]

Senator FRANKEN. Go ahead. I see that you are—I have never seen him this eager, frankly.

Mr. LITT. Mr. Chairman, if I might for a minute, this is a good example of the kind of thing I was talking about in my opening remarks. I think we all agree that the question you pose is a reasonable one, which is, How many Americans are being caught up in this?

The problem is trying to find a way to provide that information in a manner that is both operationally feasible and does not compromise sources and methods. We have got some ideas in that regard. They are not fully fleshed out yet. We do want to work with your staff and see if there are ways we can arrive at something that will give at least some sort of reasonable proxy that gives Americans an idea of what the impact of this surveillance is.

Senator FRANKEN. Thank you. I am glad I have got this answer today because this has been part of my discussions with ODNI where you said that this may be too difficult to do. But it sounds like we have got a little bit of movement on this.

I wanted to ask a question about what you were referring to, Mr. Chairman, about location information. But I really am way over my time.

Chairman LEAHY. You may go ahead.

Senator FRANKEN. Thank you for your indulgence.

This is on the capacity issue. General Alexander, in a hearing—let me go beyond that. Last week, The Washington Post asked an intelligence official speaking on the record to estimate how many Americans had had their location information collected by the NSA. The official answer: "It is awkward for us to try to provide any specific numbers." Right after he said that, the article says that an NSA spokesman interrupted the conversation to change that answer.

Do you believe it is difficult for this administration to estimate how many Americans have had their information collected, or do you think it is awkward?

General ALEXANDER. I think it is difficult, but I think we are walking by each other. If I might explain?

Senator FRANKEN. Okay. Good.

General ALEXANDER. Under the Business Records FISA, there was a series of questions on cell site location information that Senator Wyden and others had asked, and we have walked down that road. As you know, that is one that the Court said, "We are not doing that. We do not do that." There has been a few records that were done to check to see if technically it could be done. That was the first set of issues on the Business Records FISA. So there is

no cell site location data under Business Records FISA that we are using today, period.

Second, if an American travels overseas and his communications are collected, the chances are in that collection we may not know that that has been collected, that it was an American person; but the chances are if you collect A, you will probably get the cell site location with that because that is something that is also collected. The issue would be how many of those have been collected, and the answer is we are really not looking for that. It may have been collected because they talk to—you know, as we use—and I do not mean any of these people are bad. I am just using this——

Senator FRANKEN. You seem to point to them a lot.

[Laughter.]

General ALEXANDER. I just want you to be careful because they are right behind you. But I am concerned, Senator, that in that case we will not know at all who are the Americans and who are not in those issues for the same reasons as before. But what we can tell you is I think good numbers on those that we target overseas that are Americans under those procedures that we have. We can give you those numbers, 703, –4, and –5 that fall into that. And I think that is perhaps what we are really looking for. Does that make sense?

Senator FRANKEN. Yes. Thank you. And, Mr. Chairman, thank you for your indulgence. I also want to go down to the briefing. Thank you, gentlemen.

Chairman LEAHY. Say hello to everybody for me.

Senator FRANKEN. I will.

Chairman LEAHY. General, to go back to the question I asked, and not facetiously, I assure, when you said that your work with private industry on proving techniques and so forth, and I assume you would. Let us go back to the Snowden case. As you know, I have expressed grave concerns about how a 29-year-old subcontractor can come walking in and that your system of checks and balances and all was not good enough to stop him from walking out with a huge amount of data. I see something similar, although a different type of data, when our own State Department and Department of Defense put huge numbers of highly classified and highly sensitive cable traffic from some of our embassies into one location where a private first class, I believe he was, was able to go in and take it all out on a Lady Gaga CD. And we know the enormous, enormous problems caused to our diplomacy and the security of a lot of Americans and our allies because of that situation. I have never found anybody to say what we ever gain by putting all that material in one place.

So now we go to the Snowden case. Whether somebody thinks he is a hero or a villain is not so much the question as it is, I think we can all agree, that a lot of the material that has been released because of him has been very damaging to the United States. It has certainly been damaging to our allies, our relationships with our allies.

I realize, as you and others do, that some of our allies have said how terrible it is we are doing this. It has to make one think of the scene in the movie, "Casablanca": "I am shocked, shocked, to see this going on," knowing that they are doing very similar things.

But having said that, there were things that created grave problems for us.

So my question is: First, can you say with confidence that you now have checks and balances at NSA to stop something like this happening again? And, second, has anybody been disciplined at NSA for dropping the ball so badly?

General ALEXANDER. So, first, Chairman, on the checks and balances and the things that we have done, that is the 41 different actions that I discussed for Senator Grassley that our technology director is using. That does employ best industry and best practices that we have and has drastically improved that capability.

Chairman LEAHY. These are subsequent to the Snowden——

General ALEXANDER. That is correct. This is all since the Snowden thing. This gets into compartmentalizing and encrypting data to creating communities of interest. And we do have three cases that we are currently reviewing, working our way through, that I do not want to prejudge given my position.

Chairman LEAHY. I understand.

General ALEXANDER. That we will fully inform this Committee of action that we have taken once that action is complete. So we are doing that.

Chairman LEAHY. Now, first off, whether it is 41 steps or 35 or whatever, I would hope that this makes it better. The obvious question comes up: Why were these steps not taken before? Was it because there is a sense of confidence that we are the NSA, we will not make a mistake? Or was it just—well——

General ALEXANDER. Well, actually, Chairman, the reason it happened is his job was to move data. He was the person who was to move the books from Point A to Point B. He was the SharePoint server, Web server administrator. His job was, in fact, to do what he did. And therein lies part of the problem.

We had one individual who has the responsibility to move that data who betrayed that trust. We believed that they would execute that duty faithfully and in a manner that everybody had agreed should be done.

Chairman LEAHY. To use your analogy, General, let us say I run a company that sells millions of dollars worth of diamonds, and I am going to have to transfer them from my warehouse in this State to my warehouse in this State. Now, am I negligent if I say, well, look, we have got this 29-year-old subcontractor, here are the keys to the car, the truck that carries all these diamonds, get them there safely; by the way, here is a map? Or is it better off that I have two or three people who check on how it gets there?

General ALEXANDER. So prior to this event, it was standard that one person would do one job, and he would have back-up help, and you would have oversight of that. But in doing that job, it is very difficult, if not impossible, to see that person replicates a copy of what he took. A little bit different than in the diamond case, but your point is well taken. You would not give the guys the key to the car to drive your diamonds across State—especially when you did not know. In this case what we have done is we have input a two-person rule just like you would for that for these specific issues, and you will see that in parts of the write-up.

I would also point out one of the notes I got, from the WikiLeaks we were already implementing the WikiLeaks issues that had been found through the interagency process. So we were implementing that. This specific vulnerability that he exploited was not found in the WikiLeaks area. And there were some specific things that I would prefer not to go into here because——

Chairman LEAHY. Can I suggest that there are still going to be people out there who are going to want to find more things? Would we both agree on that?

General ALEXANDER. Absolutely.

Chairman LEAHY. I think we would also agree that the vast majority of people who work with you—and I do believe this—are very honest and would not want to do anything to betray the country they serve. Is that correct?

General ALEXANDER. Absolutely, Chairman.

Chairman LEAHY. Thank you.

We talked about the legal standard for bulk collection programs, and that is one thing. The other thing is, do we really need to be collecting massive amounts of data on innocent Americans to keep us safe? Just simply because you can do something, does it make sense to do it?

We had a question on an entirely different matter before this Committee once when I had raised the question about road blocks being set up by our border people in Vermont on one of our interstate highways about 40 or 50 miles from the Canadian border. And they said with great enthusiasm, well, over a period of X amount of time, they found four or five illegal immigrants and collected X amounts of marijuana and some cocaine. I said, "Wonderful." They spent a huge amount of money and set up this road block, inconveniencing everybody. I said, "Look how much more you could collect if we set up those road blocks on every single bridge coming into Washington, DC, in the morning. A couple hundred thousand, 100,000, 200,000 people come in from Maryland, same number from Virginia and West Virginia, unless we have something, a cataclysmic thing like 2 inches of snow, and then, of course, we have to close." In Vermont, anything under 5 inches of snow is called a "dusting." But I digress. But the fact it——

[Laughter.]

Chairman LEAHY. But not much. The fact is if we set up those kind of road blocks, we would collect hundreds of illegal immigrants. We would collect huge amounts of illegal drugs and probably other contraband. Would we do it? No. I mean, the place would come to a screaming halt, and there would be those people who are totally innocent and all who might be screaming about it, including Chairs of various oversight committees.

But my point is we have already established that the Section 215 phone records collection program was uniquely valuable in just one terrorism-related cases, not the 54 that have been talked about before. The NSA shut down a bulk collection program related to Internet metadata because it was not meeting operational expectations. And I was concerned to learn that the NSA has never done an assessment of the effectiveness about collection under Section 702 despite the fact the program mistakenly led to the warrantless collection of thousands of domestic emails, including their contents.

We can do a huge amount, but then at some point you have to ask, What do we get out of it?

So, General, I would ask you this: Shouldn't the NSA assess the utility of its various collection methods in a systematic way, especially if they pose a risk of obtaining Americans' communications? The question would be very simple if we were talking about going into everybody's home to look at their letters and their files and their most personal things. But somehow we are looking at it differently because it is out there electronically.

General ALEXANDER. Senator, Chairman, that was exactly why under the Pen Register/Trap and Trace the email metadata program, when we looked at that, we—and I was the key NSA official to say this program does not meet the operational requirements for the amount that we are putting in, and we recommended to the DNI and the White House that we stop that and inform Congress. So we made that operational decision based on what we got for what we put into it to what it cost us.

We did the same, we are doing the same on the Business Records FISA, the metadata program, and we looked at that. Here is the issue, quite candidly, that I am wrestling——

Chairman LEAHY. You are doing that now in the PRTT?

General ALEXANDER. We did the PRTT back in 2011 when we stopped that program, and that was based on my recommendation based on working with our people to look at what we are doing.

Chairman LEAHY. Did you find any terrorism plots it helped thwart?

General ALEXANDER. With the Pen Register/Trap and Trace? I will have to go back and get you the specifics on that. That will take more than Wednesday, though, but I will get you that answer.

Chairman LEAHY. Okay, because I am thinking, when Deputy Director Inglis testified, there was only one time where Section 215——

General ALEXANDER. Right, so that is Section—now we are going to 215. The issue that I have on 215 and why I am so concerned, I agree that what Congress, the courts, and the administration have given us here is extremely intrusive taken in its whole. But the way we have put the oversight and compliance and the regimen that we have around it and the oversight by the courts, the administration, and Congress ensure that we are doing this right. And the frequency that we look at that, less than 200 numbers now approved, and less than 300 for all of 2012, from my perspective that shows that we are being judicious in how we do it, there is oversight by all three branches of the Government, and complete auditability on every action that we do.

We do not have a better way of doing this, so that goes into that question of industry. So my question is: I do not know a better way to do it, and I am being completely candid. I am concerned with all that our country is going to face that we will have failed the Nation if an attack gets through.

And so you have asked us to do that. I cannot think of a better way. I think this is where industry—do they have a better way of doing it? We ought to put it on the table and argue that through all branches of the Government. Nobody has come up with a better way.

And so that is my concern with the metadata program that we have today. I cannot think of a better way. It is like holding on to a hornet's nest. You know, we are getting stung. You have asked us to do this for the good of the Nation, to defend the Nation, to get the intelligence we need. Nobody has come up with a better way. If we let this down, I think we will have let the Nation down. So that is why I am concerned.

Chairman LEAHY. General, I realize the world changes, but I think back to my days as a young prosecutor, and without going into war stories, I remember when as a member of the Executive Board of the National DA's Association, we had a meeting with J. Edgar Hoover, and four or five of us there, we went across the spectrum politically. We were all chilled by what we heard from him: his disregard of the Constitution, his willingness to do things—he explained to us there was no such thing as organized crime in America, even though, of course, there was a massive organized crime operation at that time. But we had to fear Communists. He even suggested to us that The New York Times and its editorial policy was very close to becoming a Communist newspaper and he was about to investigate it as such. I am serious. I am always thinking what it would have been like if he had had the power that you and the NSA have.

I had a friend who died in the Towers on 9/11. I think about that all the time. I think of my wife, who was a medical-surgical nurse at Arlington Hospital, going there, even though she had retired, to volunteer to help with any wounded coming from the Pentagon and being told there were no wounded. You were either alive and walking or you were dead. There was nothing in between. These things sear in your mind. You do not want this to ever happen again.

But I also think of the J. Edgar Hoover type thing, and I think as an American it is very easy to go to another country and complain to them about their police state—and I am not suggesting that that is what you are, but their ability to go and listen in on everybody, search everybody. We give up a lot of our privacy in this country, and frankly I worry about giving up too much. And can we be totally secure? Of course we cannot. You cannot be totally secure going out to dinner in the evening from some random shooter who is not even aiming for you.

So, I mean, I look at the administration declassifying a number of FISA Court opinions, and they get credit for doing that, but there has been no release of any FISA Court opinion from the 2006 time period containing legal and constitutional analysis of the Section 215 phone records program. Is that because it did not exist or it has not been declassified? And I ask this question—and I will let Mr. Cole give me an answer to that at some appropriate point. But I really feel that our oversight has not been adequate or that so much of it is done secretly that it is too easy to say if you knew what we knew, you would not ask us questions. And I worry as technology gets greater and greater, the temptation, whether it is this administration or the next administration or the administration after that, to people to misuse it.

So I know I have been critical of these things. I hope none of you take it personally. But as a Vermonter, I am very concerned about my privacy and everybody else's.

Did you want to add anything, Mr. Cole or Mr. Litt or General?

Mr. COLE. Mr. Chairman, you know, I think that we are all concerned to make sure that we get this balance right and that an important part of that balance is transparency to the American public, keeping their trust in what we are doing, making sure that while doing that we do not compromise our abilities to be able to use classified techniques that will help keep them safe. But that is—there is a tension between those two, and there always has been. And finding that right balance is always something that is difficult, but it is our job. And it is our collective job in all three branches of Government, including with oversight from the U.S. Congress as a very important part of that.

So I think the path that we are on now is very much the one that you are describing of trying to make sure that we find that line and find that balance of giving the information that we can give, providing the transparency while maintaining the operational integrity of what we are doing. We should not be saying to you, particularly from an oversight function, if you only knew what we knew, you would say we are doing fine. We should be in a position to be able to tell you what we are doing.

Mr. LITT. Mr. Chairman, if I can just add a couple of points there. The first is that, as I am sure you know, there is nobody in the intelligence community today who operates on the assumption that you ascribed to J. Edgar Hoover before, "I do not care what the Constitution says." Everybody is singularly focused on ensuring that we comply with the Constitution and the law. And as you know, in all the material that has come out, there has been no suggestion of any willful abuse or violation of privacy of people. The compliance violations that have occurred have been technical, they have been unintentional, but nobody has been out there attempting to illegally spy on Americans or anything else.

But the other point I want to make is sort of a more philosophical one, because the point you raise about worrying about the next person is, of course, something that was a concern all the way back to the Framers of the Constitution, which is why they set up the Constitution with checks and balances, to try to ensure that the innate tendency of human beings with power to seek to abuse that power is checked. And that is what we have tried to accomplish within the intelligence community with the degree of oversight that we have, the number of people who are looking over other people's shoulders, the number of reports that have to be done, the technological controls that we have in place.

As General Alexander said earlier, if there are ways we can do that better, we are open to that. We would like to ensure that there is oversight that is sufficient to persuade the American people that we are doing the right thing on their behalf. But we do think it is important that in considering what to do, we do not throw out the baby of national security with the bath water of oversight.

Chairman LEAHY. And if there are better ways of doing things, if there is any silver lining in the Snowden matter, I understand from General Alexander's testimony that you are taking the steps to make sure that colossal mistake would not happen again.

Mr. LITT. We are going to do our best.

Chairman LEAHY. General. And then after you speak, General, I am going to turn the gavel over to Senator Whitehouse because he is a nicer person than I am. Go ahead.

General ALEXANDER. Chairman, first, two things. As you correctly stated, there was one unique case under 215 where the metadata helped. There were seven others where it contributed and four where it did not find anything of value, and we were able to tell the FBI that.

Now, that last part, "of value," I want to point that out. This summer there was a big issue on terrorism that we all went through. This program actually helped us understand was that focused on the United States or elsewhere? We used that program to determine none of those leads were coming into this country, and we were able to focus our efforts elsewhere, which really helped both the intelligence community and the FBI in that case.

The second part, you know, I have been in this job for a little over 8 years, and my experience from dealing with the people that we have, dealing with Congress, the courts, and the administration on this, is our folks take the Constitution to heart. We see this as two roles: defend the Nation and protect our civil liberties and privacy. Everybody at NSA, including myself, takes an oath to that Constitution, that we will support and defend the Constitution. And you know the rest of that.

And I would tell you that the oversight we have, especially by the courts, ensures that what happened that you brought up will not happen here. From my perspective, we have great oversight in this program, and at times I complained that the oversight was so robust that it was crippling. But now you can see that everything that we have done, all the things that have come out were either self-reported or brought out. They were not revealed by Snowden. We had already reported those incidents. I think you can see that we are acting well and faithfully to discharge those duties.

Just to correct one thing, to add to what Bob said, there have been no willful or intentional violations under the 215 or 702. As you do know, there were 12 under Executive Order 12333. In both cases, all the violations that we know about we have self-reported. Some of those we knew would be significant. We brought them up to the White House, to the DNI, to the Department of Justice, to the courts, and to Congress. We made a mistake. These were not intentional. They were significant. And you have read the court things and you have read some of those. But from my perspective, I think what we should take great pride in the fact is this agency in every case reports on itself, tells you what it did wrong, and does everything we can to correct it.

Chairman LEAHY. Thank you.

Senator Whitehouse, would you take it from here? And I apologize to the next panel that I am going to—I may not be able to get back. I am going to try to—do you want to take this seat here?

Senator WHITEHOUSE [presiding]. Sure. I will do that when the panels shift, but let me just take a little bit of time myself right now with this panel before they are excused.

First of all, we are at a time where we have entered a new technological era, the era of big data, and I will loosely and unprofessionally define "big data" as the ability to aggregate enormous

amounts of information that do not get looked at and then figure out ways, once they are aggregated, to search for things in that big heap of data. And that raises questions about whether the aggregation is a search or whether it is not a search until a human being actually asks a question and actually the information gets to another human mind. And some of these are pretty difficult questions that we have to work our way through, and so I think the attention that the Committee is paying to this is a very sensible attention.

But our national intelligence establishment is not the only group that is playing in this big data area. We all know that Google and other private sector providers are very, very actively in big data, data mining, and doing things like that.

What can you tell me about what other governments are doing without specifying names and releasing any national security information? I take it that other foreign sovereigns are doing very aggressive things in this space to try to pull as much information as they can as well out of the cloud and out of the capacities of big data. Who would like to take that? General.

General ALEXANDER. Senator, I have some experience in that. In my opinion, none of them have the oversight by all three branches like we do, either their parliaments, congress, their courts, and their administration.

Senator WHITEHOUSE. Understood, but my point is they are all out there doing it.

General ALEXANDER. They do.

Senator WHITEHOUSE. And that if we were to—well, of the ones who have capability, a lot—the most powerful ones all do.

General ALEXANDER. That is right.

Senator WHITEHOUSE. And if we were to pass a law that prevented our intelligence and defense establishment from operating in that big data atmosphere, we would be essentially unilaterally disarming in an arena in which other governments are very active. Is that true?

General ALEXANDER. That is true. In fact, I think some have likened it to, because we have a powerful intel community or powerful Navy, we would tell our submarines to surface in those areas where people do not—their subs are not as good.

Senator WHITEHOUSE. And the actual collection of data in the sense that it is brought to the awareness of a human mind somewhere has to be overseen very scrupulously. And as I understand it, this operation is overseen by multiple inspectors general, multiple general counsels, multiple Federal executive agencies. NSA connects in ways that provide varying levels of visibility, but in most cases complete visibility to our Department of Defense; to the FBI, to the Department of Justice, Jim; to the ODNI, the Office of the Director of National Intelligence; to the President; to the National Security Council. So there is considerable attention that is being dedicated to this. We have a court that is dedicated to this that reports to the Supreme Court. We have this legislative Committee, the Senate Intelligence Committee, and the House Committees.

So it is hard for me to think of whatever we might do to add to the level of oversight, I think we may make it more efficient and effective. But I do not want anybody to leave this hearing thinking

that we kind of just leave this question to the NSA. We have built a system in which every branch of Government and within those branches of Government in many cases multiple different agencies, and in some cases within those agencies multiple different and in some cases independent sectors, all compete to have a look and to make sure that the right things are being done.

So I will let you all go. I appreciate what you are doing. I understand that we need to get this right. But I think it would be a mistake to unilaterally walk away from the realm of big data to protect our national security when we are perfectly comfortable with private companies doing that to make money and to find out more about us so they can market to us better, and when foreign governments are energetically penetrating this space in order to accomplish similar results. And I think nobody should leave this hearing not aware that the layers of oversight and checking and double-checking and triple-checking that are done here are very, very rigorous and considerable. I know you have to live with that all the time. If you would like to make any closing comment to that, I will let you do that. But otherwise I will let you go.

Mr. COLE. I think you have summarized it very well, Senator.

Senator WHITEHOUSE. All right. Well, we will leave it with that, and I appreciate very much you all being here. Thank you for your service to our country.

General ALEXANDER. Thank you, Senator.

Senator WHITEHOUSE. And we will take a minute and call up the next panel.

It was hard to get Bob Litt out of here, Professor. He loves it so much being in front of us.

All right. Let me ask the panel to stand to be sworn. Do you affirm that the testimony you are about to give to this Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. BLACK. I do.

Mr. SANCHEZ. I do.

Professor CORDERO. I do.

Senator WHITEHOUSE. Please be seated. I am delighted to welcome our second panel on this important issue, and I will go right across the table and ask each of you to make your opening statements, and we will do collective questions at the end. We may be rejoined by a number of my colleagues. This is the time that the administration briefing on Iran is taking place in the classified area, and so obviously that is of interest.

We will start with Ed Black, who has been the president and CEO of the Computer and Communications Industry Association since 1995. He previously served as Chairman of the State Department's Advisory Committee on International Communications and Information Policy, and he worked as chief of staff and legislative director for two Members of Congress.

Mr. Black, welcome. Please proceed.

STATEMENT OF EDWARD J. BLACK, PRESIDENT AND CHIEF EXECUTIVE OFFICER, COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION, WASHINGTON, DC

Mr. BLACK. Thank you very much for the opportunity to be here. Thank you, Senator Whitehouse.

This is an important subject. I want to start out by just pointing out that 16 years ago the White House charted a course for a vibrant Internet economy in the perceptive Magaziner Report, the first U.S. Government policy statement addressing the needs of Internet commerce. That policy statement correctly identified user trust as the foundation of Internet commerce. It noted: "If Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the Internet on a routine basis for commerce."

That may sound rudimentary today, but we should not take for granted decades of progress in creating security and fostering user trust, and we should not discount how easily that foundation can be damaged.

The broad NSA surveillance regime and the way it has been received internationally has harmed U.S. companies, U.S. competitiveness, and the Internet itself. The U.S. Government must be proactive in addressing these concerns. The status quo is no longer an option. If we do not act, we will put at risk our economic security and undercut our diplomatic ability to influence the future of the Internet. Therefore, Mr. Chairman, CCIA supports the USA FREEDOM Act, and we look forward to working with the Committee and staff on this important piece of legislation.

A healthy global Internet is a source of American competitive advantage. The U.S. ITC has documented a growing digital trade surplus. Our global competitiveness is not just good for commerce, it is an essential component of our long-term national security.

The Internet does not only benefit the U.S., however. The open Internet provides great global commercial benefits. The Internet economy in G–20 countries is expected to reach $4.2 trillion by 2016. Estimates show that 21 percent of economic growth in mature economies over the past 5 years is attributable to the Internet.

Traditional industries are the beneficiary of 75 percent of the economic value derived from the Internet. Thus, we should not underestimate the Internet's role in global economic development, which in turn has its own security benefits for the United States and the rest of the world.

The NSA's practices clearly impact the business of U.S. Internet companies. So much of online commerce today is fundamentally based on trust. If users are going to turn over very sensitive personal and confidential information to a company providing online email or other cloud services, they need to believe that the company will act as a responsible steward of their data. Although traditional debate on the utility of overbroad NSA surveillance has focused on hard-power arguments, one must not overlook the effect on soft power.

It is important to recognize the dramatic effect these revelations have had on our international diplomatic authority, particularly in regard to the future of Internet governance. Last year's WCIT conference showed us that there was deep international division over

whether to subordinate the open Internet to the political machinations of world governments, including repressive regimes. The U.S. needs to be a beacon for freedom and openness in this battle.

Given these risks, we propose: enhanced transparency and procedural reform; clearer protection for Americans; and baseline protections for international users.

With regard to transparency and procedural reform, we think all governments should share with citizens meaningful information about their surveillance laws, their legal interpretations, and the judicial procedures that govern the exercise of this powerful authority. Of course, the U.S. cannot demand this from others until it leads by example.

Furthermore, companies should be permitted to disclose publicly to their users the precise volume of requests from governments. Businesses should not only be permitted to release transparency reports but encouraged to do so. We categorically reject the notion that open government will cause undue damage to security. Transparency in criminal surveillance has been the norm for years and does not appear to have materially affected law enforcement.

In order to present a robust check on the Government, the FISC must also evolve to include a committed and well-resourced advocate to provide an alternative viewpoint, particularly in situations involving novel questions of law.

Second, focusing on protections for Americans, Federal laws addressing the circumstances in which the Government may collect Americans' data for national security purposes are badly in need of reform. Bulk collection of metadata is one area where that is most obvious, as it reveals a great deal of sensitive private information. Furthermore, important First Amendment rights of association are implicated by the Government assembling its own version of your social network for their own analysis. The USA FREEDOM Act addresses this problem by explicitly prohibiting this type of bulk collection both on the Internet and on telephone networks, and that is one of the reasons we are supporting it.

Third, and finally, protections for foreigners. A difficult subject to deal with, but despite the global interconnected nature of the Internet, U.S. national security policy continues to presume U.S. citizens deserve protection from unwanted surveillance, while others do not. If foreigners lack baseline privacy assurances, foreign competitors will supplant U.S. leadership in Internet innovation and digital commerce, thus undermining strategic economic and other security interests. This is especially true going forward, as foreign markets are increasingly important.

Thank you very much for the opportunity to testify. I look forward to your questions.

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

Senator WHITEHOUSE. Thank you very much, Mr. Black.

Our next witness is Julian Sanchez, who is currently a research fellow at the Cato Institute focusing on the intersection of technology, privacy, and civil liberties, with a focus on national security and surveillance issues. He previously served as the Washington editor for a technology news site and has written for a wide array of publications.

Mr. Sanchez, welcome.

STATEMENT OF JULIAN SANCHEZ, RESEARCH FELLOW, CATO INSTITUTE, WASHINGTON, DC

Mr. SANCHEZ. Thank you, Senator Whitehouse. It is a privilege to address this Committee.

I want to begin by suggesting that if we step back from the details of the disclosures of recent months, we find a disturbing pattern across multiple programs and authorities emerges. I will focus in particular on the telephony metadata program, the now defunct Internet metadata program under the pen/trap authority of the PATRIOT Act, and upstream collection under Section 702 of the FISA Amendments Act.

In each of these cases, what we see is that extraordinary but nevertheless limited authorities were secretly interpreted in ways that permitted far more extensive collection than certainly members of the general public and even, I think, many legislators believed at the time of passage had been authorized. This was done in part because the FISA Court, which was established on the premise that it would be authorizing and find probable cause in cases of specific and traditional targeted surveillance, instead found itself in the position of addressing broad programs of surveillance, often involving novel legal or technological issues that it is not clear that body was well established to consider.

In the metadata cases, these interpretations took the form of an unprecedented reading of relevance that held entire databases containing information about millions of admittedly innocent Americans to be relevant on the grounds that a fishing expedition through those records might ultimately turn up evidence that would not otherwise be detected in the absence of some specific grounds for suspicion that is probably true, but it is, of course, true of any fishing expedition and defeats, I think, the purpose of the relevance requirement if that argument is allowed to go through.

There is no real limiting principle in that argument for any type of records, and I was particularly disturbed to hear earlier Mr. Litt refuse to reassure us that the scope of the records obtainable under Section 215 does not exclude the contents of digital communications or cloud-stored documents.

It is also particularly troubling to see this applied in the case of the Internet metadata program because in that case the, in my view, shortsighted holding of *Smith v. Maryland* was applied as it referred to metadata generally, which is certainly not a term we find in the 1975 decision, when in this case it involved email metadata that is not ever stored as Business Records or usually even processed by the Internet backbone providers from whom it was presumably obtained. So there is kind of an additional constitutional question in that case, I think.

In the case of 702, we know the Supreme Court relied on a recent ruling in *Amnesty v. Clapper* on representations that only communications to or from specific overseas targets were being intercepted. We have now learned, of course, that also communications referring to overseas targets would be intercepted, and that in many cases for technical reasons a single email meeting selection criteria would lead to the entire inbox of the communicant

being obtained, including, again, potentially entirely domestic emails on what the Court believed could be a scale of many tens of thousands per year under that one collection program.

In each case, additionally we learned that for months or years, the actual technical details of how these programs operated were misrepresented to the FISA Court, which was, of course, therefore not able to effectively conduct oversight; and that in each case, again, elaborate safeguards and restrictions imposed by the FISA Court as a condition of authorizing those programs were effectively neglected because of the vast scale and complexity of those programs.

Additionally, in many cases we found that the claims of efficacy made at the time do not appear to have held up well over scrutiny from many dozens of foiled terror plots we have gotten down, in the case of the telephony metadata case, to really one instance involving funding and material support where it appears to have played some uniquely valuable role.

Given the limitations again imposed by the FISC, it is not clear why more traditional targeted orders could not have been used without incidentally sweeping in millions of innocent persons' records.

We are assured that the problems detected with these programs have not been willful or intentional. This is not especially comforting to me for several reasons.

The first is that if we look to history, we find that, in general, abuses of intelligence powers were committed by people who were well aware of the oversight mechanisms in place who often took elaborate steps to game those restrictions. In the cases of Bradley Manning and Edward Snowden, we know that it was—you know, steps were taken to evade oversight mechanisms in the case. We know that certainly happened many times in the past. And it is why abuses went undetected for so long.

Additionally, the scale of collection itself makes abuse more difficult to detect and less likely to be detected when it does occur. I think of the case of illegal wiretaps of the Southern Christian Leadership Conference's office. That at least was halted by an Attorney General who found the suspicious fact that the wiretap existed and there was a record of it. When you are doing collection on this scale, the mere existence of communications or records about an innocent party are not themselves that kind of essential indicator.

Finally, and most generally, I would just encourage the Committee to think architecturally. We should not authorize extraordinary architectures of surveillance on the basis that we now have great confidence in the probity of the persons controlling the levers. James Otis, whose condemnation of the Writs of Assistance was part of the inspiration for the Fourth Amendment, condemned those writs, saying that it is "from their mere existence that every householder in the province becomes less secure." And there is a sense in which, while they may serve some role in protecting us against foreign attacks, we are less secure when the Government maintains vast databases on Americans without particularized suspicion.

I thank you and I look forward to your questions.

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

Senator WHITEHOUSE. Thank you, Mr. Sanchez.

Our final witness is Professor Carrie Cordero—whose bio I have just mislaid, but I am sure you can get me another one very quickly. Thank you.

She is an adjunct professor of law and the director of National Security Studies at the Georgetown University Law School. She has previously held several national security-related positions with the Department of Justice and the Office of the Director of National Intelligence, and she has also testified before this Committee before.

So welcome back, Professor, and please proceed.

STATEMENT OF CARRIE F. CORDERO, DIRECTOR, NATIONAL SECURITY STUDIES, AND ADJUNCT PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER, WASHINGTON, DC

Professor CORDERO. Mr. Chairman, thank you very much. Thanks for the opportunity to return to the Committee.

Since the October hearing, the conversation, I would suggest, has shifted somewhat from where it first was. First, I would suggest that the conversation has evolved from objections to specific programs to a discussion of our understanding of and tolerance for foreign intelligence surveillance activities more broadly.

Second, the legislative proposals are coming closer to scaling back national security legal authorities in a way that might make the country back to pre-9/11 standards.

And, third, the path forward on authorized public disclosure in a way that is responsive to the concerns of the private sector remains a worthy goal, but still a significant challenge.

With respect to the telephony metadata collection under the Business Records provision of FISA, an argument increasingly is regarding the power of metadata, and basically this argument is that metadata is a very powerful tool and can reveal an awful lot about us, and there should be limits on the Government's collection and use of it.

I do not disagree with the general proposition, but the problem with the argument made in the context of the debate on 215 is that the worrisome assemblage of Americans' metadata bears no relation to the existing 215 program that Congress is currently considering. The 215 program does collect an enormous volume of Americans' telephone call detail records, but the collected information does not appear to include content of phone calls, names of subscribers, payment information, or location information. The vast majority of it is never viewed by human eyes and the records are handled under court order rules.

So of the arguments that Congress should outlaw bulk collection altogether, for better or for worse, everyday Americans use the Internet to communicate. We all, regular people, Government leaders, as well as those who are national security threats, use the Internet, computers, and smartphones to communicate. And so just as everyday citizens should not be expected to revert to using only the Postal Service and landlines, neither should the intelligence community or law enforcement have to resort to pen, paper, and

index cards to conduct national security collections or investigations. It is just as unrealistic to expect citizens to unplug as it is to expect or require the NSA or the FBI to use 20th century collection, analytic, or investigative techniques to protect the Nation from 21st century threats.

A few observations on S. 1599, the USA FREEDOM Act that has been submitted. Sections 101 and 201, which change the legal standards in FISA to obtain Business Records and implement pen register/trap and trace devices by requiring a connection to a foreign power, to an agent of a foreign power.

The sections also add a materiality requirement. The likely intended effect of these provisions is to eliminate the 215 bulk telephony metadata program. But the proposed changes would likely have far more reaching consequences for traditional, day-to-day investigations. The standards are currently aligned on the national security side with investigative authorities in the criminal context, which operate on a relevance standard. By raising the standard, these sections would render these investigative techniques nearly useless in the early stages of an investigation, which is precisely when they are most useful. These changes could return us to the days prior to September 11th, when it was harder to conduct a national security or international terrorism investigation than it was to conduct an everyday drug or fraud case.

Similarly, Section 501 would amend the collection of statutory authorities known as "national security letters" by requiring the requested records to also have a connection to an agent of a foreign power. This would have a similar effect in terms of severely limiting the FBI's ability to conduct timely and thorough national security investigations.

Another section, Section 301, would appear to prohibit the intelligence community from querying data acquired pursuant to Section 702 of FISA to search for U.S. person communications. Under the current minimization procedures approved by the Court, the NSA can query the communications already acquired under 702 for U.S. person communications. The proposed legislation would only allow the same query to take place if the U.S. person is a current target of a criminal wiretap or FISA coverage, which would require prior judicial approval based on probable cause. This proposal could arguably prohibit the intelligence community from querying already lawfully acquired data to search for the methods of communication of a valid target who happens to be also American. And in my written statement, I give an example of how I think this could potentially play out in practice.

A few words just on a particular proposal to enhance transparency that is in the bill. In my view, there is substantial value in Congress continuing to work with the executive branch and the private sector to rebuild confidence between them and for the Government to help the private sector restore confidence with consumers, customers, and investors.

But a particularly problematic proposal is Section 602 of the bill. It proposes that the Government disclose the number of persons subject to electronic surveillance. I believe that this is intended to include not only targets but persons whose communications are incidentally collected. If that is the intent, in my view this provision

would actually degrade privacy protections because a requirement to report on the numbers of persons collected would require that the intelligence community personnel look at, read, review, count, and keep records about and report on information that they otherwise would disregard in pursuit of their actual mission of discovering, analyzing, and reporting on foreign intelligence information.

So again, thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Professor Cordero appears as a submission for the record.]

Senator WHITEHOUSE. Thank you very much.

Let me start with a question for Mr. Black. There is legitimate concern that the knowledge of our national security activities casts a shadow on the ability of American companies to compete internationally. That was the basis of your testimony. Do you believe that foreign customers believe that, for instance, if they sign up for a service with Huawei that the Chinese Government is not looking into this data or the Russian Government, if they sign up in areas under its jurisdiction, or the French Government, for that matter, do you think that the U.S. Government is actually the only government that is trying to take advantage of big data?

Mr. BLACK. I hope our standard is not just to meet Huawei, but I do think the reality is that governments in general are inclined to want more and more information. Too much. That is why what we address in our testimony is, in fact, standards that all governments should be asked to undertake in terms of disclosure, in terms of limits.

The difficulty is that the United States is in a very difficult position in credibility when we are seen to have an extremely pervasive, effective, widespread, and some would say not effectively limited process. No, by no means do we want——

Senator WHITEHOUSE. Do you think that—hold on—the Chinese and the Russians actually are more effectively limited by the government performing——

Mr. BLACK. No, I am not suggesting that at all.

Senator WHITEHOUSE [continuing]. Surveillance activity than the United States is?

Mr. BLACK. No, I am not suggesting—I am not doing a comparison. First of all, I believe we do have some checks and balances that have some effectiveness. Do not get me wrong. You asked a question is the perception of the world——

Senator WHITEHOUSE. Indeed they are far better than any other country's checks and balances that are engaged in this kind of behavior, correct?

Mr. BLACK. I am not going to talk to all of the countries. I certainly hope we have better ones——

Senator WHITEHOUSE. Are you aware of any other country that has a better——

Mr. BLACK. I think there are many other countries that do not probably do as much collection as we do.

Senator WHITEHOUSE. I can name some. There are some very tiny little countries that probably barely run a phone system. But in terms of our major competitors, in terms of the major economic and political actors on the world stage, the ones——

Mr. BLACK. I think that——

Senator WHITEHOUSE [continuing]. That we are all thinking of——

Mr. BLACK. I guess the question——

Senator WHITEHOUSE [continuing]. None of whom have more robust protection——

Mr. BLACK. We are trying to say, what kind of future do we want, what kind of Internet do we want? Do we want an open Internet, an Internet which provides tremendous economic growth, tremendous empowerment, tremendous diplomatic and political opportunities around—for billions of people around the world? Do we want one where people can have association with other people without being spied on by their government or our Government or any other government? Is that a desirable outcome? If so, how do we take steps to move in that direction? Or do we accept the reality that all governments are going to do a maximum collection and go in the Big Brother direction as far as they can go and we are just in an arms race to do that? I do not think that is a future I look forward to.

It is difficult to want to restrain a government's desire for more information, especially I think our Government, where we have well-motivated people who care about national security, who really do believe in the motivation of what they are doing. But they are zealous and effective, and they are, in fact, in a position where they are able to gather a great deal of information.

Senator WHITEHOUSE. So you think our Government's security services are more dangerous to civil liberties than the government security services of China and Russia?

Mr. BLACK. Are they more interested? Absolutely. Much more interested in protecting civil liberties, absolutely.

Senator WHITEHOUSE. No, no. More——

Mr. BLACK. No doubt about it.

Senator WHITEHOUSE [continuing]. Intruding into civil liberties. You agree that our Government oversight of our national security establishment is far more interested in protecting civil liberties——

Mr. BLACK. I think it attempts——

Senator WHITEHOUSE [continuing]. Of those of competitors like China and Russia?

Mr. BLACK. Well, again, I cannot compare to other people. I do not know the details. I certainly have a presumption about how ineffective any controls they would have. I would hope——

Senator WHITEHOUSE. You put it——

Mr. BLACK. I would hope that with our Constitution we would have a really effective system. Do I think we have lived up to the best intent and good faith of our Constitution with the legal structures we have created that allow their surveillance? No, I do not think we have lived up to the principles, the core principles of the First Amendment and Fourth Amendment as faithfully as we could. Are we better than totalitarian regimes? Of course. That is not a question that I think is fair.

Senator WHITEHOUSE. You take a different view, I guess, than the courts that have overlooked this which have not found Fourth Amendment violations in any of this?

Mr. BLACK. I think some of those decisions have historical positions that are based—I mean, Business Records, for example——

Senator WHITEHOUSE. But there is no present decision——

Mr. BLACK. When the Business Records——

Senator WHITEHOUSE [continuing]. That supports your legal point of view?

Mr. BLACK. Excuse me?

Senator WHITEHOUSE. There is no present decision by any court that suggests that there has been—that this has operated in violation of the Fourth Amendment. It would take a new decision to make that conclusion that has not yet been rendered by any court. Is that not correct?

Mr. BLACK. I would suggest that various efforts to get those questions raised——

Senator WHITEHOUSE. Well, you are the one——

Mr. BLACK. In the courts have been denied.

Senator WHITEHOUSE. You are the one who said that this was being operated in violation of the Fourth Amendment. I am asking you if you can cite a case that supports that proposition.

Mr. BLACK. I believe the FISA Court made a ruling that certain practices had violated their——

Senator WHITEHOUSE. Orders.

Mr. BLACK. The orders. Well, I think the orders——

Senator WHITEHOUSE. But not the Fourth Amendment——

Mr. BLACK. Were based on the Constitution.

Senator WHITEHOUSE. Professor Cordero, for how long has incidental collection of communications with people who are not the subject of the warrant been a fact of life in law enforcement?

Professor CORDERO. Well, both on the criminal side and on the national security side, there always is going to be incidental collection. So the criminal Title III wiretaps handle it in one way. On the national security side, it is handled through minimization procedures for U.S. person communication. So it has always been a factor. The minimization procedures particularly on—well, any of the FISA minimization procedures are approved by the Court, including on the 702 collection.

Senator WHITEHOUSE. So for as long as there has been any authorized Government interception of communications, incidental collection has always been a part of that necessarily.

Professor CORDERO. That is right.

Senator WHITEHOUSE. I have gone over my time. Senator Blumenthal is here. Let me yield to the distinguished Senator from Connecticut.

Senator BLUMENTHAL. Thank you, Mr. Chairman, and thank you all for being here.

Let me focus on FISA Court reforms. Mr. Sanchez, I wonder if you could tell me your position on implementing some kind of adversarial process as I have advocated be done through a constitutional advocate and other reforms in the FISA Court that might be feasible.

Mr. SANCHEZ. I would step back from that for a moment and just say that in cases where you have something that is an authority that was clearly, I think, envisioned as something relatively targeted to acquisition of records with some nexus to terror or espio-

nage suspects, the appropriate move at that point, if it is believed that some kind of bulk collection is necessary, some kind of more programmatic use of that authority is necessary, is to return to Congress and not to, in fact, leave that decision in the hands of the FISA Court. One suggested approaching this with a rule of——

Senator BLUMENTHAL. In other words, the FISA Court should not be making law.

Mr. SANCHEZ. When a request is so broad as to effectively, I think, exceed what anyone conceived as the authority, it would be better to have congressional authorization. In closer cases, I think what we can see from some of the opinions that have now been released first is that it would, I think, benefit the Court's proceeding when novel questions of law are present to have some kind of adversarial—or I guess to raise opposing arguments, but also I think in particular to have technical expertise. I alluded briefly earlier to a kind of tricky constitutional wrinkle with respect to the use of pen register authority to intercept metadata where you do not just have, as with a phone call, the number and the content, but layers of metadata and content with——

Senator BLUMENTHAL. Do you think, though, that we ought to have a constitutional advocate?

Mr. SANCHEZ. I think that would be extraordinarily helpful, but also I think a technical advisory capacity of some kind would be useful, because sometimes I think the most difficult questions turn not just on the abstruse details of law or technology, but about the ways they intersect in surprising ways where often there is not precedent directly on point.

Senator BLUMENTHAL. Thank you.

Professor Cordero, I gather you feel there is no need for a constitutional advocate or some kind of adversarial process, but you would be willing to support some kind of amicus curiae process?

Professor CORDERO. Thank you, Senator. Well, certainly since the October hearing, this conversation has evolved, and so, you know, there are different proposals. In my view, as we discussed at the prior hearing, based on the current procedures that take place within—between the Department of Justice and the intelligence community and the Court, in my view there does not—I think that the current process is sufficient that facts from the other side are presented to the Court, the Court has independent legal advisers. These are independent Article III judges who make judgments on their own. So, in my view, there actually does not need to be an adversarial process, and I think the current process is sufficient.

However, between the competing legislative proposals, between establishing an Office of Special Advocate versus the proposal to enable the Court to call upon an amicus if the Court believes it needs it, I believe that the second option would be the better of the two options.

Senator BLUMENTHAL. And that is because you are loath to create a "bureaucracy"? Or what is the reason?

Professor CORDERO. Sure. Several reasons. So one is yes, I think that the FISA process already is very heavily bureaucratic, it is heavily layered. There are multiple offices and legal offices and different layers of management that are involved in reviewing FISA matters. So I think it already is very bureaucracy heavy, and I

think that the way that the Office of Special Advocate is described in this legislative proposal, it would simply add to that process.

I also am concerned that over time there has been a relationship of trust and a very constructive relationship between the executive branch and the FISA Court, and I actually worry that an Office of Special Advocate would in some way harm that sort of established relationship of trust by being in the middle.

With respect to the proposals to add an amicus, you know, again, if the Court——

Senator BLUMENTHAL. Isn't the problem that this relationship of trust has actually undermined trust in the American public and really threatens to completely eviscerate confidence in a system that operates in secret, makes secret law, and in the end the relationship of trust may undermine the whole system?

Professor CORDERO. Well, although, Senator, I would say that actually a concern about the Office of Special Advocate is that it will have to operate in secret, too. And so just as the creation of the FISA Court in 1978 and the creation of the office that worked in the Justice Department that was an independent, non-political office at the time was created in order to establish trust and be sort of this independent participant in the process, now people do not—you know, they are questioning the FISA Court. And so I do not know that over time—although in the sort of immediate future I can see how the Office of Special Advocate might be appealing, I do not actually think in the long term, because it will operate in secret, because it will sort of become part of this whole process, that in the long term it really will restore that——

Senator BLUMENTHAL. Well, it would operate in secret, but it could be combined with other reforms that would provide for some greater measure of transparency to the FISA Court's opinions when it makes new law that affects Americans around the world or at least in our country. Perhaps there ought to be more of these rulings and opinions that are made public.

But at any rate, my time has expired. I thank you, Mr. Chairman, and thank each of the witnesses for being here today.

Senator WHITEHOUSE. Thank you, Senator Blumenthal. I am also grateful to the witnesses for the trouble that they have taken to come in and help inform this Committee as we go about our decisions, and I welcome them.

We will hold the record of this hearing open for 1 additional week for any further materials anybody wishes to submit, and with that, we will adjourn the hearing.

[Whereupon, at 4:07 p.m., the Committee was adjourned.]

[Additional material submitted for the record follows.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

UPDATED Witness List

Hearing before the
Senate Committee on the Judiciary

On

"Continued Oversight of U.S. Government Surveillance Authorities"

Wednesday, December 11, 2013
Dirksen Senate Office Building, Room 226
2:00 p.m.

Panel I

The Honorable Keith B. Alexander
Director
National Security Agency
Fort Meade, MD

The Honorable James Cole
Deputy Attorney General
Department of Justice
Washington, DC

The Honorable Robert S. Litt
General Counsel
Office of the Director of National Intelligence
Washington, DC

Panel II

Edward Black
President & CEO
Computer & Communications Industry Association
Washington, DC

Julian Sanchez
Research Fellow
Cato Institute
Washington, DC

Carrie F. Cordero
Adjunct Professor of Law, Georgetown Law
Director, National Security Studies at Georgetown University Law Center
Washington, DC



JAMES M. COLE
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

GENERAL KEITH B. ALEXANDER
DIRECTOR
NATIONAL SECURITY AGENCY
CHIEF
CENTRAL SECURITY SERVICE

ROBERT S. LITT
GENERAL COUNSEL
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"CONTINUED OVERSIGHT OF U.S. GOVERNMENT SURVEILLANCE ACTIVITIES"

PRESENTED
DECEMBER 11, 2013

Joint Statement for the Record
of

James M. Cole
Deputy Attorney General
Department of Justice

General Keith B. Alexander
Director
National Security Agency
Chief
Central Security Service

Robert S. Litt
General Counsel
Office of the Director of National Intelligence

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Continued Oversight of United States Government Surveillance Activities"

Presented
December 11, 2013

Thank you for inviting us to continue our discussions with this Committee on our efforts to enhance public confidence in the important intelligence collection programs that have been the subject of unauthorized disclosures since earlier this year: the collection of bulk telephony metadata under the business records provision found in Section 215 of the USA PATRIOT Act, and the targeting of non-U.S. persons overseas under Section 702 of FISA. As we have

emphasized in previous appearances before this and other Committees, we remain committed, as we review any modifications to these authorities, both to protecting privacy and civil liberties in the conduct of our intelligence activities, in a manner consistent with the Constitution, the law and our values, and to ensuring that we continue to have the authorities we need to collect important foreign intelligence to protect the country from terrorism and other threats to national security. We also remain committed to working closely with this Committee as any modifications to these activities are considered.

A key step in promoting greater public confidence in these intelligence activities is to provide greater transparency so that the American people, as well as ordinary citizens around the world, understand what the activities are, how they function, and how they are overseen. As you know, many of the reports appearing in the media concerning the scope of the Government's intelligence collection efforts have been inaccurate, including with respect to the collection carried out under Sections 215 and 702. In response, the Administration has released substantial information since June to increase transparency and public understanding, while also working to ensure that these releases are consistent with national security. We welcome the opportunity to discuss ways to make more information about intelligence activities conducted under FISA available to the public in a meaningful and responsible way. At the same time, we are mindful of the need not to publicly disclose information that our adversaries could exploit to evade surveillance and harm our national security. There is no doubt that the recent unauthorized disclosures about our surveillance capabilities risk causing substantial damage to our national security, and it is essential that we not take steps that will increase that damage.

In keeping with this balance, in June the President directed the Intelligence Community to make as much information about the Section 215 and Section 702 programs available to the public as possible, consistent with the need to protect national security and sensitive sources and methods. Since then, the Director of National Intelligence has declassified and publicly released substantial information in order to facilitate informed public debate about these programs. Among other things, the Government has declassified and disclosed the primary and secondary orders from the FISA Court that describe in detail how the bulk telephony metadata collection program operates and the important restrictions on how the data collected under the program are accessed, retained, and disseminated. The Government has also released two recent FISA Court opinions, as well as an Administration white paper, that articulate in detail the legal authority and rationale for this program. We have also declassified and released to the public several other FISA Court opinions and orders concerning the two programs, including detailed discussions of compliance issues that have arisen during the programs' history and the Government's responses to these incidents. We have declassified and released extensive materials that were provided to the Congress in conjunction with its oversight and reauthorization of these authorities. Finally, just this week we have declassified and released additional materials, including FISA Court opinions relating to a separate program (no longer in operation) to collect certain internet metadata in bulk pursuant to court orders issued under the pen register/trap and trace provision of FISA (Section 402). Our efforts to promote greater transparency through declassification and public release of relevant documents are not yet complete. We will continue our efforts to promote greater transparency through declassification and public release of relevant documents, while carefully protecting information that we cannot responsibly release because of national

security concerns. These efforts are an important means of enhancing public confidence that the Intelligence Community is using its legal authorities appropriately, which has become increasingly important in the wake of confusion, concerns, and misunderstandings caused by the recent and continuing unauthorized disclosures of classified information.

As part of our ongoing efforts to increase transparency, the Director of National Intelligence has also committed to providing annual public reports that include nationwide statistical data on the Intelligence Community's use of certain FISA authorities. Specifically, for each of the following categories of FISA and related authorities, beginning in January 2014 and on an annual basis thereafter, the Intelligence Community will release to the public the total number of orders issued during the prior twelve-month period and the number of targets affected by these orders:

- FISA orders based on probable cause (Titles I and III and Sections 703 and 704 of FISA).
- Directives under Section 702 of FISA.
- FISA Business Records orders (Title V of FISA).
- FISA Pen Register/Trap and Trace orders (Title IV of FISA).
- National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. § 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709.

This information will enable the public to understand how often the Intelligence Community uses these authorities nationwide, how many persons or entities are targeted by these efforts, and how these figures change over time. The Director of National Intelligence has concluded that providing this information on a nationwide basis is an acceptable course in light of the goal of public transparency, without unduly risking national security.

We also understand the concerns that specific companies have expressed as to their ability to inform their customers of how often data is provided to the Government in response to

legal process. In light of those concerns, we have authorized companies to report within certain ranges the total number of federal, state, and local law enforcement and national security legal demands they receive on a nationwide basis, and the number of user accounts affected by such orders. This allows companies to illustrate that those demands affect only a tiny percentage of their users, even taking all of the demands together, and thus to refute inaccurate reports that companies cooperate with the Government in dragnet surveillance of all of their customers. At the same time, this approach avoids the disclosure of information to our adversaries regarding the extent or existence of FISA coverage of services or communications platforms provided by particular companies.

The scope of the voluntary disclosures by the Executive Branch concerning sensitive intelligence collection activities carried out under FISA is unprecedented. We hope that the information we have released, and will continue to release, will allow the public to understand better how our intelligence collection authorities are used. We also hope the public will appreciate the rigorous oversight conducted by all three branches of government over our intelligence activities, a whole of government approach that is unique and exacting in comparison to the many governments that conduct similar intercept programs with substantially less stringent oversight. The extensive oversight that we conduct helps to ensure that our activities protect national security, balance important privacy considerations, and operate lawfully.

In addition to the unprecedented steps we have taken to promote transparency, we are open to working with Congress on legislation designed to increase public confidence in these intelligence activities and enhance the protection of privacy and civil liberties. Regarding

Section 215, we would consider statutory restrictions on querying the data that are compatible with operational needs, including perhaps greater limits on contact chaining than what the current FISA Court orders permit. We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced statutory oversight and transparency measures, such as annual reporting on the number of identifiers used to query the data. To be clear, we believe the manner in which the bulk telephony metadata collection program has been carried out is lawful, and existing oversight mechanisms protect both privacy and security. However, there are some changes that we believe could be made that would enhance privacy and civil liberties as well as public confidence in the program, consistent with our national security needs.

On the issue of FISA Court reform, we believe that the *ex parte* nature of proceedings before the FISA Court is fundamentally sound and has worked well for decades in adjudicating the Government's applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA. However, we understand the concerns that have been raised about the lack of independent views in certain cases, such as cases involving bulk collection, that affect the privacy and civil liberties interests of the American people as a whole.

Therefore, we would be open to discussing legislation authorizing the FISA Court to appoint an *amicus*, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons. Establishing a mechanism whereby the FISA Court could solicit independent views of an *amicus* in cases that raise broader privacy and civil

liberties questions, but without compromising classified information, may further assist the Court in making informed and balanced decisions and may also serve to enhance public confidence in the FISA Court process.

While we remain open to working with Congress to effectuate meaningful reforms along the lines just described, we do not support legislation that would have the effect of ending the Section 215 program, which the Government continues to find valuable in protecting national security. And, while we support increased transparency, we do not support legislation that would require or permit public reporting of information concerning intelligence activities under FISA that could be used by our adversaries to evade surveillance, or which otherwise raises practical and operational concerns. The bill approved by the Senate Intelligence Committee includes a number of constructive provisions that we support and that we think will enhance protections for privacy and civil liberties without harming national security.

Finally, we want to address the Committee's interest in the legal standard for collection of records under Section 215. As the Administration explained in a white paper that it published in August, the telephony metadata program 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 terrorist or clandestine intelligence activities." 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 the 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 to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied, particularly in light of the strict limitations on the use of the data collected and the extensive oversight of the program.

As noted above, two decisions of the FISA Court that have recently been declassified by the Government and released publicly by the Court explain why the collection of telephony metadata in bulk is constitutional and is authorized under the statute. These opinions reflect the independent conclusions of two federal judges serving on the FISA Court that the Government's request for the production of call detail records under Section 215 meets the relevance standard and all other statutory requirements. Moreover, these opinions conclude that because the Government seeks only the production of telephony metadata, and not the content of communications, there are no Fourth Amendment impediments to the collection. Indeed, 15 separate judges of the FISA Court have held on 35 occasions that Section 215 authorizes the collection of telephony metadata in bulk in support of counterterrorism investigations. Last week, a district court in a criminal case in California also held that the collection of telephony metadata in bulk under Section 215 is consistent with the Fourth Amendment.

We appreciate that privacy concerns persist about the telephony metadata collection program, even considering the limited data the Government receives, the stringent constraints set by the FISA Court on how it is used, and the aforementioned legal rulings that have consistently upheld its legality. But we hope you will weigh those concerns against the increased risks to national security if this capability were terminated with no equivalent program that addresses

what the 9/11 Commission pointed out as a critical gap in the ability of the intelligence community to detect and "connect the dots" for foreign terror plots against our homeland. This program fills a significant gap in our ability to identify terrorist communications and, together with other authorities, can help us identify and disrupt terrorist plots, thus fulfilling the vision of the 9/11 Commission, which implored the Government to undertake mechanisms and collaboration which would prevent the recurrence of another 9/11.

We look forward to answering any questions you might have about these important intelligence collection programs and related issues. We understand that there are a variety of views in the Congress and among the American people about these activities, and we look forward to discussing these issues with this Committee as new legislation concerning these activities is considered. We hope that, with the assistance of this Committee, we can ensure that these programs are on the strongest possible footing, from the perspective of both national security and privacy, so that they will continue to enjoy Congressional support in the future. Thank you.

Computer & Communications Industry Association

1972-2012: 40 YEARS OF TECH ADVOCACY

Statement of

Edward J. Black

President & CEO of

The Computer & Communications Industry Association

Before the

Senate Judiciary Committee

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

1 Introduction

Chairman Leahy, Ranking Member Grassley, members of the Judiciary Committee, thank you for the opportunity to offer testimony today on the surveillance authorities of the National Security Agency and how those authorities are affecting the Internet and the global trade in services online. CCIA is a 40-year old international nonprofit association representing a broad cross section of computer, communications and Internet industry firms. Our members employ more than 600,000 workers and generate annual revenues in excess of $200 billion.

This testimony will outline the promise of and the challenges to the open Internet, as well as some changes in law that will help preserve the civil liberties of Americans and the vital commerce of the Internet services sector both in the U.S. and in markets around the world. I am proud to announce in that context that CCIA supports the USA FREEDOM Act offered by Chairman Leahy and Representative Sensenbrenner. There are a few areas where we have some suggestions to improve the bill and we look forward to working with the Chairman and his staff on those points. Finally, this testimony will offer some suggestions for addressing the disparity between U.S. citizens and foreigners in a global age on a global network.

It is important to step back from the current controversy to provide context. In 1997 the United States government issued what has been widely hailed as a prescient and insightful policy statement that laid the foundation of the U.S. government's approach to the Internet. A task force, led by Ira Magaziner, produced the first major review of Internet policy and global commerce in 1997. In the Framework for Global Electronic Commerce, the White House put forward five principles to guide the development of the new digital economy. These principles enshrined an extremely successful approach to Internet policy that has seen the Internet grow from a medium with approximately 100 million

users in 1997 to nearly 3 billion Internet users today. The policy statement also identified what was the most crucial variable determining whether the Internet lived up to its potential as both an economic and social medium: public trust.

> If Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the Internet on a routine basis for commerce.[1]

If the above quote seems rudimentary, it is. However, it is also easy to take for granted what has been achieved since 1997 in creating a more secure online environment for commerce and communication. It is even easier to discount how easily decades of progress in creating user trust in the fidelity of their online conversations and transactions can be eroded. Revelations about the NSA's surveillance programs have had global repercussions and threaten to undermine the very trust upon which the current success and future growth of the Internet depend.

The fallout has harmed individual U.S. companies, the competitiveness of the United States economy, and the evolution of the Internet itself. It is difficult to overemphasize how deeply felt have been the reverberations of these revelations in discussions of Internet governance, trade, and freedom around the world. Here in the United States we have been focused understandably on the rights and liberties of Americans, questions of rule of law, and public opinion across the country. While these are critical issues, it is important that the Committee also concern itself with the fact that the behavior of the NSA, combined with the global environment in which this summer's revelations were released, may well pose an existential threat to the Internet as we know it today, and, consequently, to many vital U.S. interests, including the U.S. economy. That is why a number

[1] President William J. Clinton and Vice President Albert Gore, Jr., A Framework for Global Electronic Commerce (1997), *available at* http://clinton4.nara.gov/WH/New/Commerce/read.html.

of large Internet companies earlier this week released a set of principles calling for an end to bulk collection, better oversight and transparency, and protection for free flow of information.[2] Of particular note, these principles were addressed to governments around the world, not just here at home, because this is a problem that will take all of us to fix.

2 Economic Security

The members of the committee are no doubt familiar with the great commercial benefits the open Internet provides. It allows small-and-medium-size businesses to access markets and customers well beyond their reach in the brick and mortar world, lowers costs along the entirety of global supply chains, increases efficiency in business from the Fortune 500 down to the smallest mom-and-pop shop, and is the catalyst for the online services marketplace, one of the greatest economic drivers in the country today.

As an example of the immense economic benefit of the Internet, the Boston Consulting Group conducted a study in 2012 analysing the economic promise of the Internet economy.[3] The study predicts that the Internet economy in the G-20 will reach $4.2 trillion by 2016. Another study, conducted by the McKinsey Global Institute, estimates that 21% of GDP growth over the past 5 years is attributable to the Internet and that 2.6 jobs are created for every job lost.[4] And, perhaps more telling, the same study estimates that 75% of the economic value of the Internet accrues to traditional sectors of the economy in the form of greater efficiency and expanded market access.

[2]Global Government Surveillance Reform, *available at* http://reformgovernmentsurveillance.com/.

[3]Boston Consulting Group, The $4.2 Trillion Opportunity: The Internet Economy in the G-20, March 2012, *available at* https://publicaffairs.linx.net/news/wp-content/uploads/2012/03/bcg_4trillion_opportunity.pdf.

[4]McKinsey Global Institute, Internet Matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011, *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

The U.S. government has even taken notice. A recent comprehensive report from the U.S. International Trade Commission (ITC) noted, "digital trade continues to grow both in the U.S. economy and globally" and that a "further increase in digital trade is probable, with the U.S. in the lead." In fact, the report also shows, U.S. digital exports have exceeded imports and that surplus has continually widened since 2007.[5] As traditional manufacturing and lower-skill service sector jobs migrate overseas, the Internet, and the innovative ecosystem that it has spawned, is becoming increasingly important to our global economic competitiveness. As a result, the economic security risks posed by NSA surveillance, and the international political reaction to it, should not be subjugated to traditional national security arguments, as our global competitiveness is essential to long-term American security. It is no accident that the official National Security Strategy of the United States includes increasing exports as a major component of our national defense strategy.[6]

The NSA's practices have clear impacts on the business of the U.S.-based Internet companies. So much of online commerce today is fundamentally based on trust. If users are going to turn over very sensitive information such as the contents of an inbox, to a company providing an online email or other cloud service, they need to have trust in the idea that the company will act as a responsible steward of that data. So much of the promise of the Internet is reliant on that trust, as the Magaziner report made clear 16 years ago.[7]

The images portrayed in the press of Internet companies happily working with the NSA to turn over vast troves of information about users, while almost entirely untrue, nevertheless harmed the trust of users. We have seen the effects both here in the U.S. and around the world in both public rhetoric and the bot-

[5] U.S. ITC, *Digital Trade in the U.S. and Global Economies, Part 1* (2013), at xix, *available at* http://www.usitc.gov/publications/332/pub4415.pdf.

[6] The White House, *National Security Strategy of the United States* (2010), at 32, *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[7] *Supra*, note 1.

tom line. Contracts, particularly at the enterprise and government levels, are being cancelled and there are calls to somehow limit the amount of information sent to companies within the U.S. The European Union is even seriously reconsidering the EU - U.S. Safe Harbor Agreement that permits U.S. companies to collect information about European citizens. All of these efforts have an obvious effect on commerce in a sector of the U.S. economy that has shown some of the best performance in the recent economically difficult times.

Revelations about NSA surveillance of foreign users of American service providers, however, have made that natural commerce much less fruitful. Even worse have been the discussions since the first revelations. The White House almost immediately began emphasizing the legal protections afforded to American citizens under the current system. Others in Congress and the press have continued to emphasize this line of argument. It is important to emphasize how harmful this approach is to companies trying to do business around the world. Congress cannot expect American companies to successfully export information services if the protections their customers receive are weaker than the protections provided by the foreign competition. Last week Cisco announced their latest quarterly earnings are lower than expected because of a lack of trust of an American company abroad.[8] American cloud companies also report that both governmental and enterprise purchasing of U.S. cloud services in Europe have declined.

The NSA's efforts to undermine international encryption standards have also made us economically weaker. Those same standards the NSA subverts are used by people around the world to bank and shop safely online. Weaker encryption can be used by hackers to break passwords, conduct espionage, steal identities, and create mayhem. By decreasing the effectiveness of cryptography,

[8]Richard Waters, *Cisco cites emerging markets backlash on NSA leaks for sales slump*, FINANCIAL TIMES, Nov. 13, 2013.

the NSA is singlehandedly creating cybersecurity threats at a time when our Congress has been debating how to shore up our cyber defenses. Furthermore, this is at odds with the NSA's other stated mission: protecting the security of American networks. As Matthew Green, a noted encryption expert at John Hopkins University noted, The risk is that when you build a back door into systems, youre not the only one to exploit it.... Those back doors could work against U.S. communications, too.[9]

With these affects in mind, it would be dangerously myopic to separate the economic effects of widespread Internet surveillance from its security impacts.

3 Soft Power

The Internet's value obviously cannot be summed up in just dollars and cents. It is impossible to place a monetary value on the ability for people around the world to connect with each other, exchange ideas, debate politics, and experience foreign cultures. This is the Internet's greatest value and it may do more for national security than all the surveillance the government could muster. It is sometimes said that no two countries that both have a McDonald's have ever gone to war.[10] Although this analogy might overstate the causal mechanism behind peace, it is certain that unfettered Internet access, and the international commercial and economic interdependence that flows from it, makes international military conflict more costly and therefore less likely.

U.S. national security increasingly depends as much on this "soft power" in addition to traditional hard power. It is important to recognize the dramatic effect these revelations have had on our international diplomatic sway,

[9]Jeff Larson, Nicole Perlroth, and Scott Shane, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, PROPUBLICA, Sep 5, 2013, *available at* http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[10]Thomas Friedman, THE LEXUS AND THE OLIVE TREE, (Farrar, Strauss, and Giroux 1999).

particularly in regards to the future of Internet governance.

Even before the revelations in the *Guardian*, *Washington Post*, and other papers this summer, the open Internet was in trouble. Most people associate the World Conference on International Telecommunications (WCIT) treaty conference of last year with the first attempts to wrest control of the Internet away from the bottom-up multi-stakeholder organizations that have kept it running for years, but the efforts go back even further. Numerous governments – both well-meaning and repressive – have long believed that all Internet problems could be solved, if only they were in charge.

These efforts have escalated since this summer's revelations. The U.S. government position of supporting the multi-stakeholder model of Internet governance has been compromised. We have heard increased calls for the ITU or the United Nations in general to seize Internet governance functions from organizations that are perceived to be too closely associated with the U.S. government, such as the Internet Corporation for Assigned Names and Numbers (ICANN). This is unfortunate because ICANN is one of the best examples of an independent multi-stakeholder organization. Furthermore, the Internet governance regime that ICANN has cultivated has subjugated political concerns to economic and technical decisions, which, in turn, has allowed the Internet to grow from an obscure medium largely known only to academics 20 years ago, to a tool utilized by nearly 3 billion people today.[11] ICANN and the other multi-stakeholder governance groups have also seen it necessary to move themselves further away from U.S. government control.[12]

Finally, we have been faced with a series of proposals for modifications of the engineering structure of the Internet, such as requirements that companies

[11] 2.749 billion individuals are using the Internet, according to the ITU's 2013 ICT data, *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.

[12] *See Montevideo Statement on the Future of Internet Cooperation*, ICANN, *et al.*, (2013), *available at* http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm.

host all citizens' data physically in a particular country rather than where it is most efficient or cost effective. These demands are simply digital protectionism wrapped up in the cloak of privacy protection, but they are enabled by the perception U.S. government's actions. We have unfortunately seen these demands from places as diverse as the EU, Brazil, and Indonesia.

Losing this international diplomatic battle and turning over control of the Internet to politicians and bureaucrats from around the world would have disastrous consequences for the future growth and vitality of the Internet. Given that nearly half of the world voted against the U.S.'s position on the future of Internet governance at the WCIT last December[13] before the NSA revelations were made public – ceding more rhetorical ammunition to our political enemies is detrimental to the U.S.'s diplomatic ability to protect the Internet.

The timing for this situation could not be worse. The next year will see a large number of events at which Internet governance will be a topic of discussion. Some of these, such as the ITU Plenipotentiary Conference, the World Summit on the Information Society ten year review, and the World Telecommunications Development Conference, are occurring on a set schedule but will be considerably more focused on these questions than they may otherwise have been. Others like the Internet governance meeting taking place in Brazil next year, and the new focus on governance emerging at both the UN's Commission on Science and Technology for Development and in the General Assembly, are directly a result of the NSA's actions, particularly with reference to non-U.S. citizens. We already know that there will be many countries at these meetings seeking to usurp the governance of the Internet and give it to organizations like the International Telecommunications Union. This damage to the U.S.'s reputation on governance and the potential for adverse results in international

[13]WCIT 2012, *Signatories of the Final Acts* (December 2012), *available at* http://www.itu.int/osg/wcit-12/highlights/signatories.html.

fora will take hard work and a lot of time to overcome. It is a damage that will persist unless deep, fundamental change is undertaken.

Furthermore, it is important to recognize that there is no "status quo" option in this conversation. The world is already reacting to make the NSA's programs less effective. If the Unites States comes across as stubborn or unwilling to engage on this topic, particularly where it comes to the data of foreigners, not only will the practical value of this surveillance be lessened, we will have contributed directly to the further fracturing of the global Internet.

To their credit, many within the U.S. government have seen this threat and responded, particularly within the State Department, which has made Internet Freedom a major policy initiative. Former Secretary Clinton and her staff should be applauded for their work evangelizing the open Internet. Unfortunately they have been unintentionally undermined by the actions of others in the national security establishment. Through a posture that seems to treat Americans only as sources of data, albeit ones with laws protecting them, and foreign nationals as merely sources of data alone, the NSA programs have greatly harmed the credibility of American calls for Internet freedom, multi-stakeholder governance, and the free flow of information in large portions of the world.

4 Transparency

Transparency in the use of surveillance authorities is fundamentally important. Without knowledge of what the government is doing, citizens have no means of judging whether and how to change the law. Companies who receive government demands are unable to be truthful with their users about the extent of surveillance that is happening. Finally, laws interpreted in secret courts and left generally unchallenged cannot form the basis for a healthy democracy. Transparency has therefore been a focus for the companies in the Internet services

marketplace since the first revelations and is reflected in the principles released earlier this week.

Transparency, therefore, must be a multi-pronged effort. It should involve as many avenues for getting information out to people as is feasible. The executive branch, the FISA courts, and the companies themselves all have a duty, and must be allowed the ability, to release information about surveillance programs.

The companies in particular have a great need to share this kind of information. A breakdown of what companies receive surveillance orders, and how many, will help develop the national debate surrounding surveillance in our country. In addition, companies have a unique need to inform their users publicly about how many requests they actually get from the government, particularly after the allegations made this summer. In addition, those numbers should be as precise as is feasible, because the tendency today is to be skeptical of companies that look like they are hiding something. Precision in these numbers will help combat these concerns.

Not all companies are developing transparency reports, but all of them should be encouraged to. Any company, whether U.S. based or foreign, that receives orders from any government to turn over or take down information should be releasing aggregate numbers of such demands. It will only be once we can learn the full impact of surveillance on our online services that we can make informed decisions.

Government also has an obligation to share with its citizens the laws that affect them on a day-to-day basis. The interpretations of the law, the procedures used by the surveillance authorities, and the number of times those authorities have been invoked are all vital pieces of information. This is not only true of the U.S. government, of course. Governments around the world should be encouraged to reveal this information, and if the U.S. takes this first step it will

be in a much greater position to demand the same of other countries.

The committee will no doubt hear that transparency of the sort here suggested will cause undue damage to the security of the nation. These transparency proposals are, however, no different than those permitted for years under criminal statutes. Transparency reporting in the criminal context is even enshrined in the Wiretap Act. There have been little to no complaints from law enforcement indicating organized crime has learned to evade surveillance because of such transparency. Indeed, if anything we are seeing increased demands for data under criminal statutes year over year. It would be a mistake to let vague warnings about terrorism deter the full development of transparency in this area, particularly when that obfuscation erodes our economic security.

The Surveillance Transparency Act of 2013, recently introduced by Senator Franken and the topic of a hearing last week, would go far to create the sort of transparency that will inform the public and help the companies set the record straight. That is why CCIA has also publicly supported Senator Franken's bill and why we are glad to see that Chairman Leahy has included that language in his bill.

5 Protection for Americans

Federal laws addressing under what circumstances the government may collect Americans' data for national security investigations are badly in need of reform. Many of them were understandably written in a culture of fear and since bolstered by the ever-present invocation of terrorism. What has been forgotten is the fact that one of the greatest contributors to national security is a strong

economy.[14] Today, Americans fear government intrusion more than terrorism.[15] The time has come to adjust our priorities.

One area of national security surveillance programs needing modification is the bulk collection of metadata. Despite statements by some that imply collection of metadata is not intrusive of privacy, there is a great deal that can be learned about a person if you can see a list of who they call or with whom they email. Medical conditions, religious affiliation, sexual identity, and more are all reasonably easily deduced from this sort of metadata. The government emphasizes, when discussing its metadata program, that there are many controls in place to protect the data once it is collected and housed by the NSA, but that provides little comfort. Even if the current administration's intentions are completely noble and without reproach, once the data is collected, it can be used in the future. Information, it is said, wants to be free. A corollary is perhaps that databases want to be used.

As we now know, the NSA seeks to use this sort of metadata to build a model of the social networks of Americans.[16] To store details on who we speak to and who we associate with runs into direct conflict with not just the Fourth Amendment but also the First. The Supreme Court recognized this fact as far back as 1958, when they decided NAACP v. Alabama. Justice Harlan, in denying the State of Alabama the right to peer into the NAACP's membership rolls, recognized the "vital relationship between freedom to associate and privacy in one's associations."[17] This is just one of the reasons why the principles released this week took aim so directly at bulk collection, calling on governments

[14] *See, e.g.*, Alice M. Rivlin, *National Security Depends on a Strong American Economy*, Brookings Institute (2010), *available at* http://www.brookings.edu/blogs/up-front/posts/2010/12/30-security-economy-rivlin.

[15] Pew Research Center for the People & the Press, *Few See Adequate Limits on NSA Surveillance Program*, Pew Research Center (2013), *available at* http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

[16] James Risen and Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, Sep. 28, 2013.

[17] NAACP v. Alabama, 357 U.S. 449 (1958).

to "limit surveillance to specific known users for lawful purposes, and should not undertake bulk data collection of Internet communications."[18]

The USA FREEDOM Act would directly address this issue. It is good to see that it would address collection not just under Section 215 of the USA PATRIOT Act but also under a range of other authorizations including pen register/trap and trace provisions and National Security Letters. We know from official releases by the Director of National Intelligence that bulk collection of Internet metadata had been ongoing up through 2011 under the FISA pen register/trap and trace provisions. While we don't know precisely whether bulk collection of Internet metadata continues under other authorities at the moment, it is also encouraging that the bill seeks to prohibit all forms of bulk collection, for Internet and phone calling records.

Our laws protecting Americans must also be modified with regard to the operations of the Foreign Intelligence Surveillance Court. Right now the court issues its orders *ex parte*, with only the government in the room. While this works for criminal warrants, defendants in a criminal trial have the ability to challenge any improper warrants at trial. There is usually no such opportunity under FISA. That is why an institutional opponent should be created to intercede at the FISC, particularly in cases where the Court is grappling with novel questions of law and would be well served by hearing multiple sides of an argument.

It is important that such an advocate have the knowledge and the resources to properly represent the alternative viewpoints necessary to provide counsel to the FISC. In particular, we hope that the office will have access to technological expertise, as well as legal, as the NSA's programs are technologically complex and many in the FISC system have admitted that there is not enough knowledge

[18]Global Government Surveillance Reform, *available at* http://reformgovernmentsurveillance.com/.

to fully comprehend them. Senator Blumenthal's FISA Court Reform Act of 2013 is an excellent starting point and we are encouraged to see it included in Chairman Leahy's bill.

6 Foreigners Abroad

Despite the fact that the modern Internet is a global, interconnected medium, U.S. national security policy continues to operate on the presumption that U.S. citizens online deserve protection from unwarranted surveillance while others do not. While the U.S. began this great experiment, today's Internet is an international platform for innovation and communications. The network hosts commerce, politics, and love letters of billions from all corners of the globe – a fact reinforced as more of the developing world come online.

The short-sighted position that only a fraction of those users deserve privacy protections poses very real dangers for the future of the Internet. If foreign users are not provided any baseline assurances about the privacy of their personal information, communications and associations, then America's role as the world leader in Internet innovation and digital commerce is threatened. This is especially true going forward, as the fastest growing Internet markets are foreign and many major U.S. Internet companies are already attracting more users and reaping more revenue from abroad than they do at home.

Solving these problems will need the development of new legal paradigms. Old rules focused only on citizenship or location are anachronistic when it comes to the Internet. We do not yet have all the answers, but we must cease distinguishing Internet users in such a way if we wish our American companies to succeed globally. Furthermore, given that the Internet is global platform, Americans should have baseline assurances about their privacy when using non-US Internet platforms and services as well. The principles released this week

by major Internet companies focuses on this issue and calls for a framework for handling requests across jurisdictional boundaries, such as strengthened Mutual Legal Assistance Treaties (MLATs). If we don't change our rhetoric and seek new solutions to these problems, we will face a Internet surveillance arms race to the bottom that will almost certainly diminish the future commercial and social promise of the Internet as a global communications medium.

7 Conclusion

The Internet today is at a crossroads. The tool for commerce, expression, and communications so many of us have been building for a few decades now faces threats of balkanization, censorship, and being co-opted for the purposes of mass surveillance. This is not a sacrifice that should be made lightly. The companies that CCIA represents are in many ways the stewards of their users. There is a great responsibility to protect the trust given to them, and to work unceasingly toward a free and open Internet that will benefit everyone. The discussion that we are having today is one example of that larger goal.

This committee and Congress in general has the opportunity to have an incredible effect on the future of the Internet. It seems clear that for a long time our government has made choices impacting the Internet with only security fears in mind. This committee, right now, finally has the opportunity to right that wrong. I truly hope it does so. I thank you for the opportunity to testify on this crucial issue and look forward to answering your questions.

Statement of

Julian Sanchez

Research Fellow, Cato Institute

Before the

Senate Committee on the Judiciary

Hearing on "Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Thank you Chairman Leahy, Ranking Member Grassley; it is a privilege to be invited to address this committee.

With the recent release of several Foreign Intelligence Surveillance Court opinions, concerning a now-defunct program to acquire Internet metadata in bulk under FISA's pen register/trap-and-trace authority, a pattern has begun to emerge—across multiple domains of intelligence activity.

First, an authority generally understood at the time of passage to be expansive but nevertheless limited and particularized—certainly by the general public, and apparently by many members of Congress as well—is secretly interpreted to permit bulk acquisition of information about vast numbers of Americans' communications. Once published, the legal rationale for this expansive reading is criticized as strained even by scholars generally sympathetic to the past decade's expansion of government surveillance powers. As Professor Orin Kerr

noted in *The New Republic*, the FISC's opinion in this case ignored "important statutory clues suggesting that the pen register authority does not extend to bulk programmatic uses."

Here as with the previously disclosed telephony metadata program, the Court rationalized this bulk collection by employing a strained and, for practical purposes, unlimited concept of "relevance to an authorized investigation," according to which a pool of thousands or millions of records pertaining to Americans' innocuous communications could be considered "relevant" on the grounds that subsequent analysis could detect the tiny fraction actually related to some foreign terror group. This is, however, the very definition of a fishing expedition: Indiscriminate collection untethered to any specific grounds for suspicion at the time of acquisition, on the premise that some evidence of wrongdoing is bound to turn up somewhere.

Perversely, this rationale depends on bulk collection *not* being more narrowly tailored. If, after all, the government sought to acquire in bulk all metadata pertaining to communications for an arbitrarily chosen city over some more limited time period, it could not plausibly claim that the data pool was statistically all but certain to contain records of *actually* relevant communications. On the government's theory, rather, the totality of the information obtained is relevant *because* acquisition is sweeping and indiscriminate—a train of logic that, once accepted, leaves scant incentive to develop more narrowly tailored collection criteria.

What is perhaps especially odd here is that the Court does not appear to have authorized the use of "big data" analytic tools—such as pattern matching to detect a group of targets who had changed phones or e-mail accounts—that might plausibly be said to truly *require* a comprehensive database, but rather limited queries of that data to selectors for which a particularized determination of reasonable suspicion had been made. At that point, of course, a more traditional and circumscribed conception of relevance would permit the same records to be obtained via targeted orders. Thus the full weight of the justificatory burden for untargeted collection is effectively borne by the argument that it is necessary to enable historical access to records that might ultimately be determined to be relevant.

In other words, everything is relevant now because anything might turn out to be relevant in the future. The government has gestured toward the need to articulate a limiting principle to its collection powers by stressing that communications records in particular can be fruitfully analyzed in bulk to reveal networks of association—but to the extent that the real weight of the argument is borne by the putative necessity of historical access, it would apply to any body of records not retained indefinitely that could conceivably be relevant to an investigation. This should be especially troubling given that the same "relevance" language appears in the statutes authorizing National Security Letters, which do not require advance judicial approval.

The FISC's justification of the telephony metadata program has been extensively criticized on both constitutional and statutory grounds in a recent paper

by Professor Laura Donohue, and that critique largely applies, mutatis mutandis, to the e-mail metadata program. In the latter case, however, even if we accept the government's strained reliance on *Smith v. Maryland* and the increasingly untenable legal fiction that it is unreasonable for Americans to expect any privacy in records of their communications held by third parties, there is an additional complication: It would appear, though redactions make it hard to be certain, that metadata about e-mail communications was obtained not from e-mail providers themselves, but from Internet Service Providers that do not normally retain such information in business records or, indeed, need to process it as an incident to the provision of service. Relative to the ISP, e-mail metadata—which is not *necessarily* knowingly disclosed to or retained by any third party, at least in the case of communications between entities that maintain their own mail servers—could reasonably be considered just another form of content. Again, due to redactions in the published opinions, it is unclear how adequately the FISC dealt with this technical feature of Internet communications.

Though the FISC did attempt to impose restrictions designed to protect the privacy of innocent Americans, these were "continuously violated" over a period of years, while the Court was repeatedly misinformed about the technical details of the collection program's operation. As the FISC noted in another recently disclosed opinion, this is one of at least three instances in as many years in which the government had "disclosed a substantial misrepresentation regarding the scope of a major collection program." In the case of the 215 telephony metadata program, the Court found that as a result of these misrepresentations, the rules imposed by the

FISC had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall regime... has never functioned effectively."

The third such known instance, involving overcollection of domestic communications under the FISA Amendments Act's §702 authority, did at least occur under a provision clearly intended for large-scale collection. Here, the problem was that if a single e-mail triggered the NSA"s automatic filters while a user was downloading his inbox, the entire stream — including totally domestic messages — could be captured. As the FISC observed, even if this were a relatively rare occurrence, the massive scale of NSA interception meant the agency could be vacuuming up some 56,000 wholly domestic emails annually. This approach, the court drily concluded, was "deficient on statutory and constitutional grounds."

In light of the massive scale of this collection, that the American communications are deemed to be acquired "incidentally," and the U.S. communicants are not intentionally "targeted," provides little comfort. The general warrants deplored by our Founders, which inspired the Fourth Amendment, were similarly not "targeted" at any particular U.S. person—but that was accurately seen, not as some kind of safeguard, but as the essential problem.

Concerns on this score should be compounded by diclosures that NSA databases can then be queried for selectors associated with U.S. persons. Another recent report informs us that the "intelligence purposes" for which the collected data might be used include compiling derogatory information about the embarrassing online sexual habits of "radicalizers"—apparently including, in at least

one case, a U.S. person—who are engaged in Internet speech hostile to the United States, but not directly linked to violent groups.

Finally, the broad claims of intelligence necessity upon which the FISC relied in authorizing the program appear not to have withstood scrutiny—and this program, at least, was discontinued in 2011, though it remains unclear how broadly components of the intelligence community continue to collect Internet metadata under other programs or authorities.

Similar claims about the necessity of the telephony program have not fared much better. From initial claims that dozens of "terrorist events" were "disrupted" by that program *along with* PRISM surveillance, it has become clear that in only a single material support case did the 215 program provide a unique or essential lead, and in an amicus brief filed in support of an ACLU lawsuit, several senators with access to the classified details argue that there is "no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means." Indeed, even as the FBI has repeatedly reassured the FISC of the value of this program, an exchange reported in Garret Graff's book *The Threat Matrix* quotes former FBI director Robert Mueller describing what appears to be the 215 telephony program as a "useless time suck."

This is a continuation of a pattern we have seen on numerous occasions over the past decade. Shortly after the terrorist attacks on September 11, 2001, President George W. Bush authorized the National Security Agency to conduct broad

telephone and Internet surveillance outside the procedures of the Foreign Intelligence Surveillance Act—a program that would eventually come to be known as STELLAR WIND. When one component of that program, involving warrantless telephone wiretapping, was discovered and—eventually—disclosed by reporters for *The New York Times*, the administration insisted on its effectiveness and vital importance. Former NSA director Michael Hayden claimed that it had "been successful in detecting and preventing attacks inside the United States." Vice President Dick Cheney went still further, asserting that the program had "saved thousands of lives."

Yet when the intelligence community's Inspectors General finally published an unclassified report on the program, they noted that the officials they interviewed "had difficulty citing specific instances where [the program] had directly contributed to counterterrorism successes." As one senior CIA official told NSA historian Matthew Aid: "We spent a ton on the program but got back very little in the way of solid returns. I don't think it was worth the money."

Fusion centers, massively funded by the Department of Homeland Security over the past decade, were repeatedly hailed by intelligence officials as a "vital, proven tool" and a "centerpiece of our counterterrorism strategy." It was only last year that an extensive, bipartisan Senate investigation concluded that they had in fact produced no useful counterterror intelligence, and indeed risked violating the Privacy Act by generating reports of citizens' First Amendment protected activities.

I am not, I wish to stress, claiming that intelligence officials deliberately mislead either Congress or the FISC about the importance of these programs. But the employees of every government agency naturally tend to believe that their programs and authorities serve an essential public purpose, and that internal assessment should not be uncritically accepted—especially when the authorities in question impinge on Americans' privacy and civil liberties.

It has become increasingly clear that the FISA court, conceived as a body charged with assessing and authorizing specific targeting decisions, is ill equipped in its current form to evaluate broad *programs* of surveillance and data collection. Greater transparency, and some form of adversarial process in cases where the FISC considers novel legal and technological questions, may remedy the problem somewhat, but it would be better still to require the intelligence agencies to seek specific congressional authorization for collection on that scale, limiting the existing authorities to collection with a specific nexus to a suspected foreign agent—a limitation the Senate already unanimously approved back in 2005.

I note in closing that we have been assured the violations of existing rules limiting surveillance require no further constraint because, for the most part, they have not been determined to be "willful" or "intentional." I do not find this reassuring for several reasons.

First, in any system of oversight, inadvertent violations are more likely to be discovered than willful abuses, precisely because inadvertent violators take no steps to evade detection. We know from our own history that when intelligence agencies

engaged in clearly illegal political surveillance throughout the 1960s, they took elaborate steps to evade the more anemic oversight structures in place prior to the passage of FISA, avoiding the creation of any official record of abuses. In one case discussed by historian Athan Theoharis, for instance, a member of Congress made repeated improper requests for access to FBI files on specific individuals. In each case, the request was met with a formal letter of denial—hand-delivered by an agent carrying the requested files in a briefcase. We should not expect bad actors in the future to be less ingenious.

Second, the history of intelligence abuses uncovered by the Church Committee in the 1970s *sometimes* involved wholly illegal surveillance unconnected to any legitimate intelligence purpose. Often, however, information obtained through surveillance that had some colorable intelligence justification in its inception was later—sometimes years later—misused for political purposes.

Third, and relatedly, the sheer volume of modern collection makes intentional abuse vastly harder to definitively prove. Whatever excuses might have been offered for the extensive campaign of surveillance, slander, and harassment directed at Martin Luther King and other political activists and dissidents, nobody could plausibly claim that the telephones and offices of the Southern Christian Leadership Conference had been wiretapped *inadvertently* or *incidentally*. Against the background of bulk collection, however, it is likely to be far more difficult to distinguish between deliberate abuse and a well-intentioned data query that happens to return information about innocent Americans—one reason that, at the

very minimum, Congress should require judicial approval before selectors pertaining to Americans can be used to query foreign intelligence databases.

Again, I do not mean to claim that we have reason to believe abuses of the type revealed by the Church Committee are now occurring, or have occurred in the past decade. It is entirely plausible they have not. We must recognize, however, that we have constructed—not through any one particular authority, but by the cumulative expansion of interconnected intelligence powers—an architecture of surveillance vastly more potent than anything those responsible for COINTELPRO or Operation SHAMROCK could have conceived. When even inadvertent misuse of that architecture can go undetected by overseers for years at a time, it seems unwise to wait for evidence of malice before imposing commonsensical limits on the programs that are demonstrably vital to national security—and eliminating entirely those whose value remains largely theoretical.

Statement for the Record

United States Senate

Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Carrie F. Cordero

Director of National Security Studies
& Adjunct Professor of Law

Georgetown University Law Center

Introduction

Mr. Chairman, Ranking Member Grassley, members of the Committee, thank you for this opportunity to appear before you again to share my views on the important issue of continued oversight of U.S. Government surveillance activities, including activities conducted under the Foreign Intelligence Surveillance Act (FISA).

I am currently the Director of National Security Studies and an Adjunct Professor of Law at Georgetown University Law Center, where, among other things, I teach a course on Intelligence Reform. The views presented in this statement and at this hearing are my own, and should not be construed to reflect the views of any employer, current or former. This statement was reviewed by the government for classification purposes.

By way of background, prior to joining Georgetown Law in November 2011, I spent my career as a practicing national security lawyer in the Executive Branch. In 2009, I served as Counsel to the Assistant Attorney General for National Security at the United States Department of Justice, where I co-chaired an interagency group created by the Director of National Intelligence (DNI) to improve FISA processes. From 2007-2009, I served in a joint duty capacity as a Senior Associate General Counsel at the Office of the Director of National Intelligence, where I worked behind the scenes on matters relating to the legislative efforts that resulted in the FISA Amendments Act of 2008. Once that law was passed, I was involved in many aspects of implementing the FISA Amendments Act, as well as standing up the internal executive branch interagency oversight structure. Prior to my tour at ODNI, I served for several years as an attorney in the office now called the Office of Intelligence, which is part of the National Security Division at the Department of Justice, and appeared frequently before the Foreign Intelligence Surveillance Court (FISC). I handled both counterterrorism and counterintelligence national security investigations. Later, I became involved in policy matters, including contributing to the development of the Attorney General's Guidelines for FBI Domestic Operations and updated FISA minimization procedures. I also did a short stint as a Special Assistant United States Attorney in the Northern District of Texas. Early in my career, I spent considerable time preparing information that was reported to both the Intelligence and Judiciary Committees of Congress as part of the annual public reports on FISA as well as the comprehensive semi-annual reports on FISA. In short, I am one of a very small handful of attorneys currently outside of government who has direct experience with the operational, legislative, policy, and oversight aspects of FISA, as it was practiced from 2000-2010.

Accordingly, my views are informed by this up-front perspective regarding how the USA PATRIOT Act of 2001, the Intelligence Reform and Terrorism Prevention Act of 2004, and later the FISA Amendments Act of 2008, vastly improved the Intelligence Community's ability to protect the nation from another attack on the scale of September 11th. More recently, I have had the added benefit of having spent the past three years outside of government to reflect, and to engage with the academic community, and to some extent the public, regarding some of the issues this Committee is considering today.

Since the Committee's October 2, 2013 hearing, the legislative debate and public conversation have been influenced by additional events. First, new legislation has been

introduced, in particular, S.1599, the USA FREEDOM Act, a bipartisan bill sponsored by the Chairman; as well as S.1631, the FISA Improvements Act of 2013, the bill put forth by Chairman Feinstein of the Senate Select Committee on Intelligence, who, of course, also serves on this Committee. That bill has been voted out of Committee. Second, the Executive Branch has declassified additional documents that are relevant to the current legislative debate, including but not limited to a FISC opinion on the ongoing telephony metadata program,[1] as well as a FISC opinion regarding the collection of Internet metadata that has since been discontinued.[2] Third, additional unauthorized disclosures of classified information have continued on what seems like at least a weekly basis. A recent example is the December 4, 2013 *Washington Post* story on NSA's collection of international cell site data.[3]

As a result of these and other developments, the conversation has shifted somewhat from where it was in October. I would like to offer a few observations that pick up on these developments. First, I would suggest that the conversation has evolved from objections to specific programs, such as the 215 or 702 collections (although objections do remain, particularly on 215), to a discussion of our cultural understanding and acceptance of foreign intelligence surveillance activities more broadly. Consideration of providing privacy protections to foreigners in the surveillance context, as well as whether to prohibit altogether the use of FISA for so-called "bulk" collection, have become a larger part of the debate. Second, legislative proposals, including S.1599, are coming closer to scaling back national security legal authorities in a way that would take the country backwards by reinstituting legal standards above and beyond what is required in the criminal investigative context. And, third, the path forward on authorized public disclosure in a way that both protects classified information and restores relationships between the private sector and consumers, as well as between the private sector and the U.S. Government, remains a worthy goal, but a significant challenge.

I. Proposals to Scale Back Foreign Intelligence Collection

A. Metadata Collection

Increasingly, the argument against the telephony metadata[4] collection under the business records provision of FISA, as amended by section 215 of the USA PATRIOT Act, focuses on

---

[1] Memorandum Opinion, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[2] [Redacted], PR/TT [Redacted], Opinion and Order, dated [Redacted], (available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf).

[3] Barton Geilman and Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, December 4, 2013 (http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html).

[4] Footnote 1 in Judge Mary McLaughlin's October 11, 2013 primary order defines "telephony metadata" as:

> "...comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc...), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. 2510(8), or the name, address, or

what I will call the "power of metadata" argument.[5] The argument goes something like this: metadata, that is, the information about our communications (such as dialed digits made in a phone call), can be assembled and analyzed in a way that it previously could not, both due to the way that data is communicated, retained and collected, as well as through tools that are now available to analyze it. Therefore, the argument goes, if the government collects large volumes of Americans' metadata, and then assembles, maps and/or analyzes that information, the government could learn an awful lot about a person, or a group of persons, simply by looking at metadata. Accordingly, metadata is a very powerful tool and there should be limits on the government's collection and use of it.

I doubt most Americans would argue with this proposition. I certainly don't. The problem with this argument made in the context of the debate concerning the current NSA surveillance activities under FISA, and the 215 program in particular, is that the worrisome assemblage of Americans' metadata bears no relation to the existing 215 program under consideration by Congress. According to the information that has been publicly disclosed by the Government, the telephony metadata program under section 215 does collect an enormous volume of Americans' telephone call detail records.[6] The collected information does not appear to include the content of phone calls, names of subscribers, payment information, or location information. The vast majority of the information collected is never viewed by human eyes. It simply sits in a so-called electronic or digital "black box," held by the NSA, and eventually ages off the system. The records are collected under FISA Court order that requires that the data acquired under this program: (i) only be used for counterterrorism purposes; (ii) only be queried by trained, designated personnel and that the queries themselves are approved by a smaller number of designated supervisory personnel; (iii) only be queried according to standards set out in the order; (iv) be destroyed within five years of collection; and (v) be subject to additional handling and processing procedures as directed by the FISC in its order.[7] The Court has said, in a written opinion, that without all of the limits in place, the Court would not have approved the program.[8]

Moreover, current Supreme Court precedent holds that there is no expectation of privacy in our telephone metadata, that is, the numbers we dial or the numbers that dial us. A warrant is not required to obtain this information.[9] Likewise, Supreme Court precedent also still holds that

---

financial information of a subscriber or customer. Furthermore, this Order does not authorize the production of cell site location information (CSLI)." (opinion and order available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[5] I previously described this and a second issue discussed in this statement in a post on *Lawfare* on November 14, 2013 (http://www.lawfareblog.com/2013/11/thoughts-on-two-propositions-the-power-of-metadata-and-providing-privacy-protections-to-foreigners/).

[6] *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-109, dated August 29, 2013, at p.4 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[7] Memorandum Opinion, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[8] *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-109, dated August 29, 2013, at p.3 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[9] *Smith v. Maryland*, 442 U.S. 735 (1979).

we do not have a reasonable expectation of privacy in records voluntarily turned over to a third party.[10] In the first publicly-released FISC opinion on the 215 program dated August 29, 2013, Judge Claire Eagan, approving continuation of the business records metadata program, offered a straightforward analysis of the law:

> In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such Orders were lawful and required, and the requested Orders were therefore issued.[11]

Since this Committee's October 2, 2013 hearing, the Government has released a new written opinion, by Judge Mary McLaughlin, who had not previously ruled on the 215 program. Judge McLaughlin approved the continuation of the program, and adopted Judge Eagan's previous analysis. In addition, she distinguished *United States v. Jones*,[12] the 2012 case concerning GPS surveillance, stating that "*Jones* involved the acquisition of a different type of information through different means."[13] She went on to state:

> The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, *Smith* remains controlling with respect to the acquisition by the government from service providers of non-content telephony metadata such as the information to be produced in this matter.[14]

In the meantime, current collection activities, based on the FISC opinions and accompanying materials that have been declassified by the government, are consistent with *current* precedent and *existing* interpretations of the laws.

As I noted in my previous statement, with respect to 215 in particular and intelligence programs generally, I believe that they should be regularly reviewed and evaluated to determine whether they continue to be necessary and valuable. It is wholly appropriate to end a collection program that has outlived its usefulness, or perhaps is no longer necessary based on new

---

[10] *United States v. Miller*, 425 U.S. 435 (1976).

[11] *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-109, dated August 29, 2013, at p.3 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[12] 132 S.Ct. 945 (2012).

[13] Memorandum Opinion, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013, at p.4 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[14] Memorandum Opinion, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013, at p.5-6 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

technologies or methods of collecting intelligence that may be more efficient or productive. As we now know publicly from the release of the opinion regarding the now-defunct Internet metadata program, intelligence programs come and go. And so it may be useful for Congress to look beyond the immediate focus on 215, and think more broadly regarding what limits it may or may not want to place on the Intelligence Community in light of as-yet-unforeseen threats or needs.

Some will argue that Congress should outlaw bulk collection under FISA, based on the "power of metadata" argument as well as arguments about our changing expectation of privacy in light of the methods of modern communications. But everyday Americans, or friends in foreign nations, are not the only people using the Internet to communicate. We *all* - - regular people, government leaders, as well as those who pose national security threats such as terrorists, terrorist financiers and facilitators, proliferators of weapons of mass destruction, spies, sophisticated hackers, and cyber intruders - - use the Internet, computers, and smart phones to communicate. And so just as regular people should not be expected to turn off their modern communications and revert to old fashioned modes of communication, neither should the Intelligence Community or law enforcement resort to pen, paper and index cards to conduct national security collection or investigations. It is just as unrealistic to expect citizens to unplug, as it is to expect or require the NSA or FBI to use 20th century collection, analytic or investigative techniques or methods to protect the nation from 21st century threats.

B. Providing Privacy Protections to Foreigners

In light of recent unauthorized disclosures, concerns have also been expressed regarding the NSA's collection targeting or pertaining to foreign persons located outside the United States. Suggestions have been made that U.S. foreign intelligence collection should recognize some sort of privacy right for non-U.S. persons.

In fact, the U.S. Intelligence Community has a recent history of affording Constitutional protections to persons who are not entitled to them. Congress made a deliberate decision with the passage of the FISA Amendments Act of 2008 to end that practice. And for good reason: prior to 2007, the U.S. government was, in fact, going through incredible hoops to acquire certain communications of foreign terrorist targets overseas. Two parallel processes caused this to happen. The first was described in a written statement for the record by the Director of National Intelligence before this Committee in September 2007[15]

> "...[P]rior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a

[15] Statement for the Record of J. Michael McConnell, Director of National Intelligence, Before the Senate Judiciary Committee, September 25, 2007 (available at http://www.dni.gov/files/documents/Newsroom/Testimonies/20070925_testimony.pdf).

> foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests."

In other words, the Intelligence Community, because of the requirements of the FISA statute prior to 2007, found itself in a position where it was seeking individual probable cause-based orders from the FISC to target terrorists overseas. When the government needed to obtain certain communications of a terrorist target, located in, as examples, Pakistan or Yemen, it was preparing a full application to the FISC, with a detailed factual showing providing probable cause that the target was an agent of a foreign power, and obtaining the signatures of a high ranking national security official and the Attorney General, and then submitting that application to the FISC for approval. This extensive process, in addition to being unnecessary from a Constitutional perspective, was a crushing force on the system.

In a separate but somewhat related chain of events and as described in the Senate Select Committee on Intelligence's Report of October 26, 2007,[16] in January 2007, the Attorney General announced that collection that had previously been conducted under the Terrorist Surveillance Program had transitioned to collection authorized by the FISC. The FISC's authorization was based on findings that "'there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist group.'"[17] According to the SSCI report, Congress subsequently received the Administration's proposal to modernize FISA in April 2007. The report went on to state:

> "The Administration's proposal for FISA modernization was comprehensive, and had been coordinated within the Department of Justice and the intelligence community. At the end of May 2007, however, attention was drawn to the FISA Court. When a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information from the Court. In late July, the DNI informed Congress that the decision of the second FISA Court judge had led to the *degraded capabilities in the face of a heightened terrorist threat environment*. The DNI urged the Congress to act prior to the August recess to *eliminate the requirement of a court order to collect foreign intelligence about foreign targets located overseas*."[18] [emphasis added]

As this Committee is aware, in August 2007, Congress enacted the Protect America Act of 2007, the interim law. Next came the FISA Amendments Act of 2008, including the significant section 702, which enabled collection against non-U.S. persons reasonably believed to be outside the

---

[16] Report 110-209, Senate Select Committee on Intelligence, Foreign Intelligence Surveillance Act of 1978, Amendments Act of 2007, (http://www.intelligence.senate.gov/071025/report.pdf).
[17] *Id.* at p.5.
[18] *Id.* at p. 5-6.

United States to proceed, not under probable cause requirements, but under a Director of National Intelligence and Attorney General approved certification, and under targeting and minimization procedures approved by the FISC. Future considerations of affording Constitutional protections to foreigners outside the United States should take the experiences of this recent history into account.

II. Analysis of Selected Sections of S.1599

I would next like to highlight four components of S.1599. The first three would, in my view, significantly limit the effectiveness of the U.S. Government to conduct foreign intelligence activities to protect the nation from the national security threats of today, and, tomorrow. The fourth is a brief comment on competing proposals to add an adversarial component to the FISA process.

First, sections 101 and 201 would change the legal standards to obtain business records and implement pen register/trap and trace devices by requiring a connection to an agent of a foreign power. The sections also add a "materiality" requirement in addition to relevance. The likely intended effect of these provisions is to eliminate the utility of these provisions for large scale collection, such as the 215 telephony metadata program. But the proposed changes would likely have far more dramatic, and harmful, consequences to more traditional, day-to-day, national security investigations. The standards are currently aligned with investigative authorities in the criminal investigative context, such as subpoenas and pen register/trap and trace surveillance conducted under Title 18. Both of those criminal authorities operate on a relevance standard. By raising the standard to requiring a connection to an agent of a foreign power, these sections would render these investigative techniques nearly useless in the early stages of an investigation, which is precisely when they are most useful. Investigators may never get to determine whether a target rises to the agent of a foreign power standard, if they cannot conduct the less intrusive records request or pen register/trap and trace surveillance as part of an investigation. These changes, if made law, would return us to the days prior to September 11, 2001, when it was harder for an investigator to request records or conduct pen register/trap and trace surveillance in an international terrorism case than it was in an everyday drug or fraud case.

Similarly, section 501 would amend the collection of statutory authorities known as "national security letters" by requiring the requested records to have a connection to an agent of a foreign power. The effect of this provision, if it became law, cannot be understated: it would severely limit the FBI's ability to conduct timely and thorough national security investigations. The criminal investigative counterpart to a national security letter is a subpoena. Subpoenas are issued based on relevance to an investigation. By requiring a nexus to an agent of a foreign power, which is a defined set of terms under FISA, the bill limits the ability of the FBI to request records at early stages of investigation. Moreover, Attorney General Guidelines require that national security letters may only be used in the context of a predicated investigation, which must meet certain factual thresholds and supervisory approvals; national security letters may not be used in an assessment alone.[19] This limiting guideline already imposes a higher bar to

[19] *Attorney General Guidelines for FBI Domestic Operations* (September 29, 2008) (http://www.justice.gov/ag/readingroom/ guidelines.pdf).

obtaining a national security letter than a subpoena for telephone or electronic mail subscriber information, which may be used at the assessment stage.[20]

Second, section 301 would appear to prohibit the Intelligence Community from querying data acquired pursuant to section 702 of FISA to search for U.S. person communications. Under the current minimization procedures approved by the FISC for 702 collection, the NSA may query communications already acquired under section 702 for U.S. person communications.[21] The proposed legislation would only allow the same query to take place if the U.S. person (presumably about whom the query is made) is the "subject of an order" of current surveillance, search or acquisition pursuant to FISA or criminal authorities. In other words, the U.S. person would already have to have been found to be an agent of a foreign power by the FISC, or the target of a criminal wiretap, both of which would require prior judicial approval based on probable cause. (The legislation does include emergency and consent exceptions to the proposed prohibition).

Consider the following hypothetical: this proposal could arguably prohibit the Intelligence Community from querying already lawfully acquired data to search for the methods of communication used by, say, Adam Gadahn, or someone like him. As Members of this Committee are aware, Adam Gadahn is a U.S. citizen who is on the FBI's Most Wanted Terrorist List.[22] He is a known al Qaeda propagandist and is the subject of a pending indictment on charges of providing material support to terrorism, among other charges.[23] Most recently, according to press reports, Gadahn posted an audio speech encouraging militants to attack U.S. interests.[24] Several days later, on December 5, 2013, American teacher Ronald Thomas Smith II was attacked and killed in Benghazi, Libya.[25] Let's assume for a moment that the U.S. Intelligence Community does not currently know what telephone numbers or email addresses Gadahn uses to communicate. (Again, I have no idea whether it does or does not have this information, or whether Gadahn even uses such modes of communication.) In such a case, querying existing, lawfully-acquired 702 data for accounts or identifiers used by Gadahn would be of significant foreign intelligence value. And, the issue is not whether Gadahn could be found to be an agent of a foreign power; under the legislation as drafted, it only matters whether he is, currently, the target of existing collection. If the U.S. Intelligence Community does not know what methods he uses to communicate, then he would not, as a practical matter, be a target of current collection authority, because there would be no number, account or identifier to collect against. In short, the proposed section 301 limitation would prevent the U.S. Intelligence Community of learning exactly the type of information we expect it to discover to protect U.S. interests and Americans from terrorist activity.

---

[20] *Id.*

[21] *See Exhibit B, Minimization Procedures Used By the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, dated October 31, 2011, at p.6 (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf).

[22] http://www.fbi.gov/wanted/wanted_terrorists.

[23] http://www.justice.gov/opa/documents/adam_indictment.pdf.

[24] Associated Press, *U.S. Teacher Shot Dead in Benghazi*, December 5, 2013 (available at http://online.wsj.com/news/articles/SB10001424052702303997604579240163015786696).

[25] *Id.*

This is not to suggest that querying NSA databases for U.S. person information is not sensitive. It is. And it should be done in accordance with meaningful procedures, approvals and oversight. Indeed, according to the now-declassified minimization procedures governing 702 collection, the "use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures[,]" and are subject to oversight by the Department of Justice and the Office of the Direct of National Intelligence.[26] Accordingly, while I do see the issue of NSA queries using U.S. person identifiers to be a legitimate issue for this Committee and/or the Intelligence Committee to conduct oversight of, I would submit that the legislative proposal to prohibit such queries is inappropriately restrictive in the context of the national security mission.

Third, section 302 would appear to limit the way in which NSA uses its collection technologies against valid foreign intelligence targets. Unfortunately, in an effort to limit certain kinds of collection to only those circumstances that would protect against international terrorism or the proliferation of weapons of mass destruction, this provision leaves open the possibility that certain collection techniques would not be available against other valid threats, such as cyber-based threats. For example, a cyber attack directed against U.S. critical infrastructure, perpetrated by or at the direction of a foreign power, would appear not to fall into the exception. Understanding that the intent of this provision is likely intended to make certain collection techniques available only in the most serious of threats, articulating them in the statute itself would leave the Intelligence Community vulnerable to facing operational situations where the law again lags behind the threats and sophistication of hostile actors.

Fourth, section 901 of the bill would add an Office of Special Advocate. I would refer the Committee to my previous statement, in which I discuss why, in my view, a separate office is both unnecessary given the FISC's independent oversight of Executive Branch activities, and would add significant bureaucracy to an already heavily lawyered FISA process. However, given the increasing Congressional and public interest in providing the FISC with the ability to call on outside views in considering novel issues, I would submit that the approach offered in S.1631, which gives the FISC discretion to appoint an *amicus curiae* for either legal or technical advice or views, is less objectionable than establishing a permanent Office of the Special Advocate.

III. Proposals to Enhance Transparency

S.1599 contains a number of transparency provisions directed at both surveillance authorities and national security letters. The legislation approaches the public reporting from two perspectives: what the companies can release, and what the U.S. government should release. In my view, there is substantial value in Congress continuing to work with the Executive Branch and the private sector to rebuild confidence between them, and for the U.S. Government to help the private sector restore confidence with consumers, customers and investors. In 2008, Congress acted in this area by including liability protection in the FISA Amendments Act for companies

[26] *See Exhibit B, Minimization Procedures Used By the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended,* dated October 31, 2011, at p.6 (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf).

that had voluntarily assisted the government after September 11, 2001, and whose cooperation was subsequently exposed by the significant unauthorized disclosure that took place in 2005.

In my previous statement, I suggested that, in the interests of facilitating transparency while reducing the reactive nature of each authorized public release, Congress could amend the reporting provisions in FISA to provide additional public information—whether it is statistics, declassified legal opinions, summaries of implementation actions or reports on compliance matters—semi-annually, quarterly, or at some other appropriate regular interval. I note that S.1599 contains several reporting provisions that would occur either annually, or quarterly.

With respect to the content of the proposed public reports, I would suggest that further consideration and revision is in order, on several fronts. As a guiding principle, I would suggest that any new public reporting only be mandated by law if Congress is confident that it can reasonably be produced *accurately*. Inaccurate or inconsistent reporting will lead to more questions and less confidence, and may be worse than no reporting at all.

While I would expect that representatives of the Intelligence Community will address concerns with the legislation about disclosing information about targets of surveillance or other data points that may be impossible to produce, I would like to highlight several sections that would benefit from additional consideration:

- Section 601 provides that electronic service providers may report on estimates of demands and requests made and complied with, and estimates of numbers of users or accounts. It may be that the providers and government prefer estimates versus actual numbers, but the proposal does raise some concerns that public reporting from different sources will be inconsistent, which may have the unintended consequence of undermining confidence, not bolstering it. I would also urge caution on releasing numbers of users or accounts affected: if targets use multiple accounts, the number may be misleadingly high.

- Section 601 also proposes to define "surveillance law." Curiously, the section includes the national security letter statutes, which are not surveillance laws, but appears to exclude the federal criminal wiretap law.

- Section 602 proposes that the government disclose numbers of persons "subject to electronic surveillance." If the intent of this proposal is to release how many individuals' communications were collected—either through targeting or incidentally—then it is important to consider the reverse effect on privacy protections that this disclosure would have. Because intelligence analysts only review communications in pursuit of identifying foreign intelligence information, there is a body of collected information that is either never reviewed, or, reviewed but not analyzed, reported, or counted for any statistical purposes. Similarly, minimization procedures would require that analysts not write reports about U.S. persons who may be incidentally collected but whose communications do not appear to be foreign intelligence information. Accordingly, a requirement to report on numbers of persons collected would actually degrade privacy practices: it would require that Intelligence Community personnel look at, read, review, count, keep records

about and report on information that they otherwise would disregard in pursuit of their actual mission of discovering, analyzing and reporting foreign intelligence information.

Conclusion

I thank the Chairman, Ranking Member and Committee Members for providing me with this additional opportunity to share my views on the efforts to reform U.S. Government surveillance activities. Although there is significant public and political pressure to act to reform surveillance activities, I continue to urge the Committee to move cautiously: changes made quickly now will have consequences for the nation's security for years to come. I look forward to continuing to work with the Members and staff of this Committee on these important issues.

Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing on "Continued Oversight of U.S. Government Surveillance Authorities"
December 11, 2013

Today, the Judiciary Committee meets to conduct further oversight of the intelligence community's surveillance activities. This Committee has held a series of open hearings that have sharpened the Committee's thinking and furthered the public dialogue on these important issues. Today marks our third full Committee hearing, and Senator Franken also convened a hearing on transparency issues last month in the Subcommittee on Privacy, Technology and the Law.

At our first hearing in July, we discussed with Deputy Attorney General Cole the broad "relevance" standard that is being used to justify the bulk collection of Americans' phone records under Section 215 of the USA PATRIOT Act, and I appreciate that the Deputy Attorney General has returned today to continue that discussion. We also discussed the utility of the bulk phone records collection program in light of statements by some officials that had conflated the usefulness of Section 215 with Section 702 of the Foreign Intelligence Surveillance Act (FISA), and left the inaccurate impression that 54 terrorist "plots" had been "thwarted" as a result of these programs. Deputy Director Inglis helped to clear up this confusion, and we learned that in fact there was only one example of the Section 215 phone records program being the "but-for" cause of disrupting a terrorist event. That sole example was a material support prosecution of a San Diego cabdriver who sent roughly $8,000 to Somalia.

At our second hearing in early October, General Alexander confirmed that the notion that the Section 215 phone records program had helped to thwart 54 terrorist plots was inaccurate. General Alexander and Director of National Intelligence Clapper also answered questions about the trust deficit arising from the range of serious legal violations committed in programs conducted under Section 215 of the USA PATRIOT Act and Section 702 of FISA.

Today, the Committee renews its examination of government surveillance activities – once again in the wake of a series of new revelations. These new disclosures raise significant questions about the scope and wisdom of our surveillance activities both at home and abroad. It is clear that the oversight work of the Committee is far from finished.

Just in the last week, there have been press reports that the NSA is collecting billions of records a day of cell phone locations around the world, and can track individuals and map their relationships. There also have been reports that the NSA is monitoring online video games.

And last month, the administration released a set of documents revealing details about yet another massive dragnet collection program, in addition to the phone records program. This time the NSA was gathering in bulk an enormous amount of Internet metadata, under the pen register and trap and trace device authority in FISA. Just like Section 215, there is nothing in the pen register statute that expressly authorizes the dragnet collection of data on this scale.

Although the Internet metadata collection program is not currently operational, it resulted in a series of major compliance problems – just like the Section 215 program. According to the FISA Court, the NSA exceeded the scope of authorized acquisition not just once or twice, but "continuously" during many of the years the program was in operation. The problems were so severe that the FISA Court ultimately suspended the program entirely for a period of time before approving its renewal. Once renewed, the government asserted that this bulk collection was an important foreign intelligence tool – which is the claim it makes now about the Section 215 phone records program. But then in 2011 the government ended this Internet metadata program because, as Director Clapper explained, it was no longer meeting "operational expectations." It is important to note that the administration does not believe that there is any legal impediment to re-starting this bulk Internet data collection program if it – or a future administration – wanted to do so.

The legal justification for this Internet metadata collection is troubling. As with the Section 215 program, the Internet metadata program was based on a "relevance" standard. And as with the Section 215 program, there is no adequate limiting principle to this legal rationale. The American people have been told that all of their phone records are relevant to counterterrorism investigations. Now they are told that all Internet metadata is also relevant; and apparently fair game for the NSA to collect. This legal interpretation is extraordinary, and will have serious privacy and business implications in the future – particularly as new communications and data technologies are developed.

So it should come as no surprise that the American technology industry is greatly concerned about these issues. I have heard from a number of companies who worry that their global competitiveness has been weakened and undermined. American businesses stand to lose tens of billions of dollars in the coming years, and we need to make substantial reforms to our surveillance laws to rebuild confidence in the U.S. technology industry.

Earlier this week, eight major technology companies – including Microsoft, Google, Apple, Facebook, and Yahoo – released a set of five principles for surveillance reform. Citing the "urgent need to reform government surveillance practices worldwide," the companies call for greater oversight and transparency, but importantly they also advocate for limits that would require the government to rely on targeted searches about specific individuals, rather than the bulk collection of Internet communications.

I have introduced the USA FREEDOM Act with Senator Lee here in the Senate, and our bill takes many of these steps. I appreciate the support we have received from the technology industry for those efforts, and I look forward to hearing its perspective on the second panel. Without objection I will place in the record the open letter and reform principles from the technology companies, an earlier letter from technology companies applauding the USA FREEDOM Act, and a supportive letter from a coalition of civil society organizations, companies, trade associations and investors.

Support from the technology industry is representative of the broad-based, bipartisan support for our legislation. Organizations across the spectrum have endorsed the bill, from the ACLU to the NRA. I also want to thank Senator Lee, Senator Durbin, Senator Blumenthal and Senator Hirono

on this Committee for their cosponsorship. Our bipartisan, bicameral legislation is a commonsense bill that makes real and necessary reforms. I welcome input on this legislation, and I look forward to working on this effort in the coming months. I want to thank our witnesses for being here today, and in particular for returning to this Committee after our unexpected postponement of this hearing in November.

#####

QUESTIONS FOR THE RECORD – Chairman Leahy
12/11/13 FISA Hearing

Questions for NSA Director Alexander

During the hearing, you agreed to provide additional documents and answers to questions. I have included a copy of the letter that Senator Grassley and I wrote last week with those questions. I appreciate your willingness to assist the Committee's oversight efforts by promptly gathering that material, and the responses you have provided thus far. I look forward to reviewing your complete responses to all of these questions as soon as possible.

QUESTIONS FOR THE RECORD – Chairman Leahy
12/11/13 FISA Hearing

Questions for Deputy Attorney General Cole

1. During the hearing, you agreed to provide additional documents and answers to questions. I have included a copy of the letter that Senator Grassley and I wrote last week with those questions. I appreciate your willingness to assist the Committee's oversight efforts by promptly gathering that material, and the responses you have provided thus far. I look forward to reviewing your complete responses to all of these questions as soon as possible.

2. A May 6, 2004, Office of Legal Counsel memorandum signed by Jack Goldsmith has been partially declassified and is available here: http://www.justice.gov/olc/docs/memo-president-surveillance-program.pdf. Has the administration considered declassifying additional portions of this memorandum? If not, will you commit to reviewing that memorandum and considering additional disclosures? If so, please explain the reasoning for not declassifying additional portions of the memorandum.

3. On November 18, 2013, the Director of National Intelligence declassified a FISA Court Opinion and Order by Judge Colleen Kollar-Kotelly, permitting the NSA to collect bulk Internet metadata under the FISA pen register statute. Although the time of day the order was signed and the hour it would expire were declassified, the full dates of the order and its expiration were both redacted.

   a. Please provide an explanation of the decision to redact the date of this opinion and its expiration date, including the harm to national security that would result from declassification.
   b. Please provide the date that Judge Kollar-Kotelly's order was signed and its expiration date.
   c. Please provide the dates of the subsequent declassified FISA Court orders and opinions relating to the Internet metadata bulk collection program under the FISA pen register statute.

4. When the FISA Court authorized the bulk collection programs for phone records and Internet metadata, was the NSA already collecting that information in bulk? If so, what legal authority was the government relying upon?

5. As a legal matter, can the NSA or any other element of the U.S. government engage in bulk collection of Americans' phone records or Internet metadata without a court order? Are there other legal authorities that do not require court orders that elements of the U.S. government could rely upon to gather this information? If so, please identify these authorities.

6. The Committee has heard testimony that it can be difficult to draw a line between content and non-content information in the Internet context. Much of the information in the FISC

opinions discussing the categories of data that NSA obtained under its Internet metadata bulk collection program is redacted. Yet the legal theory underpinning these programs relies heavily on the fact that they collect only non-content information.

a. Please provide a list of the Internet metadata that was obtained under the FISA pen register bulk collection program.
b. As a general matter, where has the executive branch drawn the line between content and non-content with respect to Internet communications? Please provide examples.
c. Is there a consistent practice across the criminal and intelligence surveillance authorities with respect to what constitutes the content of Internet communications?

QUESTIONS FOR THE RECORD – Chairman Leahy
12/11/13 FISA Hearing

Questions for ODNI General Counsel Bob Litt

1. During the hearing, you agreed to provide additional documents and answers to questions. I have included a copy of the letter that Senator Grassley and I wrote last week with those questions. I appreciate your willingness to assist the Committee's oversight efforts by promptly gathering that material, and the responses you have provided thus far. I look forward to reviewing your complete responses to all of these questions as soon as possible.

2. On November 18, 2013, the Director of National Intelligence declassified a FISA Court Opinion and Order by Judge Colleen Kollar-Kotelly, permitting the NSA to collect bulk Internet metadata under the FISA pen register statute. Although the time of day the order was signed and the hour it would expire were declassified, the full dates of the order and its expiration were both redacted.

   a. Please provide an explanation of the decision to redact the date of this opinion and its expiration date, including the harm to national security that would result from declassification.
   b. Please provide the date that Judge Kollar-Kotelly's order was signed and its expiration date.
   c. Please provide the dates of the subsequent declassified FISA Court orders and opinions relating to the Internet metadata bulk collection program under the FISA pen register statute.

3. When the FISA Court authorized the bulk collection programs for phone records and Internet metadata, was the NSA already collecting that information in bulk? If so, what legal authority was the government relying upon?

4. As a legal matter, can the NSA or any other element of the U.S. government engage in bulk collection of Americans' phone records or Internet metadata without a court order? Are there other legal authorities that do not require court orders that elements of the U.S. government could rely upon to gather this information? If so, please identify these authorities.

5. Please provide a list of all law enforcement or intelligence agencies that, at any point since September 11, 2001, have collected Americans' telephone and/or Internet metadata in bulk, and the legal authority relied upon. Please include a brief description of each program.

6. Please provide a list of all law enforcement or intelligence agencies that, at any point since October 26, 2001, have engaged in bulk collection of records of Americans relying upon Section 215 of the USA PATRIOT Act. Please include a description of each program.

7. For each bulk collection program identified in the previous two answers, please list the Inspector General reports (and associated dates) that have been conducted to review any aspect of those programs, and whether each Inspector General report was provided to Congress.

8. The Committee has heard testimony that it can be difficult to draw a line between content and non-content information in the Internet context. Much of the information in the FISC opinions discussing the categories of data that NSA obtained under its Internet metadata bulk collection program is redacted. Yet the legal theory underpinning these programs relies heavily on the fact that they collect only non-content information.

    a. Please provide a list of the Internet metadata that was obtained under the FISA pen register bulk collection program.
    b. As a general matter, where has the executive branch drawn the line between content and non-content with respect to Internet communications? Please provide examples.
    c. Is there a consistent practice across the criminal and intelligence surveillance authorities with respect to what constitutes the content of Internet communications?

Senator Amy Klobuchar
U.S. Senate Committee on the Judiciary
Full Committee Hearing
"Continued Oversight of U.S. Government Surveillance Authorities"
December 11, 2013
Questions for the Record

Questions For General Alexander and Deputy Attorney General Cole

Private Sector Disclosure

A number of leading technology firms, including Google, Apple, Yahoo, Facebook, AOL, Twitter, LinkedIn, and Microsoft, have signed an open letter calling for greater limitations on bulk collection and more transparency of the government's requests for data.

- Some of the legislation this committee may consider would allow companies to disclose the demands they receive from the government for bulk collection of customer data. Do you support such measures?
- Is there an alternate arrangement that could be made between the government and these companies to allow rapid access to necessary data while not engaging in bulk collection?
- I understand American technology firms are increasingly concerned that their association, knowingly or unknowingly, with the NSA's bulk collection is threatening their business overseas, costing them the trust of consumers and generating support for burdensome new foreign regulations on U.S. tech companies. Have you considered the impact of these revelations, and continued bulk collection, on our businesses?

Senator Amy Klobuchar
U.S. Senate Committee on the Judiciary
Full Committee Hearing
"Continued Oversight of U.S. Government Surveillance Authorities"
December 11, 2013
Questions for the Record

Questions For Mr. Black

Private Sector Disclosure

- Mr. Black, in your testimony, you discuss the importance of allowing companies to disclose the demands they receive from the Government for bulk collection of customer data. Why is this level of transparency important? Can you provide some concrete examples of the way this would help these companies?

- Is there an alternate arrangement that could be made between the government and these companies to allow rapid access to necessary data while not engaging in bulk collection?

Senate Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Ed Black

1. In your prepared testimony you criticized U.S. national security policy for operating "on the presumption that U.S. citizens online deserve protection from unwanted surveillance, while others do not." What new legal protections do you suggest U.S. law recognize for foreign terrorists abroad? For example, do you believe the government should be required to get a warrant to spy on a terrorist sitting in an internet café in Europe or Asia? Shouldn't our government be doing everything within the current law it can to fight terrorists, as opposed to giving them new legal rights?

Senate Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Professor Carrie Cordero

1. Based on your experience, what would the day to day operational effect be on the government's ability to keep the country safe if we recognized new legal rights that would protect foreign terrorists abroad from "unwanted surveillance"?

2. Please further elaborate and explain why you believe the *amicus* proposal contained in the Senate Intelligence Committee's FISA reform bill is a more advisable approach to making the FISA Court process more adversarial than the advocate proposal contained in the USA FREEDOM Act.

Senate Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Julian Sanchez

1. Concerns have been raised about whether the advocate position that would be established under the USA FREEDOM Act is constitutional. For example, it's unclear whether the advocate would have constitutional standing to be a party before the FISA Court. And it may not be consistent with the separation of powers to create an office housed in the judicial branch, without any oversight from the executive branch, which appears to possess executive branch powers and responsibilities. Do you share any of these concerns that may be important to those of us who interpret the Constitution strictly? If so, what are they?

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 9, 2015

The Honorable Amy Klobuchar
Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Klobuchar:

Please find enclosed responses to questions arising from the December 11, 2013, appearance of Deputy Attorney General James Cole and then-National Security Agency director General Keith B. Alexander before the Committee, at a hearing entitled "Continued Oversight of U.S. Government Surveillance Authorities." We hope this information is helpful. Please do not hesitate to contact this office if we may be of additional assistance to you. The Office of Management and Budget has advised us that there is no objection to submission of this letter from the perspective of the Administration's program.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Chairman

The Honorable Patrick J. Leahy
Ranking Minority Member

Hearing Before the
Committee on the Judiciary
United States Senate

Entitled
"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Questions for the Record from Senator Klobuchar for

General Keith B. Alexander

and

Deputy Attorney General James M. Cole

Private Sector Disclosure

A number of leading technology firms, including Google, Apple, Yahoo, Facebook, AOL, Twitter, LinkedIn, and Microsoft, have signed an open letter calling for greater limitations on bulk collection and more transparency of the government's requests for data.

- **Some of the legislation this committee may consider would allow companies to disclose the demands they receive from the government for bulk collection of customer data. Do you support such measures?**

Answer:

We understand the concerns that specific companies have expressed regarding their ability to inform their customers of how often data is provided to the Government in response to legal process. Accordingly, on January 27, 2014, the Administration acted to allow more detailed semi-annual disclosures by companies about the number of FISA orders issued to communications providers and the number of customer accounts targeted under those orders. As a result, a number of providers dismissed their lawsuit against the Department of Justice seeking greater disclosure. The policy reflects the Executive Branch's continuing commitment to making information about the Government's intelligence activities publicly available where consistent with the national security of our nation. We will review proposed legislation on these issues and work constructively with the Committee on approaches that balance transparency interests with national security.

- **Is there an alternate arrangement that could be made between the government and these companies to allow rapid access to necessary data while not engaging in bulk collection?**

Answer:

We understand this question to address the bulk collection of telephony metadata, which does not involve these companies. With regard to the bulk collection of telephony metadata, on January 17, 2014, the President directed a transition that will end the bulk Section 215 program as it currently exists. As part of that transition, the Administration consulted with Congress, the private sector, privacy and civil liberties groups, and other interested groups. For example, the Administration solicited information on U.S. industry's commercially available capabilities that could provide a viable alternative to the current program, and also held a listening session with experts and advocates to explore a range of expert outside opinions. Throughout this process, we welcomed public debate and discussion about how best to strike the right balance between our national security and the privacy of our citizens. On the basis of these consultations, and after having carefully considered the available options, the President decided, on March 27, 2014, on a proposal that, with the passage of appropriate legislation, will allow the government to end bulk collection of telephony metadata records under Section 215, while ensuring that the government has access to the information it needs to meet its national security requirements. The Administration has urged Congress to pass such legislation and supported efforts to pass the USA FREEDOM Act.

- **I understand American technology firms are increasingly concerned that their association, knowingly or unknowingly, with the NSA's bulk collection is threatening their business overseas, costing them the trust of consumers and generating support for burdensome new foreign regulations on U.S. tech companies. Have you considered the impact of these revelations, and continued bulk collection, on our businesses?**

Answer:

The Administration understands the difficult position that technology firms have been put in as a result of the unauthorized intelligence disclosures relating to lawful demands by the U.S. Government for data they possess. In December 2013, the President and the Vice President met with executives from leading technology firms to discuss issues of shared importance to the federal government and the technology sector, including the national security and economic impacts of these unauthorized intelligence disclosures and the national security interests at stake. In response to requests by companies to be able to provide more information about the national security and law enforcement requests that they receive from the government, and consistent with the President's direction in his speech on January 17, 2014, the Government now enables

communications providers to make public more information than ever before about the number of national security orders and requests issued to them, and the number of customer accounts targeted under those orders and requests. Permitting these detailed disclosures will allow companies to illustrate that national security orders and requests affect only a tiny percentage of their users, even taking all of the demands together, and thus to refute inaccurate reports that companies cooperate with the Government in dragnet surveillance of all of their customers.

Computer & Communications Industry Association

Tech Advocacy Since 1972

Questions for the record to

Edward J. Black

President & CEO of

The Computer & Communications Industry Association

Before the

Senate Judiciary Committee

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

1 Klobuchar:

Q: Mr. Black, in your testimony, you discuss the importance of allowing companies to disclose the demands they receive from the Government for bulk collection of customer data. Why is this level of transparency important? Can you provide some concrete examples of the way this would help these companies?

A: As in many other industries, consumer trust is vital to Internet services companies such as our members. Users today want to know how and why data about them is shared, because data today can reveal so much about a person. That is why CCIAs members and nearly every other company operating online today have privacy policies detailing what information they collect, how it is used, and with whom it is shared, so that consumers who want to be informed can do so. In fact, in a poll conducted recently by Benenson Strategy Group and American Viewpoint on behalf of CCIA, 65% of respondents reported that they read privacy policies as a means of understanding their privacy online better. What is good for the consumer is even better for the citizen, as citizens cannot simply choose to live under a different surveillance regime with a simple click. Without this kind of transparency, there can be no larger conversation about the ongoing use of surveillance in our country.

Trust is also the more parochial answer to your question. There are those who now presume that Silicon Valley and Ft. Meade are simply two sides of the same coin. We know that this does not represent the truth. Transparency about the numbers of requests will give customers data instead of speculation to base their decisions on. In this it is also essential that the data be as exact as possible. In a situation where suspicion is as high as it is right now, hiding behind large ranges of numbers in transparency reporting risks doing as much damage as reporting no numbers at all. The question will always be what do they have to hide?

Q: Is there an alternate arrangement that could be made between the government and these companies to allow rapid access to necessary data while not engaging in bulk collection?

A: With due respect, Senator, we believe that where the data lives at the end of the day is the wrong question. If the NSA is going to be engaging in three-hop contact chaining using this information, they will be sweeping in information about millions of Americans. The government has claimed that this sort of information carries no privilege of privacy under the Fourth Amendment. Whether or not that is true – and we are finally starting to see the judiciary come directly into contact with this idea and finding it repugnant to the Constitution – we should be asking ourselves whether large-scale analysis of information about Americans communications is something a democratic government should be engaging in.

Wherever the data lives, the fact will remain that the bulk phone records analysis program presents a grave risk to Americans privacy, and produces dubious national security benefits, as was pointed out last month by both Judge Leon of the DC District Court, and the Presidents own Review Group Report.

2 Grassley:

Q: In your prepared testimony you criticized U.S. national security policy for operating on the presumption that U.S. citizens online deserve protection from unwanted surveillance, while others do not. What new legal protections do you suggest U.S. law recognize for foreign terrorists abroad? For example, do you believe the government should be required to get a warrant to spy on a terrorist sitting in an internet caf in Europe or Asia? Shouldnt our government be doing everything within the current law it can to fight terrorists, as opposed to giving them new legal rights?

A: CCIA does not yet have concrete suggestions for the protections due to non-US citizens, but we do believe this subject should be one that Congress closely contemplates. Your question, Senator, focuses exclusively on what terrorists must be hiding abroad and the implications of giving them legal rights. What your questions ignores, however, are the billions of non-terrorists living their lives abroad. Billions of ordinary people over whom our government claims great power through its indiscriminate surveillance. Billions of potential customers for American Internet companies, along with the global customers of American products being sold online, who may now have second thoughts. Swiss data hosting providers, to provide an example, are experiencing growth in the hundreds of percent per year as companies migrate away from US-provided products. Cisco, on its most recent earnings call, made clear that it is seeing a dramatic decrease in sales in the very countries who are most upset about the Snowden disclosures. A recent survey of purchasing intention made clear that US-sourced products already face a significant competitive disadvantage due to the surveillance disclosures. If we continue to treat all foreigners as fair game for unlimited surveillance, US-based companies will not be able to sell to them. The source of our national security flows not only from surveillance, but also from the vitality of our economy, and our current choices on how we treat non-nationals is damaging our economic competitiveness and therefore our national security. Many leading members of Congress have long called for more cost / benefit analysis in evaluating government programs. Here, we are pointing out that there are massive economic and security costs to sweeping worldwide surveillance, that need to be, and have not yet, been fully understood.

The danger is not just to trade, but also to the idea of the open Internet as a vehicle for democracy and freedom around the world. Some of our members recognized this when they wrote the Global Government Surveillance Princi-

ples, particularly the principle of Respecting the Free Flow of Information. In response to the NSAs blanket surveillance of people from around the world, there have been calls to disrupt the non-geographical nature of the Internet by forcing data to live in certain places. These calls directly challenge the idea of a borderless Internet and threaten the free flow of data.

Nobody has suggested, and nor would we ever suggest, that surveillance is not appropriate over some small percentage of the worlds people. Even other countries agree with this fact. Of course the NSA must be able to analyze and track actual terrorists who aim to inflict imminent damage upon the United States. However, that does not mean that some measure of due process for the people of the world against our overwhelming ability to gather information on them cannot exist. Surely the country that put men on the moon, invented the technical underpinnings of the Internet, and created the Marshall Plan is capable of the vision required to meet this challenge.

United States Senate

Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

on December 11, 2013

Responses to Questions for the Record

submitted January 10, 2014

Carrie F. Cordero
Director of National Security Studies
& Adjunct Professor of Law
Georgetown University Law Center

Senate Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Questions for the Record from Ranking Member Charles E. Grassley

1. **Based on your experience, what would the day to day operational effect be on the government's ability to keep the country safe if we recognized new legal rights that would protect foreign terrorists abroad from "unwanted surveillance."?**

   Since the unauthorized disclosures, the public debate has included suggestions that U.S. national security surveillance activities should recognize the "privacy" rights of foreigners. There are a number of reasons why the U.S. Government should not go down this path. First, existing Supreme Court precedent maintains that non-U.S. persons outside the United States are not subject to constitutional protection. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). Second, as described in my written statement for the record, the U.S. Intelligence Community already has experience with what extending FISA probable cause protections to foreigners looks like, and the result was a FISA process stretched to its limits. Third, the issue of what is the proper extent of national security surveillance against foreign leaders or other sensitive targets belongs in the realm of foreign policy considerations, and should be therefore be addressed as a policy matter, not as a legal one.

   With respect to the operational impact more specifically, my written statement for the record describes the pre-2008 history of the FISA process which included seeking FISC approval for targeting certain terrorist targets overseas based on a finding of probable cause that the target was an agent of a foreign power. As a number of senior intelligence officials have previously testified before Congress, this resulted in a gap in foreign intelligence collection in support of the counterterrorism mission, both because of the heightened legal standard as well as because of the burden on the FISA process administratively. Future consideration of affording so-called privacy protections to foreign targets should take this recent history into account. Finally, I would submit that more time spent by U.S. Government operational and oversight personnel focusing on the legal rights of foreign targets could have the effect of diverting or diluting their attention to matters affecting U.S. persons or other persons inside the United States who are afforded constitutional protections.

2. **Please further elaborate and explain why you believe the amicus proposal contained in the Senate Intelligence Committee's FISA reform bill is a more advisable approach to making the FISA Court process more adversarial than the advocate proposal contained in the USA Freedom Act.**

As referenced in my two statements for the record submitted to this Committee for the October 2, 2013 and December 11, 2013 hearings, and responses to questions for the record related to the October 2, 2013 hearing, my view is that there are a variety of factors that weigh against creating an office of special advocate.

Operationally, a permanent office of special advocate has the potential to slow down intelligence activities by adding an additional layer of review on top of an already multi-layered legal and management process within the Executive Branch. An office of special advocate is likely redundant with existing bureaucratic processes. As FISC Judge Reggie Walton's letter of July 29, 2013 to the Chairman explains, there is also extensive review by and interaction between the Executive Branch and the FISC's legal advisors and judges. The existing levels of review include legal review within the requesting agencies, by the Department of Justice's National Security Division (and likely additional senior executives in the Department of Justice if a particular request is complex or novel), by the FISC's professional legal advisors, and finally by the judges themselves, who are independent federal district court judges. Adding an additional office of review duplicates work currently performed by Department of Justice attorneys (who are outside of the Intelligence Community) whose job it is to review applications for legal sufficiency, including conformity with the requirements of the Act as well as the protection of constitutional rights.

From a policy perspective, adding an office of special advocate also raises the possibility that the result will be less-well developed and considered requests for national security surveillance authority. At the Committee's December 11, 2013 hearing, in response to a question from Senator Blumenthal regarding the proposals for an office of special advocate, I stated that over time there has been a relationship "of trust" that has developed between the Executive Branch and the FISC. To further explain this perspective, what I was referring to by describing the relationship of trust is, in particular, the *credibility* that the Executive Branch, and the Department of Justice, in particular, has with the FISC. As described in my October 2, 2013 statement for the record, it has previously been suggested by outside observers and reviews that, at times, the Department of Justice has been cautious, perhaps to a fault, in presenting matters to the FISC. Current FISA practice consists of Department of Justice attorneys who present matters to the FISC conduct business according to the high standards of disclosure demanded by the ethics of *ex parte* procedure. By adding an institutional adversarial opponent, the proceedings would no longer be *ex parte*, therefore, there is the potential for the Executive Branch, and the Court, to, over time, become overly reliant on the special advocate to challenge requests for surveillance. This could have the unintended effect of actually reducing the scrutiny and care the Executive Branch gives to its applications. This outcome would be bad for national security and bad for civil liberties, because the FISC, over time, could potentially lose confidence in the Executive Branch's commitment to disclosing unfavorable facts and circumstances. It is not in the interests of U.S. national security to produce an adversarial process that could have the effect of eroding the confidence of the FISC that the Executive Branch is presenting matters

under a historical practice of full disclosure and the highest degree of candor as required by *ex parte* practice.

Accordingly, between the two options, the office of special advocate versus providing an avenue for the FISA Court to appoint an *amicus* in circumstance that raise novel issues of law or technology, I believe the *amicus* is preferable because it will likely only be invoked in rare circumstances, and will not run the risk of institutionalizing adversarial proceedings in the FISA process. It is worth nothing that in the criminal investigative context, requests for surveillance or search are similarly conducted *ex parte*. However, I do believe that the current FISA system is preferable to both, as I do not believe that either proposal will necessarily achieve what is likely the intended long-term objective of raising public confidence in activities conducted under FISA. This is because FISC deliberations will continue to (rightfully) be conducted in a classified setting, and so much of the criticism since the recent unauthorized disclosures have focused on the transparency of the FISA process and legal interpretations.

Senate Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Julian Sanchez

1. Concerns have been raised about whether the advocate position that would be established under the USA FREEDOM Act is constitutional. For example, it's unclear whether the advocate would have constitutional standing to be a party before the FISA Court. And it may not be consistent with the separation of powers to create an office housed in the judicial branch, without any oversight from the executive branch, which appears to possess executive branch powers and responsibilities. Do you share any of these concerns that may be important to those of us who interpret the Constitution strictly? If so, what are they?

ANSWER: I do not believe the creation of a special "advocate" to argue before the FISC in cases involving novel or complex questions of law presents any inherent constitutional difficulties on either standing or separation of powers grounds. The Advocate would serve in an effectively advisory role before the court, exercising no independent executive powers. Though superficially appearing before the court in as an adverse party, the practical role of the Advocate would be no different than that of an amicus or, for that matter, a thoughtful clerk ensuring that the FISC judges had an opportunity to consider a broad range of constitutional and statutory arguments bearing on the issue at hand.

If there are questions of standing stemming from the "cases or controversies" clause, at least with respect to arguments before the FISC or FISCR, they do not arise with the creation of an Advocate, but with the existence of the FISC itself, as a court structured to hear ex parte arguments not ultimately intended to result in—or, indeed, affording in most cases any opportunity for—an eventual adversarial proceeding between the government and the target of surveillance. If we assume the constitutionality of the basic FISA structure itself, the addition of an advocate presents no further constitutional problems. Standing problems *would* arise if the Advocate were intended to have further recourse to the Supreme Court, since she would represent no genuinely adverse party with a direct personal stake in the Court's ruling, but again, that would raise questions distinct from any implicated by the Advocate's role within the FISC itself. Given the profound Fourth Amendment implications of cases decided by the FISC, however, it may be desirable to consider mechanisms that might enable more frequent appellate review of FISC rulings by the Supreme Court, especially in light of that Court's ruling in

Amnesty v. Clapper, which would appear to effectively foreclose review even in cases where NSA programs entail ongoing Fourth Amendment searches affecting large numbers of American citizens whose identities are unlikely to ever be known.

October 31, 2013

The Honorable Patrick J. Leahy
Chairman, Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Michael S. Lee
Member, Committee on the Judiciary
United States Senate
316 Hart Senate Office Building
Washington, DC 20510

The Honorable John Conyers, Jr.
Ranking Member, Committee on the Judiciary
U.S. House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank James Sensenbrenner, Jr.
Member, Committee on the Judiciary
U.S. House of Representatives
2449 Rayburn House Office Building
Washington, DC 20510

Dear Messrs. Chairman, Ranking Members and Members:

As companies whose services are used by hundreds of millions of people around the world, we welcome the debate about how to protect both national security and privacy interests and we applaud the sponsors of the USA Freedom Act for making an important contribution to this discussion.

Recent disclosures regarding surveillance activity raise important concerns both in the United States and abroad. The volume and complexity of the information that has been disclosed in recent months has created significant confusion here and around the world, making it more difficult to identify appropriate policy prescriptions. Our companies have consistently made clear that we only respond to legal demands for customer and user information that are targeted and specific. Allowing companies to be transparent about the number and nature of requests will help the public better understand the facts about the government's authority to compel technology companies to disclose user data and how technology companies respond to the targeted legal demands we receive. Transparency in this regard will also help to counter erroneous reports that we permit intelligence agencies "direct access" to our companies' servers or that we are participants in a bulk Internet records collection program.

Transparency is a critical first step to an informed public debate, but it is clear that more needs to be done. Our companies believe that government surveillance practices should also be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs.

We also continue to encourage the Administration to increase its transparency efforts and allow us to release more information about the number and types of requests that we receive, so that the public debate on these issues can be informed by facts about how these programs operate. We urge the Administration to work with Congress in addressing these critical reforms that would provide much needed transparency and help rebuild the trust of Internet users around the world.

We look forward to working with you, the co-sponsors of your bills, and other members on legislation that takes into account the need of governments to keep individuals around the world safe as well as the legitimate privacy interests of our users around the world.

Sincerely,

Majority Leader Harry Reid
Minority Leader Mitch McConnell
United States Senate

Chairman Patrick Leahy
Ranking Member Charles Grassley
Committee on the Judiciary
United States Senate

Chairman Diane Feinstein
Vice Chairman Saxby Chambliss
Senate Permanent Select Committee on Intelligence
United States Senate

Speaker John Boehner
Minority Leader Nancy Pelosi
United States House of Representatives

Chairman Bob Goodlatte
Ranking Member John Conyers, Jr.
Committee on the Judiciary
United States House of Representatives

Chairman Mike Rogers
Ranking Member Dutch Ruppersberger
House Permanent Select Committee on Intelligence
United States House of Representatives

November 21, 2013

We the undersigned civil society groups, trade associations, companies and investors are supporters of the free and open Internet. We are writing to urge that intelligence surveillance practices be reformed by limiting the scope of surveillance and by substantially enhancing the privacy protections, oversight, and accountability mechanisms that govern that surveillance.

Recent disclosures regarding intelligence surveillance activity raise important concerns about the privacy and security of communications. This surveillance has already eroded trust that is essential to the free flow of information and to the exercise of human rights and civil liberties both in the United States and around the world.

To rebuild trust, we urge that the U.S. government act expeditiously to:

- allow companies to be much more transparent about the number and type of surveillance demands they receive;
- be much more transparent itself about the surveillance demands it makes, the surveillance activities in which it engages, and the legal bases for both;
- focus intelligence collection on terrorists, spies and other agents of foreign powers, rather than on everyone else; and
- ensure that its surveillance practices honor both Constitutional and human rights.

Toward this end, we welcome introduction in the House and Senate of the USA FREEDOM Act – legislation which promotes these goals. We oppose legislation that codifies sweeping bulk collection activities. We look forward to working with you on the USA FREEDOM Act and other legislation designed to protect the privacy of Internet users while permitting appropriately targeted intelligence surveillance necessary to protect against terrorism.

Sincerely,

Nonprofit Organizations
Access
Advocacy for Principled Action in Government
AIDS Policy Project
American Association of Law Libraries
American Booksellers Foundation for Free Expression

Companies and Trade Organizations
Automattic Inc.
CloudFlare
Computer and Communications Industry Assoc.
CREDO Mobile
Data Foundry
DreamHost

Nonprofit Organizations
(cont'd)
American Library Association
American Civil Liberties Union
Arab American Institute
Association of Research Libraries
Center for Democracy and Technology
Center for Financial Privacy and Human Rights
Center for National Security Studies
Citizens for Responsibility and Ethics in Washington
Coalition Against Unsolicited E-mail
Competitive Enterprise Institute
The Constitution Project
Consumer Action
Council on American-Islamic Relations
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org
Electronic Frontier Foundation
First Amendment Coalition
Freedom House
Free Press Action Fund
Freedom of the Press Foundation
Freedom to Read Foundation
FreedomWorks
Foundation for Innovation and Internet Freedom
Global Network Initiative
Government Accountability Project
Human Rights Watch
Liberty Coalition
OpenTheGovernment.org
Open Technology Institute
National Association of Criminal Defense Lawyers
National Coalition Against Censorship
National Security Counselors
Public Knowledge
OpenMedia.org
Personal Democracy Media
Project on Government Oversight
Reporters Without Borders
Republican Liberty Caucus
Rutherford Institute
TechFreedom
Texas Liberty Foundation

Companies and Trade Organizations
World Press Freedom Committee
(cont'd)
Dropbox
DuckDuckGo
Evoca
Golden Frog
Hewlett-Packard Company
Internet Infrastructure Coalition
Meetup
Mozilla
NetChoice
NY Tech Meetup
Reddit
ServInt
Sonic.net
SpiderOak
Tumblr
Twilio

Investors
Domini Social Investments
New Atlantic Ventures

An open letter to Washington

Dear Mr. President and Members of Congress,

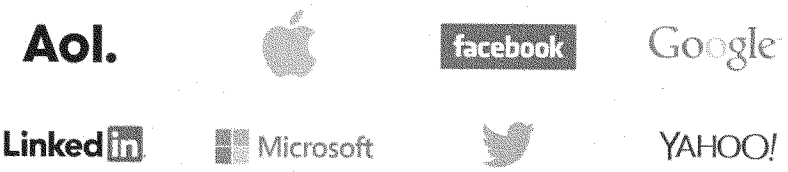
We understand that governments have a duty to protect their citizens. But this summer's revelations highlighted the urgent need to reform government surveillance practices worldwide. The balance in many countries has tipped too far in favor of the state and away from the rights of the individual — rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It's time for change.

For our part, we are focused on keeping users' data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks, and by pushing back on government requests to ensure that they are legal and reasonable in scope.

We urge the US to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight. To see the full set of principles we support, visit ReformGovernmentSurveillance.com

Sincerely,

AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo



Surveillance Reform Principles

1. **Limiting Governments' Authority to Collect Users' Information**

Governments should codify sensible limitations on their ability to compel service providers to disclose user data that balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the Internet. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications.

2. **Oversight and Accountability**

Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.

3. **Transparency About Government Demands**

Transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly.

4. **Respecting the Free Flow of Information**

The ability of data to flow or be accessed across borders is essential to a robust 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country. Governments should not require service providers to locate infrastructure within a country's borders or operate locally.

5. **Avoiding Conflicts Among Governments**

In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty — or "MLAT" — processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.

○