



OCTOBER 29, 2013

POTENTIAL CHANGES TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED THIRTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

Opening Statement

Mr. Mike Rogers [\[view PDF\]](#)

Chairman, House Permanent Select Committee on Intelligence

Mr. C. A. Dutch Ruppertsberger [\[view PDF\]](#)

Ranking Member

Witness Testimony

Panel 1, [\[view Joint Statement for the Record\]](#)

Mr. James R. Clapper

Director of National Intelligence

General Keith B. Alexander

Director, National Security Agency; Chief, Central Security Service

Mr. James M. Cole

Deputy Attorney General, Department of Justice

Panel 2

Mr. Steven G. Bradbury [\[view PDF\]](#)

Partner, Dechert LLP

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*

Mr. Stewart A. Baker [\[view PDF\]](#)

Partner, Steptoe & Johnson LLP

Mr. Stephen I. Vladeck [\[view PDF\]](#)

Professor of Law and Associate Dean for Scholarship, American University
Washington College of Law

COMPILED FROM:

- <http://intelligence.house.gov/hearing/nsa-programs>

Permanent Select Committee on Intelligence

October 29, 2013

Committee Open Hearing Potential FISA Changes

HPSCI Chairman Mike Rogers Opening Remarks

The Committee will come to order.

I'd like to welcome our first panel today: Director of National Intelligence James Clapper, Deputy Attorney General James Cole, National Security Agency Director General Keith Alexander, and Deputy Director of the NSA Chris Inglis.

Following the first panel, we will move immediately into the second panel of non-government experts who are all very knowledgeable on FISA and privacy issues.

Today's hearing will provide an open forum to discuss potential amendments to the Foreign Intelligence Surveillance Act and possible changes to the way FISA applications are handled by the Department of Justice and the NSA. I hope that all of our witnesses will give clear answers about how proposals under consideration in Congress would affect the NSA's ability to stop terrorist attacks before they occur.

As a starting point, we first need to consider why America collects foreign intelligence. The United States began collecting

foreign intelligence even before we were a nation, when George Washington sent Nathan Hale covertly into New York to try to understand what British plans were during the Revolutionary War.

In 1929, the Secretary of State shut down the State Department's cryptanalytic office saying, "Gentlemen don't read each other's mail." The world was a dangerous place back then, with growing and aggressive military threats from Japan and Germany, both bent on world domination. Those threats eventually dragged us into a world war that killed millions. We didn't have the luxury of turning off intelligence capabilities as threats were growing back then, and we can't afford to do so today.

Today, we gather foreign intelligence to help understand the plans and intentions of our adversaries, such as North Korea and Iran. We collect foreign intelligence to learn about terrorist plots before they happen, as well as to learn about rogue nations developing the most dangerous weapons.

Every nation collects foreign intelligence. That is not unique to the United States. What is unique to the United States is our level of oversight, our commitment to privacy protections, and our checks and balances on intelligence collection. China does not ask a FISA court for a warrant to listen to a phone call on their state-owned and censored network. The Russian Duma

does not conduct oversight on the FSB. But America has those checks; America has those balances. That is why we should be proud of the manner in which America collects intelligence.

The world is more connected today than ever before. This allows terrorists and spies to hide in civilian populations all over the world. They use the Internet and telephone networks of our enemies and our allies. They are just as likely to be found in terrorist safe havens as in allied nations overseas.

We cannot protect only our homeland. Americans live all over the world and our businesses set up shop all over the world. We have embassies in more than 150 countries; we have military bases in dozens of countries to protect our interests and allies; we bring stability to chaotic areas; and we help secure the global economy. That is why collecting foreign intelligence is so important.

In July during floor debate, I committed to working with other Members to bring increased transparency and additional privacy protections to NSA's counterterrorism programs.

Our challenge is to build confidence and transparency while keeping our intelligence services agile and effective against our adversaries.

One change we are considering would require the Attorney General or his designee to make the reasonable, articulable

suspicion (or “RAS”) determination that a particular phone number is related to a terrorist and may be used to search the bulk telephone records data. This process would move the RAS determination outside of the NSA, and is similar to the way an FBI investigator works with an Assistant United States Attorney when trying to find the person responsible for a crime.

We are also looking at providing more transparency into FISA Court orders whenever possible. Reforms to the statute could include requiring more court orders to be declassified or publicly released in redacted form.

Additional transparency into the process may also be helpful. For example, we could put into statute the process and standards for how information incidentally collected about U.S. persons who are not the targets of our programs is handled and require more public reporting on the number of times that happens.

The recent debate over NSA programs often misses the fact that the 215 and 702 collection programs are conducted wholly within the bounds of the law and are approved by the FISA Court. More transparency can help share that outstanding track record with the American people.

Some proposals pending before Congress, however, would effectively gut the operational usefulness of programs that are necessary to protect America’s national security.

For example, ending bulk collection under the business records provision would take away a vital tool for the FBI to find connections between terrorists operating in the United States. We can't ask the FBI to find terrorists plotting an attack and then not provide them with the information they need. If we didn't have the bulk phone records collection back in 2009, we may not have known there was a plot to attack the New York Subway system until bombs went off on the subway platforms.

In the words of the 9/11 Commission Report, before 2001, narrow-minded legal interpretations "blocked the arteries of information sharing" between the intelligence community and law enforcement. We cannot go back to a pre-9/11 mindset and risk failing to "connect the dots" again.

I look forward to having a frank discussion about your perspectives on potential changes to FISA and how those changes could impact our ability to disrupt terrorist plots before they happen.

Before turning the floor over to our witnesses, I recognize the Ranking Member for any opening comments he would like to make.

###



**Embargoed Until Delivered
October 29, 2013**

**Contact: Allison Getty
allison.getty@mail.house.gov
202-225-7690**

**Opening Statement:
Open Hearing on NSA Programs and FISA Reform
Ranking Member C.A. Dutch Ruppersberger
October 29, 2013**

Thank you, Mr. Chairman, and thank you to our witnesses:

- General Keith Alexander, Director of the National Security Agency;
- James Clapper, Director of National Intelligence;
- Chris Inglis, Deputy Director of NSA; and
- James Cole, Deputy Attorney General, Department of Justice.

I also want to thank the people of the Intelligence Community who work day and night to protect the security of our nation.

With all the criticism leveled at these programs, it is important that we not forget that these men and women are doing what we have told them to do, within the confines of the laws we've passed, and doing so to keep us safe.

The most important thing we can do here today is let the public know the true facts so that we can engage in a meaningful process of reform that will enhance transparency and privacy, while maintaining the necessary capabilities.

There's been a lot in the media about this situation -- some right, some wrong. Much has been mischaracterized, which is not helpful for those of us who are serious about both privacy and national security.

After these leaks came out, Chairman Rogers and I and other Members of Congress urged the Intelligence Community to release more information to help the public understand, which they've done.

Today, we are holding this open hearing so we can continue to get out the facts, and so that the American people can hear directly from the Intelligence Community-- and outside legal experts.

One key fact we need to keep in mind is that NSA's focus is on *foreign* threats. Under FISA, NSA does not target Americans in the U.S. and does not target Americans *anywhere* else, without a court order.

There are two FISA authorities that have been highlighted in the press.

First, the business records provision, known as Section 215, which allows the government to legally collect what is called metadata—a phone number, a length of call, NOT content. No names, no conversations, no content.

Let me be clear again: Under 215, the NSA cannot listen to anyone's phone calls.

What Section 215 does allow is the Government to connect the dots. These dots should have—and likely could have been—connected to prevent 9/11, and are necessary to prevent the next attack.

With this tool, we could have determined that one of the 9/11 hijackers was in San Diego and made a call to a known Al Qaeda number in Yemen. I shudder to think what connections will be missed if the program were to be completely eliminated.

Keep in mind, law enforcement obtains and analyzes these types of records every day to stop organized crime and to keep drugs out of the country. We don't want to make it easier to be a terrorist than a criminal in our country.

The second authority is known as Section 702 of the FISA Amendments Act. It allows the Government to collect the content of email and phone calls of foreigners-- not Americans-- who are located outside the United States.

This authority allows the government to get information about terrorists, cyber threats, and clandestine activities.

But again, this authority prohibits the targeting of American citizens or U.S. permanent residents without a court order, no matter where they are located. Both of these authorities are legal. Congress approved and reauthorized both of them over the last two years, and no court has ever struck them down.

The NSA is also subject to layered and constant oversight from the Executive, Judicial and Legislative branches of government. But let me be clear: more needs to be done. The Foreign Intelligence Surveillance Act must be reformed.

We have worked with the Administration, the Senate, telecommunication companies, and other stakeholders, to evaluate and vet a range of options. We must improve transparency, privacy protections and thereby restore the public's confidence:

You cannot truly have privacy without security, or security without privacy.

So, we are exploring a proposal to require a declassification review of any FISA Court decision, order or opinion, to improve transparency without threatening sources and methods.

We are also evaluating expanding Congressional reporting so that all Members of Congress, not just those on Committees of jurisdiction, can view the *classified* reporting about the programs.

We are vetting a measure that would create a presidentially appointed, Senate confirmed Inspector General of the NSA to provide an extra, independent check.

We are discussing ways to change the makeup of the FISA Court to correct the perception that it is controlled by one political party or the other.

We are looking into creating a privacy advocate, a non-Executive branch lawyer who would take an independent position on matters before the FISA Court that involve significant constructions or interpretations of FISA.

And the most intriguing, but also the most operationally challenging, is changing how section 215 is implemented. Can we move away from bulk collection and towards a system like the one used in the criminal prosecution system, in which the Government subpoenas individual call data records - phone numbers, no content - to be used for link analysis?

We've spent months working very hard on these proposals, and we would like to hear your thoughts on them.

We brought you here today to get your input in an open forum and allow all Members and the American people to hear your responses for themselves.

I thank you for your time today and look forward to a thoughtful discussion on the range of reform proposals out there.

Mr. Chairman, I yield back.

###



**JOINT STATEMENT FOR THE RECORD
OF**

**JAMES R. CLAPPER
DIRECTOR OF NATIONAL INTELLIGENCE**

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

**JAMES M. COLE
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE**

**BEFORE THE
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

OCTOBER 29, 2013

**Joint Statement for the Record
of**

**James R. Clapper
Director of National Intelligence**

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

**James M. Cole
Deputy Attorney General
Department of Justice**

**Before the
House Permanent Select Committee on Intelligence**

October 29, 2013

Thank you for inviting us to discuss the Administration's 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. We remain committed, as we review these activities, both to ensuring that we have the authorities we need to collect important foreign intelligence to protect the country from terrorism and other threats to national security, and to protecting privacy and civil liberties in a manner consistent with our values. We also remain

committed to working closely with this Committee as any modifications to these activities are considered. We understand that some of the initiatives announced by the President in his statement on August 9 are of interest to the Committee, and we welcome the opportunity to discuss them with you and to work together in moving forward.

The first step in promoting greater public confidence in these intelligence activities is to provide greater transparency so that the American people 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 have worked to provide the public greater insight into the operation of the bulk telephony metadata business records collection program under section 215. In early June, the Director of National Intelligence (DNI) released a public statement explaining that the program is carried out only pursuant to orders of the Foreign Intelligence Surveillance Court (FISC) and is subject to executive, judicial, and Congressional oversight. The DNI emphasized that, under this program, we do not collect the content of any telephone calls or any information identifying the callers, nor do we collect cell phone locational information. Rather, the Government obtains business records created and retained by telecommunication companies for their own internal purposes, such as billing. The DNI also explained that the Government is authorized to query the bulk metadata only when there is a reasonable, articulable suspicion, based on specific facts,

that the identifier—e.g., a telephone number—used to query the data is associated with a foreign terrorist organization previously approved by the FISC. Subsequently, the DNI declassified and released the FISC’s primary order that accompanied the secondary order that had been disclosed in the media, so that the American people could have a more complete picture of the legal parameters under which this activity occurs and the extensive oversight that the FISC requires. The primary order confirms that the Government must adhere to strict limitations on querying, retaining, and disseminating the business records acquired through this program. The Director of NSA also released information concerning the value of the bulk telephony metadata collection program in support of a number of counterterrorism investigations.

In August, the Administration published an extensive white paper to provide more detailed information concerning the section 215 business records program and its legal basis. The white paper explained the process and importance of “contact chaining” under which the NSA may obtain metadata records as many as three “hops” from an identifier associated with a foreign terrorist organization that is used to query the data. It also explained why the telephony metadata collection program meets the “relevance” standard of section 215 and why the program is fully consistent with settled Fourth Amendment law, including the Supreme Court’s precedent holding that participants in telephone calls lack a reasonable expectation of privacy in the telephone numbers dialed. Then, in early September the DNI declassified and released more documents concerning the business records program. These documents discuss compliance incidents that were discovered by NSA and DOJ four years ago, reported to the FISC and to the intelligence and judiciary committees, and subsequently resolved. These materials (and others) show that the oversight system worked. The problems were reported to the FISC, the FISC

conducted a rigorous review to ensure compliance with its orders and the protection of Americans' privacy, and the Intelligence Community responded effectively.

We have also substantially increased the transparency of the Government's collection under section 702 of FISA. Even before the recent unauthorized disclosures, the Administration had prepared a public white paper in conjunction with reauthorization of the FISA Amendments Act (FAA) at the end of last year, explaining its intelligence collection activities under the FAA and focusing in particular on collection under section 702. That paper emphasized that section 702 collection targets only non-U.S. persons overseas, and that targeting and minimization procedures and acquisition guidelines are required to ensure that the statutory restrictions are followed and to govern the handling of any U.S. person information that may be incidentally acquired. After the unauthorized disclosures concerning section 702 collection, the DNI refuted much of the inaccurate reporting about the program by releasing a public statement making clear that the Government does not have access to communications carried by U.S. electronic communications service providers without appropriate legal authority. Under section 702 such companies are legally required to provide targeted information to the Government only in response to lawful Government directives, which are issued after the FISC examines and approves certifications required under section 702. The DNI's statement also explained that the Government cannot collect information under section 702 unless there is an appropriate and documented foreign intelligence purpose, such as preventing terrorism or weapons of mass destruction proliferation.

In August, the DNI declassified and released three opinions from the FISC concerning the section 702 program. As was the case with the section 215 opinions, these opinions

concerned a significant compliance incident that caused the Court to criticize the manner in which the section 702 program was being carried out. And, similarly, these opinions provide the public with considerable insight into the nature and functioning of section 702 collection, while also displaying the detailed and intricate extent of the FISC's review. Indeed, while the FISA statute describes the basic procedures by which the Intelligence Community seeks various authorizations from the FISC, the opinions released reveal fully the thorough, thoughtful, independent review that the FISC provides.

The Administration has taken other steps toward increasing transparency more generally in the context of intelligence collection. For example, the DNI recently introduced a new website called "IC on the Record," which provides ongoing, direct access to information about the foreign intelligence collection activities carried out by the Intelligence Community. Administration officials have also made a number of important public statements relating to the Government's foreign intelligence collection efforts, including a speech by the General Counsel of the Office of the Director of National Intelligence at the Brookings Institution. Moreover, the Government has permitted companies interested in providing greater transparency as to their role in these programs to release certain aggregate statistics about their cooperation with lawful demands from the Government, in a way that will avoid revealing the Government's intelligence collection capabilities with respect to particular providers or platforms. And of course there have been a number of open hearings before committees of the Congress on these issues.

Overall, this is a lot of activity for three months. As we have worked toward greater transparency, we have been mindful of the need to protect intelligence sources and methods. Unfortunately, because of the unauthorized disclosures, a great deal of information that was

previously classified about these intelligence programs is now in the public domain. These unauthorized disclosures have already caused significant harm to national security, and inaccurate or incomplete press coverage of the unauthorized disclosures has also undermined public confidence in our efforts to protect Americans' privacy. We have to consider these effects as we assess whether additional harm will flow from releasing additional information. There is still substantial information about these activities that can and must remain classified, and we have therefore taken great care to ensure that any documents that are considered for release are carefully reviewed and redacted as appropriate to protect national security. Ultimately, the Government must walk a fine line by disclosing enough information to assure the American public that the Government is acting lawfully but not disclosing so much information that we put the American public in danger.

To complement these transparency efforts, the Administration has taken a series of steps to enhance independent review of U.S. intelligence collection programs. In his August 9 statement, the President noted the importance of the Privacy and Civil Liberties Oversight Board's (PCLOB's) review. PCLOB's statutory mission is "to analyze and review actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties." PCLOB is taking an active role in reviewing the intelligence activities carried out under sections 215 and 702. The Board has received extensive briefings from Administration officials concerning these activities and visited the NSA. In July PCLOB sponsored a public workshop to hear from expert panels and the public.

In his speech in August, President Obama also announced the establishment of a Review Group on Intelligence and Communications Technologies. The Review Group's task is to advise the President "on how, in light of advancements in technology, the United States can employ its technical collection capabilities in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure." The group is charged with conducting an independent review and will report to the President. Group members have received briefings from Administration officials and have met with privacy and civil liberties experts, as well as information technology companies and experts. The group will also be soliciting public comments. The Review Group has been directed to submit an interim report to the President within 60 days and a final report by the end of the year.

Throughout this period, the FISC has continued to exercise its central oversight role with respect to intelligence collection carried out under FISA. In July, ODNI announced that the FISC had renewed its approval for the section 215 program. In connection with that renewal, the FISC has also publicly released an opinion explaining the legal rationale for its decision.

Moreover, as the President discussed in his August 9 statement, the executive branch stands ready to work with Congress to pursue appropriate reforms to section 215, to discuss certain changes to practice before the FISC to ensure that civil liberties concerns have an independent voice in appropriate cases, and to consider efforts at strengthening the transparency of these and other intelligence activities, all in ways consistent with protecting national security. Regarding section 215, we are open to a number of ideas that have been proposed in various

quarters to address concerns about the business records program. For example, 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 FISC orders permit. We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced 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 can 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 FISC reform, we believe that the *ex parte* nature of proceedings before the FISC 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 FISC 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 FISC could solicit independent views of an *amicus* in a subset of 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 FISC process.

And with regard to enhancing transparency and accountability, the President has directed that the Intelligence Community declassify and make public as much information as possible about certain sensitive intelligence collection programs, including programs undertaken pursuant to sections 215 and 702, while being mindful of the need to protect sensitive classified intelligence and national security. Consistent with that direction, the DNI has directed the Intelligence Community to release publicly, on an annual basis, aggregate information concerning compulsory legal processes under certain national security authorities. We stand ready to discuss whether legislation would be helpful in advancing the President's objective of ensuring greater transparency for the activities of the Intelligence Community, where consistent with the protection of classified information.

While it is important that we have the aforementioned dialogue about security and civil liberties, we'd also like to take a moment to reiterate some of the comments the President has made about the hard-working men and women of the intelligence community who work every single day to keep us safe because they love this country and believe in its values. These professionals are Americans, too—they come from the same communities, go to the same schools, and care about the same things all Americans do. While the ongoing debate is an important one, and may well result in changes, that dialogue should in no way be perceived as a negative reflection on the dedicated professionals of our Intelligence Community.

We look forward to working with you on these important issues, and we remain grateful for this Committee's support for these particular intelligence collection programs, which we

continue to believe play an important role in our broader foreign intelligence collection efforts.

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 enjoy broader public and Congressional support in the future. Thank you.

TESTIMONY OF STEVEN G. BRADBURY

Before the HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

Open Hearing on Legislative Proposals for Modifying NSA Programs and Amending FISA Authorities

October 29, 2013

Thank you, Chairman Rogers, Ranking Member Ruppertsberger, and distinguished Members of the Committee.

I'm honored to appear before the Committee today to discuss the foreign intelligence acquisition and surveillance authorities of the executive branch—with particular focus on the recently revealed programs of the National Security Agency (“NSA”)—and to offer views on several proposals currently under consideration in Congress for modifying or curtailing the NSA’s programs and for amending key provisions of the Foreign Intelligence Surveillance Act, or “FISA.”¹

Summary

Any debate over proposals to restrict the NSA activities revealed by the Snowden leaks or to make significant amendments to FISA in response to those leaks should carefully consider whether the foreign intelligence programs that would be affected by the proposals are lawful and whether they continue to be necessary.

If the NSA programs are lawful and if, in the estimation of this Committee, they remain necessary to protect the Nation from foreign threats, then Congress should be very wary indeed about approving any legislative changes that might undermine the effectiveness of the programs or that might diminish the ample

¹ The author is an attorney in Washington, D.C., and the former head of the Office of Legal Counsel in the U.S. Department of Justice from 2005 to 2009, where he advised the executive branch on legal matters relating to national security, including surveillance authorities under FISA. The views presented are solely the personal views of the author and do not represent the views of his law firm or of any current or former client.

existing security measures, privacy protections, and oversight protocols under which they operate.

Based on that premise, I wish to emphasize the following three points:

First, there is no serious argument that the NSA programs as currently configured violate any applicable statutory or constitutional restrictions.

The independent federal judges who sit on the FISA court have repeatedly scrutinized these programs over the past several years and ensured that they comply in all respects with the requirements of FISA and are fully consistent with the Fourth and First Amendments of the Constitution. A review of the FISA court opinions recently declassified and released to the public amply demonstrates that the FISA court is no rubber stamp for the surveillance policies of the executive branch.

The judges of the FISA court, as well as the attorneys of the National Security Division of the Justice Department, the Inspectors General of the Intelligence Community and the Justice Department, and the diligent oversight of the Intelligence Committees of Congress, have held the NSA to the highest standards possible in the operations of these programs, including by ordering the prompt correction of significant compliance issues identified to the court by the Agency and its overseers.

The FISA court's decisions confirm that both the bulk telephone metadata acquisition and focused analysis currently occurring under the business records provision of FISA (commonly known as section 215 of the PATRIOT Act) and the broad foreign-targeted surveillance of international communications conducted under section 702 of FISA comply in all respects with the Constitution and the terms of the relevant statutes and are consistent with the intent of Congress.

Indeed, I understand that all Members of Congress, specifically including the Judiciary Committees, were informed about the details of these two NSA programs or were at least given the opportunity to receive such briefings in connection with the reauthorizations of sections 215 and 702. The large majorities of both Houses that voted to reauthorize these statutes in 2011 and 2012 therefore represented, at least constructively, a clear approval and ratification of the legal

interpretations supporting the NSA's collection and surveillance activities, including the bulk acquisition of telephone metadata. Any claim in recent months of lack of prior awareness and understanding of these programs in reaction to the public controversy generated by the Snowden leaks should be taken with a truckload of salt.

Second, I accept the judgment of the President, the Director of National Intelligence ("DNI"), and Gen. Alexander, the Director of the NSA, that the NSA programs revealed by Snowden are critically important to preserving the security of the United States and its allies and that these programs continue to make an essential contribution to our counterterrorism defenses. From everything I know, these programs are, as they were designed to be, among the most effective tools for detecting and identifying connections between foreign terrorist organizations and active cells within the United States and for discovering new leads, including new phone numbers, in furtherance of counterterrorism investigations.

If that's true, it is, of course, primarily the duty of the President to stand up and defend the programs before the American people and Congress. But as an important supplement to presidential leadership, or in the absence of such leadership, it is incumbent on this Committee and the Intelligence Committee of the Senate to validate the necessity and effectiveness of these programs and to educate and persuade a majority of colleagues in both Houses of the need to support and preserve these essential foreign intelligence capabilities in the face of popular reaction. The national interest must trump narrow political interests.

Third, it is my conviction that all of the major proposals under consideration in Congress for curtailing, restricting, or modifying the NSA programs (most especially the section 215 telephone metadata program) and for reforming the scope and use of FISA authorities in reaction to the Snowden leaks should be rejected.

As discussed in more detail below, certain proposals would expose the Nation to vulnerability by substantially weakening or even destroying outright the effectiveness of the 215 program. Other proposals would significantly diminish the ability of the government to ensure the security and oversight of the program. Still others would unnecessarily hamper foreign intelligence efforts by adding layers of lawyering or litigation-like process that would not actually achieve

greater civil liberties protections for the public but that would, I fear, prove dangerously unworkable in the event of the next catastrophic attack on the United States.

I therefore strongly urge the Committee to avoid endorsing proposals for substantial modification of the NSA programs or FISA provisions. If reforms are adopted that would severely constrain the effectiveness and utility of the NSA programs, then Edward Snowden and his collaborators will have achieved their explicit objective of weakening the national security defenses and capabilities of the United States and diminishing the position of strength that America occupies in the world post-9/11.

The NSA Programs Satisfy All Statutory and Constitutional Requirements

I have previously explained in detail why both the section 215 bulk acquisition of telephone metadata and the section 702 foreign-targeted surveillance of international communications are authorized by statute, consistent with the Constitution and congressional intent, and appropriately protective of privacy and civil liberties.² I will not repeat the full analysis here, but I do offer the following brief summary.

Section 215 Telephone Metadata Program.

The telephone metadata acquired by the NSA under the section 215 business records order consists only of tables of numbers indicating which phone numbers called which numbers and the time and duration of the calls. It does not reveal any other subscriber information, and it does not enable the government to listen to anyone's phone calls.

The Fourth Amendment does not require a search warrant or other individualized court order for the government to acquire this type of purely transactional metadata, as distinct from the content of communications. The acquisition of such call-detail information, either in bulk or for the

² See Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata under Section 215 and Foreign-Targeted Collection under Section 702*, 1 *Lawfare Res. Paper Series No. 3* (Sept. 2013), available at <http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf>.

communications of identified individuals, does not constitute a “search” for Fourth Amendment purposes with respect to the individuals whose calls are detailed in the records. The information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore consistently held that there is no reasonable expectation by the individuals making the calls that this information will remain private. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).³

The force of this conclusion is not diminished by the large size of the data set being acquired by the NSA. Indeed, the individual privacy interests of the tens of millions of telephone customers whose calling records are collected by the NSA are lessened even further because of the vastness and anonymity of the data set.

This acquisition is authorized under the terms of section 215, which permits the acquisition of business records that are “relevant to an authorized investigation.” Here, the telephone metadata is “relevant” to counterterrorism investigations because the use of the database is essential to conduct a link analysis of terrorist phone numbers, and this type of analysis is a critical building block in these investigations. Acquiring a comprehensive database is needed to enable effective analysis of the telephone links and calling patterns of terrorist suspects, which is often the only way to discover new phone numbers being used by terrorists. To “connect the dots” effectively requires the broadest set of telephone metadata.

The legal standard of relevance incorporated into section 215 is the same common standard that courts have long held governs the enforcement of administrative subpoenas, grand jury subpoenas, and document production orders in civil litigation, which, unlike section 215 business records orders, do not require the advance approval of a court.⁴

³ *Accord Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-05 (9th Cir. 2008) (same analysis for email addressing information).

⁴ *See* 152 Cong. Rec. 2426 (2006) (Statement of Sen. Kyl) (explaining the “relevant to” language added to section 215 in 2006) (“Relevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders.”).

The Supreme Court has long held that courts must enforce administrative subpoenas so long as the agency can show that the subpoena was issued for a lawfully authorized purpose and seeks information relevant to the agency's inquiry.⁵ This standard of relevance is exceedingly broad; it permits agencies to obtain "access to virtually any material that might cast light on" the matters under inquiry,⁶ and to subpoena records "of even *potential* relevance to an ongoing investigation."⁷ Grand jury subpoenas are given equally broad scope and may only be quashed where "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."⁸ And in civil discovery, the concept of relevance is applied "broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case."⁹

The relevance standard does not require a separate showing that every individual record in a subpoenaed database is "relevant" to the investigation.¹⁰ The standard is satisfied if there is good reason to believe that the database contains information pertinent to the investigation and if, as here, the acquisition of the database is needed to preserve the data and to be able to conduct focused queries to find particular records useful to the investigation.¹¹

⁵ See *United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 313 (1978); *United States v. Powell*, 379 U.S. 48, 57 (1964); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946).

⁶ *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984).

⁷ *United States v. Arthur Young & Co.*, 465 U.S. 805, 814 (1984) (emphasis in original).

⁸ *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

⁹ *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978).

¹⁰ See *In re Grand Jury Proceedings*, 616 F.3d 1186, 1202, 1205 (10th Cir. 2010) (confirming (1) that the categorical approach to relevance for grand jury subpoenas "contemplates that the district court will assess relevancy based on the broad types of material sought" and will not "engag[e] in a document-by-document" or "line-by-line assessment of relevancy," and (2) that "[i]ncidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury's broad investigative powers and the categorical approach to relevancy").

¹¹ See, e.g., *In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000); *FTC v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987); *Associated Container Transp. (Aus.) Ltd. v. United States*, 705 F.2d 53, 58 (2d Cir. 1983). The same approach is sanctioned in the federal rules governing criminal search warrants. See Fed. R. Crim. P. 41(e)(2)(B) ("A warrant . . . may authorize the

The effective analysis of terrorist calling connections and the discovery through that analysis of new phone numbers being used by terrorist suspects require the NSA to assemble and maintain the most comprehensive set of telephone metadata, and the section 215 order provides that unique capability.

While the metadata order is extraordinary in the amount of data acquired, it's also extraordinarily narrow and focused because of the strict limitations placed on accessing the data. There's no data mining or trolling through the database looking for suspicious patterns. By court order, the data can only be accessed when the government has reasonable suspicion that a particular phone number is associated with a foreign terrorist organization, and then that number is tested against the database to discover its connections. If it appears to be a U.S. number, the necessary suspicion cannot be based solely on First Amendment-protected activity.

Because of this limited focus, only a tiny fraction of the total data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers. Any data records older than five years are continually deleted from the system.

The order must be reviewed and reapproved every 90 days, and since 2006, this metadata order has been approved at least 35 times by at least 15 different federal judges.

In addition to court approval, the 215 program is also subject to oversight by the executive branch and Congress. FISA mandates periodic audits by inspectors general and reporting to the Intelligence and Judiciary Committees of Congress. When section 215 was reauthorized in 2011, the administration briefed the leaders of Congress and the members of these Committees on the details of this program. The administration also provided detailed written descriptions of the program to

seizure of electronic storage media or . . . information” subject to “a later review of the media or information consistent with the warrant”); *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006) (sanctioning “blanket seizure” of computer system based on showing of need); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (sanctioning “seizure and subsequent off-premises search” of computer database).

the chairs of the Intelligence Committees, and the administration requested that those descriptions be made available to all Members of Congress in connection with the renewal of section 215.

These briefing documents specifically included the disclosure that under this program, the NSA acquires the call-detail metadata for “substantially all of the telephone calls handled by the [phone] companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.”¹² Public reports indicate that the Intelligence Committees provided briefings on the details of the program to all interested Members of Congress, and the administration has conducted further detailed briefings on this program since the Snowden leaks became public.

Section 702 Collection.

The second NSA program revealed by the Snowden leaks—the foreign-targeted surveillance of international communications—is conducted under section 702 of FISA.

With court approval, section 702 authorizes a program of foreign-focused surveillance for periods of one year at a time. This authority may only be used if the surveillance does *not* (1) intentionally target any person, of any nationality, known to be located in the United States, (2) target a person outside the U.S. if the purpose is to reverse target any particular person believed to be in the U.S., (3) intentionally target a U.S. person anywhere in the world, and (4) intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S.

Section 702 mandates court approval of the targeting protocols and of minimization procedures to ensure that any information about U.S. persons that may be captured in this surveillance will not be retained or disseminated except as necessary for foreign intelligence purposes.

¹² Report on the National Security Agency’s Bulk Collection Programs for USA PATRIOT Act Reauthorization at 3, *enclosed with* Letters for Chairmen of House and Senate Intelligence Committees from Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, Department of Justice (Feb. 2, 2011). The identical disclosure was also made in a similar report enclosed with letters dated December 14, 2009.

From everything that's been disclosed about the foreign-targeted surveillance program, including the so-called PRISM Internet collection, it appears to be precisely what section 702 was designed to permit.

The 702 program is also fully consistent with the Constitution. As a background principle, the Fourth Amendment does not require the government to obtain a court-approved warrant supported by probable cause before conducting foreign intelligence surveillance. The Supreme Court has reserved judgment on the question,¹³ but the courts of appeals have consistently held that the President has inherent constitutional authority to conduct warrantless searches and surveillance to obtain intelligence information about the activities of foreign powers, both inside and outside the United States and both in wartime and peacetime.¹⁴

The absence of a warrant requirement does not mean the Fourth Amendment has no application to foreign intelligence surveillance. Rather, searches and surveillance conducted in the United States by the executive branch for foreign intelligence purposes are subject to the general reasonableness standard of the Fourth Amendment. See *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995) (holding that the touchstone for government compliance with the Fourth Amendment is whether the search is “reasonable” and recognizing that the warrant requirement is inapplicable in situations involving “special needs” that go beyond routine law enforcement).

¹³ See *United States v. United States District Court* (the “Keith” case), 407 U.S. 297, 308 (1972) (explaining that the Court did not have occasion to judge “the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country”); *Katz v. United States*, 389 U.S. 347 (1967).

¹⁴ See, e.g., *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 914-15 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir.), *cert. denied sub nom. Ivanov v. United States*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir.1973), *cert. denied*, 415 U.S. 960 (1974). *But see Zweibon v. Mitchell*, 516 F.2d 594, 619-20 (D.C.Cir.1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation), *cert. denied*, 425 U.S. 944 (1976).

The reasonableness of foreign intelligence surveillance, like other “special needs” searches, is judged under a general balancing standard “by assessing, on the one hand, the degree to which [the search] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). In the context of authorized NSA surveillance directed at protecting against foreign threats to the United States, the governmental interest is of the highest order. *See Haig v. Agee*, 453 U.S. 280, 307 (1981) (“It is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.”).

On that basis, prior to 1978, Presidents conducted surveillance of national security threats without court supervision. That practice led to the abuses that were documented by the Church and Pike Committees and eventually resulted in the passage of FISA.

FISA was enacted as an accommodation between Congress and the executive branch. It was designed to ensure the reasonableness of surveillance by requiring the approval of a federal judge for certain defined types of clandestine foreign intelligence surveillance conducted in the United States, instituting oversight of the process by the Intelligence Committees of Congress, providing for procedures to “minimize” the retention and dissemination of information about U.S. persons collected as part of foreign intelligence investigations, and regularizing procedures for the use of evidence obtained in such investigations in criminal proceedings.

Under FISA, electronic surveillance of persons in the United States for foreign intelligence purposes requires an order approved by a judge and supported by individualized probable cause to believe the target is an agent of a foreign power or engaged in international terrorism.

Ever since FISA was enacted, it’s been recognized that FISA raises significant constitutional issues to the extent it might impinge on the President’s ability to carry out his constitutional duty to protect the United States from foreign attack.

Importantly, in its original conception, FISA was not intended to govern the conduct of communications intelligence anywhere overseas or the NSA's collection and surveillance of international communications into and out of the United States. FISA's definition of "electronic surveillance" focuses on the interception of wire communications on facilities in the United States and on the interception of certain categories of domestic radio communications. *See* 50 U.S.C. § 1801(f). In 1978, most international calls were carried by satellite, and thus the statute's definition of "electronic surveillance" was carefully designed at the time to exclude from the jurisdiction of the FISA court not only all surveillance conducted outside the United States, but also the surveillance of nearly all international communications.¹⁵

FISA also exempted from statutory regulation the acquisition of intelligence information from "international or foreign communications" not involving "electronic surveillance" as defined in FISA,¹⁶ and this change, too, was "designed to make clear that the legislation does not deal with the international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."¹⁷ Congress specifically understood that the NSA surveillance that these carve-outs would categorically exclude from FISA included the monitoring of international communications into and out of the United States of U.S. citizens.¹⁸

In the years following the passage of FISA, however, communications technologies evolved in ways that Congress had not anticipated. International lines of communications that once were transmitted largely by satellite migrated to undersea fiber optic cables. This evolution increased greatly with the advent of the Internet. In the new world of packet-switched Internet communications and

¹⁵ *See* S. Rep. No. 95-604, at 33-34, reprinted in 1978 U.S.C.C.A.N. 3904, 3934-36.

¹⁶ *See* Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), *codified at* 18 U.S.C. § 2511(2)(f) (1982).

¹⁷ S. Rep. No. 95-604, at 64, 1978 U.S.C.C.A.N. at 3965.

¹⁸ *See id.* at 64 n.63 (describing the excluded NSA activities by reference to a Church Committee report, S. Rep. No. 94-755, at Book II, 308 (1976), which stated: "[T]he NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans . . .").

international fiber optic cables, FISA's original regime of individualized court orders for foreign intelligence surveillance conducted on facilities in the United States became cumbersome, because it now required case-by-case court approvals for the surveillance of international communications that were previously exempt from FISA coverage. Nevertheless, prior to 9/11, the executive branch found the FISA system to be adequate and workable for most national security purposes.

All of that changed with the attacks of 9/11. In the estimation of the President and the NSA, the imperative of conducting fast, flexible, and broad-scale signals intelligence of international communications in order to detect and prevent further terrorist attacks on the U.S. homeland proved to be incompatible with the traditional FISA procedures for individualized court orders and the cumbersome approval process then in place. As the Justice Department later explained in a public white paper addressing the legal basis for the NSA's warrantless surveillance of international communications involving suspected terrorists that was authorized by special order of the President following 9/11, "[t]he President ha[d] determined that the speed and agility required to carry out the[se] NSA activities successfully could not have been achieved under FISA."¹⁹

The public disclosures in 2005 and 2006 concerning the President's authorization of warrantless surveillance by the NSA precipitated extensive debates and hearings in Congress. Ultimately, these debates culminated in passage of the FISA Amendments Act of 2008 and the addition of section 702 to FISA. Section 702 was designed to return to a model of foreign surveillance regulation similar to the original conception of FISA by greatly streamlining the court review and approval of a program of surveillance of international communications targeted at foreign persons believed to be outside the United States. Under section 702, such foreign-targeted surveillance may be authorized by the Attorney General and DNI without individualized court orders for periods of up to one year at a time upon the approval by the FISA court of the required targeting protocols and minimization procedures. *See* 50 U.S.C. § 1881a.

By establishing procedures for court approval (albeit more streamlined and "programmatic" approval than required for traditional individualized FISA surveillance orders) and by strengthening congressional oversight of the resulting

¹⁹ U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 34 (Jan. 19, 2006).

program, section 702 continues to provide a system of foreign intelligence surveillance, including for international communications and surveillance targeted at foreign persons outside the U.S., that is more restrictive and protective than the Constitution would otherwise require.

As publicly described, the NSA's section 702 program of foreign-targeted Internet surveillance easily meets the reasonableness requirements of the Fourth Amendment. The surveillance is conducted for foreign intelligence purposes, which carry great weight in the Fourth Amendment balance, and the retention and use of information collected in the program about U.S. persons are subject to extensive and detailed minimization procedures designed to protect the reasonable privacy interests of Americans, and these minimization procedures have been reviewed and approved by a federal court.

There Is Every Reason to Believe that the NSA Programs Remain Necessary to Protect the National Security of the United States and Its Allies

As an institutional matter, this Committee and the Intelligence Committee of the Senate are in the best position to affirm for Members of Congress the ongoing importance and necessity of the NSA programs.

Both of the programs at issue are intended to provide quick and efficient detection and identification of contacts between known agents of foreign terrorist organizations and unknown operatives that may be hiding out within the United States. For my part, I believe that the need for such detection is just as acute today as it was in the immediate wake of 9/11.

More specifically with regard to the 215 order, from all that I know, I have every confidence that the bulk acquisition of the telephone metadata is necessary to preserve the data for use in the FBI's counterterrorism investigations and to combine the call-detail records generated by multiple telephone companies into a single searchable database. Furthermore, the use of the entire integrated database is essential to conduct focused link analysis and contact chaining of terrorist phone numbers and thereby discover new terrorist phone numbers that we did not know about before.

It is necessary to retain the data for a sufficient period, such as five years, to be able to conduct historical analysis to find connections between newly discovered phone numbers and the numbers of known terrorist agents that may have been the subjects of past investigations.

I believe that the 215 program provides a frequent and important input for ongoing investigations of terrorist activities. I don't believe the proper test of the program's necessity is whether it has provided the one primary piece of information required to thwart a specific terrorist plot just before an attack has been carried out. Any such narrow focus on the interdiction of particular mature plots is unrealistic because it does not take account of how these investigations are conducted and the fact that nearly all counterterrorism efforts involve numerous inputs from diverse sources over an extended period of time.

The Major Proposals for Curtailing or Modifying the NSA Programs and for Amending the FISA Authorities Should Be Rejected

I offer the following thoughts on why the principal legislative proposals for modifying the authorities of the NSA under FISA should not be approved.

The most sweeping change under consideration, as I understand it, would restrict the government's authority under section 215 to acquiring on an item-by-item basis only those individual business records, including telephone call-detail records, that directly pertain to the person who is the subject of the counterterrorism investigation. A variation on this proposal would limit the NSA to conducting one-by-one queries of the call-detail databases of the phone companies only while the data is retained by the companies in the ordinary course of business.

Such requirements would kill the NSA's telephone metadata program, because they would, by design, deny the NSA the broad field of data needed to conduct in an efficient and workable manner the link analysis and contact chaining that is enabled by the current program.

At the same time, denying the NSA the authority to acquire the metadata in bulk and to retain it for a period of years would preclude any historical analysis of connections between a terrorist phone number and other, yet undiscovered

numbers, and the ability to examine historical connections and patterns is among the most valuable capabilities of the 215 metadata program. Indeed, any proposal to limit the length of metadata retention to a period of less than the current five years should be approached with great care, because it would by definition diminish the capacity of the NSA to conduct this important historical contact analysis.

A less sweeping but still very significant restriction would prohibit the NSA from taking possession of the call-detail records obtained under the 215 order and would instead require that the data be maintained for an extended period under the control of the telephone companies, presumably at the expense of the federal government. The current program enables the NSA to acquire all of the telephone metadata on an ongoing basis from several companies in order to preserve the data in a segregated and secure manner and combine it together in a form that is efficiently usable and searchable. Ceding control of the combined database to the phone companies would presumably require the involvement of a private, third-party contractor to house and manage the data, since no single phone company has the ability to maintain and aggregate all of the data of the several companies and host the data on servers for a sufficient period of years in a searchable form.

Any such arrangement involving a third-party contractor, however, would be distinctly less efficient, less secure, and less subject to effective oversight by the executive branch, the FISA court, and Congress than the current program. That result cannot be a desirable one, both in terms of national security and in terms of the privacy of the data and the potential for its abuse.

Another proposal would require FISA court approval in advance of each query of the telephone metadata—in other words, a one-by-one court determination that there is reasonable articulable suspicion that the phone number to be queried against the database is associated with one of the specified foreign terrorist organizations. Such a requirement would place a significant restraint on the speed and flexibility of the program, and, if applied to second and third “hops” from the original seed number, would throttle the utility of the program entirely. Moreover, requiring court approval of each reasonable articulable suspicion determination would impose a legalistic judicial overlay on a judgment that is more appropriately made by seasoned intelligence analysts. The alternative proposal of requiring approval by the lawyers of the National Security Division of

the Justice Department would suffer from the same defect: It would interpose a lawyer's sensibility in place of the practical judgment of intelligence professionals.

One further proposal often raised is to attempt to graft onto the traditionally *ex parte* procedures of the FISA court a litigation-like adversary process—for example, by creating the position of a “Public Advocate” for the FISA court. Under certain of these proposals, the Public Advocate would be charged with representing the “public interest” or the “privacy interests” of the targets of the surveillance and would be expected to oppose the government's applications, at least in cases raising novel interpretations of FISA or asking to extend the law beyond how it has previously been applied. One such proposal would require that the Public Advocate receive a copy of each application for a FISA order and would give the Public Advocate the right to appeal any FISA order approved by the court.

This concept of introducing a Public Advocate into the FISA process raises constitutional concerns. Because the review of FISA applications requires access to the most sensitive national security information, any appointed advocate would have to be a permanent, trusted officer of the executive branch or of the FISA court with the necessary security clearances. Constitutional issues would arise in any mandate that the President invariably permit the Public Advocate to have access to the most sensitive classified information. Constitutional issues would also follow if the Public Advocate, an employee of the Judicial Branch, were given the power to appeal a decision of the FISA court over the objections of the executive branch. Among other things, the Public Advocate would lack the Article III standing necessary to initiate an appeal. If intended to act as an “independent” officer within the Judicial Branch, not simply an adviser to the judges but empowered to appeal rulings of the FISA court and granted the mandate to appear in court as an adversary to the executive branch, the Public Advocate would fall outside the three-branch framework established in the Constitution.

Moreover, if done in a constitutional form, introducing such an advocate position would not likely achieve the meaningful benefits that proponents hope for. The judges assigned to the FISA court are already assisted by permanent legal advisers who are steeped in the precedents of the court and whose job is to second-guess the arguments and analyses of the executive branch. If a particular FISA application raises significant questions, the legal advisers are already asked to prepare separate, in-depth analyses for the judges. The recently disclosed opinions

of the FISA court convincingly show that the judges of the court and their legal advisers are not shy about applying a thoroughly independent review of the issues that is in no way beholding to the executive branch. If a Public Advocate were part of the executive branch, the advocate would always ultimately be answerable to the President. If employed by the court, the advocate would be little different from the existing legal advisers. Either way, the Public Advocate could never actually be a true independent adversary representing the interests of those under surveillance.

One final observation that I believe is important to keep in mind: Many of the reform proposals discussed above, including those that would attempt to convert the FISA process into an adversary proceeding and those that would impose more frequent judicial approvals or bureaucratic processing of decisions heretofore made in real time by intelligence analysts, would run the risk of recreating the type of cumbersome, overlawyered foreign intelligence regime that proved so inadequate in the face of 9/11.

This Committee knows far better than I how likely it is (or rather how inevitable) that America will suffer another catastrophic terrorist attack at some point in the years ahead. In the event of such an attack, I fear that the constrained and lawyerly process for conducting signals intelligence required under the proposed reforms would prove inadequate, and the President, any President, would be forced once again to fall back on his Article II authority to conduct the effective surveillance he determines necessary to protect the country from follow-on attacks. Indeed, I believe the American people would demand no less.

That cannot be a result this Congress would prefer. But it is, unfortunately, a very real possibility if the proposals currently under consideration were to be adopted.

Testimony of Stewart A. Baker

Before the Permanent Select Committee on Intelligence United States House of Representatives

“Potential Amendments to the Foreign Intelligence Surveillance Act”

October 29, 2013

Chairman Rogers, Ranking Member Ruppertsberger, members of the committee, it is a great honor to testify before you today on the issues raised by the Snowden leaks. I was the General Counsel of the National Security Agency in the early 1990s, under both George H.W. Bush and Bill Clinton. I have closely followed NSA issues as a private lawyer, as general counsel of the Robb-Silberman Commission on intelligence failures involving Iraq and weapons of mass destruction, and as an author and blogger.

It seems to me that the issues raised by the Snowden disclosures fall into two categories. The first is a topic that has received less attention from Congress but one that poses the greatest threat to the country's security. That is the current campaign by Glenn Greenwald and others who control the Snowden documents to cause the greatest possible diplomatic damage to the United States and its intelligence capabilities.

I fear that this international campaign has forced the executive branch into a defensive crouch. Other nations are taking advantage of the moment to demand concessions that the White House is already halfway to granting. If so, we will regret them as a country long after the embarrassment of fielding angry phone calls from national leaders has faded into a short passage in President Obama's memoirs.

It is time for Congress to look more closely at the long-term security interests of the country and to set limits on the intelligence concessions that other nations demand and that the Executive can make. I will explain why in the first part of my testimony.

The second issue is more familiar. The domestic fallout from the Snowden leaks has been concentrated heavily on NSA's collection of telephone metadata under section 215 of the USA PATRIOT Act. A lot of changes have been proposed in response. Most of them are bad ideas.

But there are bad ideas and worse ones. In the second part of my testimony, I will explain why I think the NSA collection is justified and why the reaction is not. I'll then offer thoughts on which of the reform proposals will do the least harm and which the most.

1. International intelligence gathering

The harder problem at the moment, the one we haven't come close to solving, stems from the fact that Americans aren't the only people following the debate over intelligence collection. So does the rest of the world. And it doesn't take much comfort from legal assurances that the privacy

interests of *Americans* are well protected from our intelligence agencies' reach. So, while the debate over U.S. intelligence gathering may be receding in this country, the storm is still gathering abroad.

Foreign intelligence is crucial

Attacks on NSA's collection of intelligence on foreign governments outside the United States are new. And it's important for the American people to understand how critical NSA's foreign intelligence collection is to our ability to influence events and to protect our people around the world. NSA's ability to track terrorists abroad has been crucial to the degradation of al Qaeda's central command. Terrorists come from every nation, and we cannot offer a refuge in the name of privacy. After all, the attacks of 9/11 were planned in Hamburg, Germany. NSA's aggressive pursuit of terrorists has also paid dividends for other nations with less advanced capabilities – including some of those countries complaining loudest.

But we don't need foreign intelligence capabilities just to track terrorists. The world is full of nations whose interests conflict with ours. Indeed, it is hard to find a country whose interests do not at least occasionally diverge from our own. When that happens, we can expect the other country to do everything it can to help itself and its citizens at the expense of ours. Other countries may protect well-connected criminals or terrorists who victimize Americans; they may help their companies break the trade embargo on Iran; they may be planning to cut off crucial commodity or technology shipments to the United States; they may be getting ready to attack another country or to conduct a genocide; they may be engaged in negotiations over issues from peace in the Middle East to arms control. In every case, our ability to respond to surprises around the globe depends on gathering intelligence on other countries' plans.

We cannot afford to exempt countries that often see themselves as allies from the possibility of intelligence collection. Our interests often diverge from those of even generally friendly countries. Even allies can have bitter disputes, where every bit of information may be needed to ensure a favorable outcome. To take one example, the European Union is filled with NATO allies, but that has not kept Brussels from using hard-nosed tactics to disadvantage U.S. industry and to obstruct important U.S. diplomatic goals on a regular basis.

Equally, we cannot restrict our intelligence community to gathering “what we need, not what we can.” Intelligence is not a like electricity, available on demand. It can take years to get into position to collect intelligence – and more years before the intelligence is needed. But when it is needed, the need is often unexpected and urgent, and the years of painstaking effort to gather “what we can” are suddenly worthwhile.

I recognize the diplomatic harm that the Snowden leaks and their orchestration by Glenn Greenwald have caused. Many other countries have complained about the idea that NSA may be spying on their citizens. Politicians in France, Brazil, Germany, the Netherlands, the United Kingdom, Belgium, and Romania, among others, have expressed shock and called for investigations. The European Parliament has threatened to suspend law enforcement and intelligence agreements.¹ German Chancellor Angela Merkel has personally called President

¹ European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme,

Obama to extract an assurance that her phone is not now being targeted. Germany and France have demanded a new international agreement to stop spying between allies.

European hypocrisy

Some of this is just hypocrisy. Shortly after President Hollande demanded that the United States “immediately stop” its intercepts² and the French Interior Minister used his position as guest of honor at a July 4th celebration to chide the United States for its intercepts, *Le Monde* disclosed what both French officials well knew – that France has its own program for large-scale interception of international telecommunications traffic.³ According to French Foreign Minister Bernard Kouchner, “Let’s be honest, we eavesdrop, too. Everyone is listening to everyone else. But we don’t have the same means as the United States, which makes us jealous.”

And let's not forget that Chancellor Merkel visited China right after public disclosures that the Chinese had penetrated her computer network, yet she managed to be “all smiles” for the Chinese while praising relations between the two countries as “open and constructive.”⁴ There were no calls for sanctions or agreements to put an end to China’s notorious hacking campaign.

What’s more, practically every comparative study of law enforcement and security practice shows that the United States imposes more restriction on its agencies and protects its citizens’ privacy rights from government surveillance more carefully than Europe.

I’ve included below two figures that illustrate this phenomenon. One is from a study done by the Max Planck Institute, estimating the number of surveillance orders per 100,000 people in several countries. While the statistics in each are not exactly comparable, the chart published in that study shows an unmistakable overall trend. The number of U.S. orders is circled, because it’s practically invisible next to most European nations; indeed, an Italian or Dutch citizen is over a hundred times more likely to be wiretapped by his government than an American.⁵

surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)) (July 4, 2013), available at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN> [hereinafter *European Parliament Resolution*].

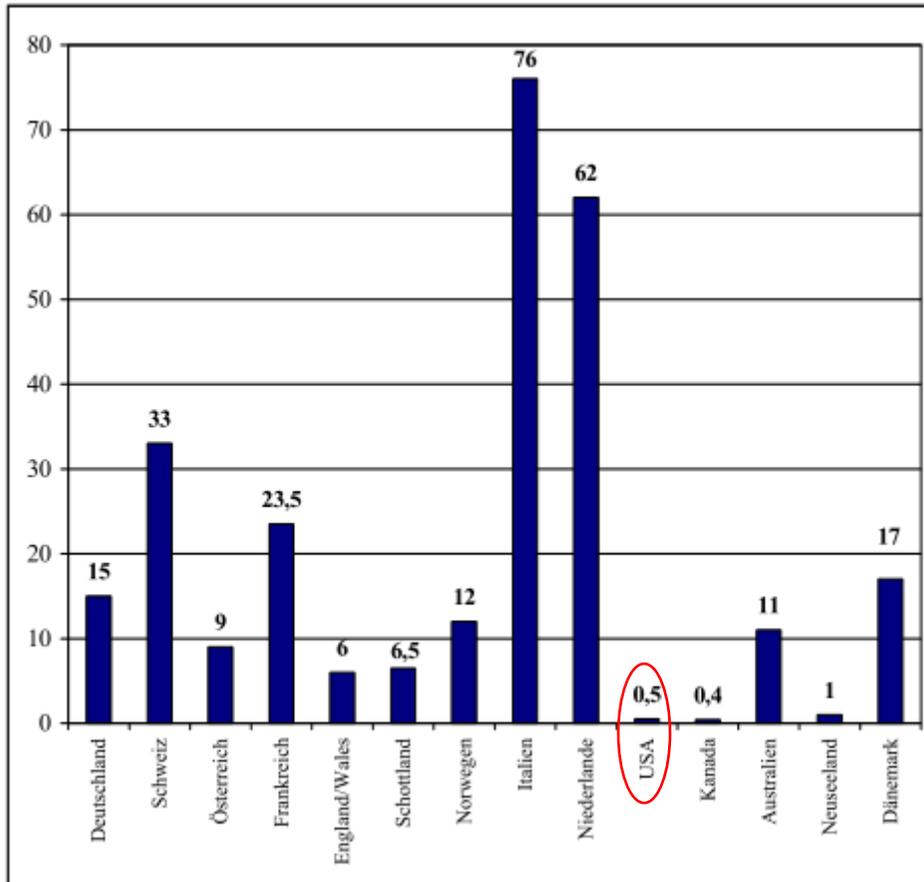
² Sébastien Seibt, *France's 'hypocritical' spying claims 'hide real scandal'*, FRANCE24 (July 3, 2013), <http://www.france24.com/en/20130702-france-usa-spying-snowden-hollande-nsa-prism-hypocritical> (last visited Oct. 28, 2013).

³ Jacques Follorou and Franck Johannès, *In English: Revelations on the French Big Brother*, LE MONDE (July 4, 2013, 5:24 PM), http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html (last visited Oct. 28, 2013).

⁴ *See Espionage Report: Merkel's China Visit Marred by Hacking Allegations*, DER SPIEGEL (Aug. 27, 2007), <http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html> (last visited Oct. 28, 2013).

⁵ Hans-Jörg Albrecht, et al., *Legal Reality and Efficiency of the Surveillance of Telecommunications*, MAX PLANCK INSTITUTE 104 (2003), http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_%20abschlussbericht.pdf (last visited Oct. 28, 2013).

Which countries do the most surveillance per capita?



European regimes, by and large, offer also far less protection against arbitrary collection of personal data – and expose their programs to far less public scrutiny. One recent study showed that, out of a dozen advanced democracies, only two – the United States and Japan – impose serious limits on what electronic data private companies can give to the government without legal process. In most other countries, and particularly in Europe, little or no process is required before a provider hands over information about subscribers.⁶

⁶ Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS (July 18, 2012).

Which countries allow providers simply to volunteer information to government investigators instead of requiring lawful process?

	Can the government use legal orders to force cloud providers to disclose customer information – as in PRISM?	Can the government skip the legal orders and just get the cloud provider to disclose customer information voluntarily?
Australia	Yes	Yes
Canada	Yes	Yes*
Denmark	Yes	Yes*
France	Yes	Yes**
Germany	Yes	Yes**
Ireland	Yes	Yes*
Japan	Yes	No
Spain	Yes	Yes*
UK	Yes	Yes*
USA	Yes	No

*Voluntary disclosure of personal data requires valid reason

**Some restrictions on voluntary disclosure of personal data without a valid reason and of some telecommunications data

At most, European providers must have a good reason for sharing personal data, but assisting law enforcement investigations is highly likely to satisfy this requirement. In the United States, such sharing is prohibited in the absence of legal process. Indeed, when one Ars Technica reporter who believed the European hype about its privacy rules took a closer look at European webmail providers, disillusionment set in fast.⁷ He found that, unlike their US counterparts, German email providers are unable to issue transparency reports of the sort that US companies have been publishing:

⁷ See Cyrus Farivar, *Europe won't save you: Why e-mail is probably safer in the US*, ARS TECHNICA (Oct. 13, 2013, 5:00 pm), <http://arstechnica.com/tech-policy/2013/10/europe-wont-save-you-why-e-mail-is-probably-safer-in-the-us/2/>.

German law forbids providers to talk about inquiries for user data or handing over user data ... We are currently investigating a possible way with our lawyer to issue a transparency report about questions from police like Google, Microsoft, and [many] other US providers do, but we can not promise we will be able to do so. We try hard.

In addition, while US authorities can get a specific "gag" order to prevent subscribers from knowing that their mail has been seized; the orders can be challenged and often expire on their own. It appears that in Europe disclosure is not an option:

[A]n American provider could notify its customer that he or she is the target of a judicial investigation. Google has a user notification policy, for instance, that stands unless the court forbids it from disclosing that information. ... German court orders, by contrast, appear to be sealed automatically.

And finally, it appears that European mail providers cannot challenge government discovery orders before turning over the data. In Germany and the Netherlands, the only jurisdictions the writer examined, providers turn over the data first, and then argue about whether they should have to do so. One supplier said that it:

could challenge a secret court order after the fact, unlike in the case of the United States, where such challenges can be made before such a handover. "If we think the order was not right, we can complain afterwards—and we would do so."

Finally, the European Union, which is threatening to abrogate the SWIFT financial terrorism information sharing agreement, stands in a class by itself for hypocrisy. For more than fifty years, Brussels has watched as the French government spied on other European nations, and as those nations returned the favor, without ever proposing to stop the snooping. It doesn't even have a serious set of data protection rules for the law enforcement agencies of Europe, despite surveillance levels up to 100 times what we experience in the United States. It's true that, unlike our section 215 program, the EU doesn't have a big metadata database. But that's because Europe doesn't need one. Instead, the European Parliament passed a measure forcing all of its information technology providers to create and retain their own metadata databases so that law enforcement and security agencies could conveniently search up to two years' worth of logs.⁸ These databases are full of data about American citizens, and under EU law any database held anywhere in Europe is open to search (and quite likely to "voluntary" disclosures and automatic gag orders) at the request of any government agency anywhere between Bulgaria and Portugal. Yet that abysmal track record on privacy has stopped the European Parliament from declaring its immediate intent to regulate *American* surveillance.

The threat to American intelligence capabilities

⁸ See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML> (last visited Oct. 28, 2013).

Just because much of the outrage around the world is manufactured does not mean that it is without risk for the United States. Quite the contrary, European and other nations see the prospect for enormous gains at the expense of the U.S., in part because President Obama seems genuinely embarrassed and unwilling to defend the National Security Agency. Instead, he is offering assurances to select world leaders that they are not targets, and his homeland security adviser is declaring that “the president has directed us to review our surveillance capabilities, including with respect to our foreign partners. We want to ensure we are collecting information because we *need* it and not just because we *can* [and that] we are balancing our security needs with the privacy concerns all people share.”⁹ Administration sources have begun criticizing the NSA for putting the President in this bind, and they are hinting at the possibility of negotiating reciprocal deals with other countries that will bar espionage directed at each other while sharing intelligence.

Meanwhile foreign officials are seizing on the disclosures to fuel a new kind of information protectionism. During a French parliament hearing, France’s Minister for the Digital Economy declared that, if the report about PRISM “turns out to be true, it makes [it] relatively relevant to locate datacenters and servers in [French] national territory in order to better ensure data security.”¹⁰ Germany’s Interior Minister was even more explicit, saying, “Whoever fears their communication is being intercepted in any way should use services that don’t go through American servers.”¹¹ And Neelie Kroes, Vice President of the European Commission, said, “If European cloud customers cannot trust the United States government or their assurances, then maybe they won’t trust US cloud providers either. That is my guess. And if I am right then there are multi-billion euro consequences for American companies.”¹²

I suspect that the rest of the world sees an opportunity for a kind of “three-fer” in trying to force companies to store data in France or Germany or Brazil rather than the United States. First, local data storage means more data storage jobs and investment at home and less in the United States. Second, it means that the data (including data about Americans) will be easily available to French and German and Brazilian investigators – without legal process. And third, it makes the United States intelligence agencies weaker and more dependent on the cooperation of Europeans – creating another bargaining chip like the SWIFT arrangement that Europe is already using as leverage in the current flap.

⁹ Lisa Monaco, *Obama administration: Surveillance policies under review*, USA TODAY (Oct. 24, 2013, 8:43 pm), <http://www.usatoday.com/story/opinion/2013/10/24/nsa-foreign-leaders-president-obama-lisa-monaco-editorials-debates/3183331/> (last visited Oct. 28, 2013)

¹⁰ Valéry Marchive *France hopes to turn PRISM worries into cloud opportunities*, ZDNET (June 21, 2013, 9:02 GMT), <http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/> (last visited Oct. 28, 2013).

¹¹ *German minister: Drop US sites if you fear spying*, ASSOCIATED PRESS (July 3, 2013), <http://www.usatoday.com/story/news/world/2013/07/03/nsa-germany-snowden-websites/2487125/> (last visited Oct. 28, 2013).

¹² Neelie Kroes, Vice President, European Commission, Statement after the meeting of European Cloud Partnership Board, Tallinn, Estonia (July 4, 2013), available at http://europa.eu/rapid/press-release_MEMO-13-654_en.htm.

What Congress Can Do

In short, we face the prospect of two serious attacks on U.S. interests as a result of the Snowden leaks. First, foreign nations will threaten our companies in the hope of moving data and jobs out of the United States. Second, they will capitalize on President Obama's defensive crouch to extract diplomatic and intelligence concessions that would have been unthinkable a year ago.

At the same time, I note, these nations have asked China, which is subjecting them to the most notorious and noisy computer hacking campaign on the planet, for, well, for nothing at all. The reason for that reticence is simple. They know that China will give them nothing.

And that, it seems to me, is where Congress comes in. Sometimes an American negotiator's best friend is an unreasonable Congress. As far as European negotiators are concerned, the United States Congress is almost in China's league. If Congress sets limits on what the executive branch can concede to its foreign counterparts, those limits will be observed. And if Congress specifies consequences for threatening U.S. industry, threatening U.S. industry will be much less attractive.

That's why I suggest that any legislation addressing the domestic intelligence program also address the international campaign to weaken U.S. intelligence capabilities. What would that legislation say? Let me suggest a few possibilities, any one of which would provide U.S. negotiators with useful limits and leverage:

- A “cooling off” provision requiring that any intelligence reciprocity agreement with any nation be submitted to Congress for review prior to taking effect.
- A “start with common ground” provision prohibiting reciprocal intelligence talks with any nation unless the DNI determines that the nation does not use its intelligence services to steal commercial information from private American companies for the benefit of its own companies.
- A “true reciprocity” provision requiring an independent report to this committee from the CIA, NSA, and other agencies prior to any proposed intelligence reciprocity arrangement taking effect; no such arrangement could take effect without a determination by Congress that the arrangement provided benefits to the U.S. intelligence community that matched the benefits to the counterpart nation.
- A “trust but verify” provision requiring that the DNI certify that any reciprocal “no spying” promise in an international agreement be verifiable and enforceable.
- A “no hostage-taking” provision that bars negotiations – and counterterrorism intelligence-sharing – with any European Union member if the European Union terminates its existing terrorism information sharing arrangements with the United States or takes action to punish U.S. companies in an effort to regulate U.S. intelligence or law enforcement agencies. Exceptions for intelligence sharing would require a determination

by the DNI that the sharing is in the national interest of the United States and that the country in question took action to oppose the termination.

- A “stay in your lane” provision barring any negotiation with the European Union that touches on intelligence. The European Union has no authority over European intelligence, and its role in past counterterrorism negotiations has been uniformly hostile to American interests.
- A “sauce for the goose” provision requiring declassified reports from the intelligence community on (1) the scope and intrusiveness of other nations' surveillance of American officials, businessmen, and private citizens and (2) how much data about individual Americans is being retained by companies in Europe and elsewhere, how often it is accessed by European governments, and whether that access meets our constitutional and legal standards.

2. Domestic intelligence-gathering and the telephone metadata program

Why the program makes sense

NSA's telephone metadata program was intended to cure one of the failings of our intelligence community in the run-up to 9/11. NSA intercepted calls that one of the hijacking ringleaders, Khalid al Mihdhar, made from San Diego to a known al Qaeda number in Yemen. But NSA did not have an easy way to determine that the hijacker was already in the United States. That crucial fact would not be discovered until a few weeks before the attacks.

The metadata program filled a gap in our defenses that had cost three thousand lives. It collected a very large amount of information. Taken out of context – and Snowden and Greenwald worked hard to make sure it *was* taken out of context by withholding the minimization guidelines from their readers for two weeks – this was a troubling disclosure. But the minimization guidelines that the journalists withheld show that collecting data isn't the same as actually looking at it. Under the minimization rules, metadata could only be examined by one of two dozen NSA analysts, and they had to supply specific, articulable facts to justify the suspicious nature of the number they wanted to check. In fact the minimization rules were interpreted so strictly that last year the agency only actually looked at records for 300 subscribers and after looking at their records, the agency only passed 500 numbers to the FBI for investigation and identification of the subscriber.¹³

Much of the argument about whether the program was lawful has died down as the rationale approved by the FISA court has become public, and I will leave that issue to Steve Bradbury. I do want to talk about the policy basis for the program. In the absence of the metadata collection, tracing a phone number's contacts would require access to several carriers' records. The effort would be limited by how long the different carriers choose to keep their data, and hampered by

¹³ Dana Priest, *Piercing the confusion around NSA's phone surveillance program*, THE WASHINGTON POST (Aug. 8, 2013), http://articles.washingtonpost.com/2013-08-08/world/41198127_1_phone-records-phone-surveillance-program-metadata-program (last visited Oct. 28, 2013).

the different data storage systems they use. It would also be less secure, since every number of interest would have to be sent to every carrier that keeps billing records, including many foreign companies supplying “virtual networks” in the United States. The safest and the fastest way to search the data is to put it in one place.

As long as the rules about access are observed, the end result of the collection-first approach is much the same as a standard law enforcement inquiry, and often it is better. In the standard inquiry, the government establishes the relevance of its inquiry first and is then allowed to collect and search the data. In the new collection-first model, the government collects the data first and then must establish the relevance of each inquiry before it's allowed to conduct a search. In fact, the standard approach almost always sweeps up irrelevant as well as relevant data, and once it has been collected, that data can be searched without limit.

I know it's fashionable to say that letting the government collect all that data could lead to abuses if later administrations change the rules. In fact, the risk of rule-breaking is pretty much the same whether the collection comes first or second. Either way, you have to count on the government to tell the truth to the court about what it wants and why, and you have to count on the court to apply the rules. If you don't trust them to do their job, then neither model offers much protection against abuses.

But if in fact abuses were common, we'd know it by now. Today, law enforcement agencies collect over a million telephone billing records a year using nothing but a subpoena.¹⁴ That means you're roughly a thousand times more likely to have your telephone calling patterns reviewed by a law enforcement agency than by NSA. (And the chance that law enforcement will look at your records is itself low, around 0.25% in the case of one carrier¹⁵). Law enforcement has been gaining access to our call metadata for as long as billing records have existed – nearly a century.

If this were the road to Orwell's 1984, we'd be there by now, and without any help from NSA's 300 searches.

How can the program be reformed?

In my view the minimization procedures are working. If anything, the government did too good a job in thinking of restrictions that could be imposed on the program. It is hard to add more without hurting the program's effectiveness. Nonetheless, I recognize the reality that something more must be done if the program is to survive. So I offer below some thoughts on the kinds of reforms now under consideration.

¹⁴ In 2012, Rep. Markey sent letters to a large number of cell phone companies, asking among other things how many law enforcement requests for subscriber records the companies received over the past five years. The three largest carriers alone reported receiving more than a million law enforcement subpoenas a year. Markey Letters to Wireless Carriers on Enforcement Requests, http://www.markey.senate.gov/Markey_Letters_to_Wireless_Carriers.cfm (last visited Oct. 28, 2013).

¹⁵ Letter from Timothy P. McKone, Exec. Vice President, AT&T, to Congressman Edward J. Markey (May 29, 2012), available at http://www.markey.senate.gov/documents/2012-05-22_ATT_CarrierResponse.pdf.

“Roamer” authority. Of all the proposals for reform currently being advanced, the best is the proposal to cut NSA some slack when a foreign target unexpectedly shows up in the United States, thus triggering all the legal protections applicable on US soil. It's often difficult for the agency to know that a number is calling from the United States, but today the NSA has to report itself as having violated those rules every time a target makes a call while changing planes in New York or Miami. That is by far the largest category of “violation” that has been used by opponents as evidence that the agency does not obey the law. Rather than set the agency up for an entirely predictable fall, the law should give it time to seek FISA court approval when it finds a foreign target suddenly communicating from the United States, just as we allow emergency FISA taps without court approval for a limited period of time.

Oversight. One of the most troubling aspects of the Snowden affair was the airy dismissal by opponents of the elaborate set of internal controls on intelligence abuses that were erected after the Church and Pike investigations of the 1970s. In an effort to show for the first time that intelligence could be conducted effectively under law and with oversight, Congress created intelligence oversight committees, the FIS court, and a host of internal review authorities such as inspectors general. All of these institutions have top security clearances and independence from the intelligence community. This “1970s model” has been followed for decades, gradually growing stricter. Everyone in Washington accepted it because it seemed the only way to have independent scrutiny of the intelligence community without revealing sensitive programs.

Yet large swaths of the public now dismiss the 1970s model out of hand. These critics didn't have much to offer in its place, other than a vague notion that we need a detailed public debate over every intrusive intelligence program so that every member of Congress and every citizen can weigh in. That won't work. But there is deep public skepticism about allowing the intelligence committees and the court to serve as proxies for the public. Given those doubts, the public may not be much reassured by measures strengthening the independence of the NSA inspector general, say, or tweaking the way the judges of the FIS court are appointed. What's more, as I discuss later, the costs of further expanding the FIS court's role are growing.

Section 215. We cannot play “pick-up sticks” with national security, removing first one and then another of the protections adopted in the wake of 9/11, waiting to see which move actually causes the structure to collapse. The section 215 metadata program was a direct response to the 9/11 attacks, and it is fair to ask opponents of the program how they would close the gap revealed by Khalid al Mihdhar's phone call to Yemen. There may be ways to tighten the program while still protecting the seam between domestic and international intelligence collection, but the burden of doing so should be on proponents.

Some propose to rely on the phone companies to store and produce the data now stored by NSA. I doubt that such a solution would be affordable. It certainly would not be efficient. Nor would it be particularly private, since any metadata stored with the carriers would be subject to subpoena not just by the government but by every divorce lawyer in the country.

FIS Court. Proposals to appoint a special counsel to argue against the government in the FIS court run into the same problem of public trust as the rest of the 1970s model. Anyone whom the court could appoint will have to have a security clearance and intimate familiarity with NSA's

programs. They will need a cleared staff and clerical assistance in classified facilities. They will be, for all intents and purposes, a part of the U.S. government and dependent on the government to function. This will be pointed out by critics every time the court ends up ruling for the government. So setting up yet another advocate against aggressive intelligence gathering isn't likely to restore public trust.

But it will create an imbalance in advocacy. If anything, there are already too many offices competing for the job of protecting citizens' privacy by limiting NSA's capabilities. The NSA inspector general and general counsel see that as part of their jobs, as do the various privacy and civil liberties officers for the intelligence community and the administration as a whole. On top of that, the FISA process has yet another set of officials charged with second-guessing NSA on privacy and law. The Department of Justice sees itself not as the agency's advocate but as a kind of umpire, responsible for balancing privacy and security independent of the agency. The staff attorneys at the FIS court also see themselves playing a significant role in protecting privacy rights. They apparently review and negotiate over FISA warrant applications before they reach the judges, who provide a third layer of umpiring. Every one of these levels of review, I think it's safe to say, is more inclined to trim, condition, and restrict than to expand the searches that NSA proposes.

The justification for having all these umpires is that there's no one on the other side to challenge NSA's requests. But if we're now going to appoint an advocate to argue against the agency's requests, we ought to let the agency argue *for* its requests. As any Red Sox fan will tell you, when the other team takes the field, the umpires should let both teams play. One team should not have three umpires on its side too. So any effort to make the FIS court more truly adversarial should work both ways; NSA should be allowed to file directly in the FIS court and to decide which rulings to appeal.

If there is a problem at the FIS court, it is not the lack of an advocate on the other side. Rather it is the odd, quasi-managerial role we keep pressing on the FIS court. It leaves the court in an awkward spot. The court has been widely criticized as a rubber stamp, and it's clear that the criticism stings. It recently announced that it was keeping statistics to show how often it forces modifications of FISA orders.¹⁶ This raises questions about its even-handed application of the law. Would you want to be judged by a court that goes out of its way to publicize a scorecard of how often it rules against you?

What's more, because the court is so intimately involved in the agency's affairs, the court comes to feel that it has responsibility for the details of how its orders are administered but only limited tools to fulfill that responsibility. Unlike real managers, who have many administrative tools to make sure their policies are carried out, the FIS court has only two: legal rulings and contempt findings. As the court becomes more familiar with the agency, it grows more invested in the implementation of particular measures and policies. The temptation to declare these measures legally necessary is very great. Similarly, when the court is disappointed or surprised by the

¹⁶ See Letter from the Honorable Reggie B. Walton, Presiding Judge, the United States Foreign Intelligence Surveillance Court, to the Honorable Charles E. Grassley, Ranking Member, Committee on the Judiciary, United States Senate (Oct. 11, 2013), available at <http://www.uscourts.gov/uscourts/courts/fisc/ranking-member-grassley-letter-131011.pdf>.

agency's implementation of the measures, the temptation to reach for the contempt power is strong. That was certainly true of Presiding Judge Lamberth, who spent most of 2001 pursuing sanctions on a well-regarded FBI agent for not observing the "wall" between law enforcement and intelligence. The judge was so aggressive in this pursuit that the FBI was unable to use its most effective counterterrorism teams to find the al Qaeda plotters whom we learned were in the country in August of 2001. The court of appeals ultimately found the wall to be utterly without a basis in law but by then it was too late. That may be the most egregious misstep by the FIS court, but it is symptomatic of an institutional canker that has recurred under other presiding judges as well.

In the long run, I fear it will become clear that we have given Article III judges responsibilities that belong to the executive branch, and that we will pay another price for that mistake like the one we paid in 2001. For those reasons, I look with great skepticism on expansions of the FIS court's role and discretionary powers, including the authority to bring in outside advocates of its choosing and the authority to appoint an independent and largely permanent staff of lawyers who are bound to develop their own policy views on the intelligence community.

Conclusion

Thirty-five years of trying to write detailed laws for intelligence gathering have revealed just how hard that exercise is – and why so few nations have tried to do it. Domestic and international forces are pushing the United States toward a new understanding of how to govern our intelligence capabilities. If we make the wrong decisions in the next few months, our intelligence capabilities may be handicapped for a generation – or until some disaster reveals our errors in stark relief.

The responsibility for those choices falls on the President -- and on this committee.

NSA PROGRAMS
Hearing Before the House Permanent Select Committee on Intelligence
Tuesday, October 29, 2013

Written Testimony of Stephen I. Vladeck
Professor of Law and Associate Dean for Scholarship,
American University Washington College of Law;
Co-Editor-in-Chief, [@Just Security](#)

Chairman Rogers, Ranking Member Ruppertsberger, and distinguished members of the Committee:

Thank you for inviting me to testify today—and for inviting the views of outsiders like me on what have historically been such a closely held series of conversations.

Reasonable people will certainly continue to disagree about the proper scope of the NSA’s surveillance authorities, especially those undertaken pursuant to section 702 of the Foreign Intelligence Surveillance Act (FISA),¹ and section 215 of the USA PATRIOT Act.² Rather than devote my time to taking sides in a debate that has been thoroughly joined,³ I would like to focus my testimony today on three different, but related propositions—points on which I hope we all have common cause:

First, it is important to keep in mind the extent to which these surveillance authorities should be calibrated—as FISA was in 1978—in order to work around and avoid resolution of *unresolved* tensions in the Supreme Court’s Fourth Amendment jurisprudence. Of course, Congress is free to—and oftentimes must—legislate in the shadow of the Constitution, and in the gaps created by the Supreme Court’s jurisprudence. But there is a significant risk when Congress does so: Whereas such drafting-into-gaps empowers the government to act, the more expansively the Executive Branch *fills* those gaps, the more likely it is to invite judicial intervention—and even circumscription, if the courts are uneasy about the adequacy of the statutory limitations that the legislature has prescribed. Indeed, as

1. Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438–48 (codified at 50 U.S.C. § 1881a).

2. Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861).

3. Compare, e.g., Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, LAWFARE RESEARCH PAPER SERIES NO. 3 (Sept. 1, 2013), <http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf>, and David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RESEARCH PAPER SERIES NO. 4 (Sept. 29, 2013), <http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf>, with Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL’Y (forthcoming 2013), available at <http://justsecurity.org/wp-content/uploads/2013/10/Just-Security-Donohue-PDF.pdf>, and Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 “Metadata” Collection Program*, JUST SECURITY, Oct. 1, 2013 (5:25 p.m.), <http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/>.

the pending lawsuits filed by the ACLU⁴ and EPIC⁵ (among others) illustrate, we may already be reaching the point in which the federal judiciary beyond the FISA Court will be reviewing these programs.

Second, regardless of where one comes down on the merits, the inevitability of full-throated judicial review of these programs should provide its own impetus for meaningful reform. It's obvious why those who question the government's interpretation (and underlying constitutionality) of these authorities desire change. But even those who *approve* of programs such as bulk telephony metadata collection and PRISM should also embrace reform—if only to increase the likelihood that these programs will *survive* such judicial review. On the statutory side, it should follow that the more precise the fit between the substantive authorities Congress has provided and the specific programs the government is undertaking, the more likely courts will uphold the Executive Branch's understandings. And with regard to constitutional considerations, the clearer it is that these authorities include meaningful checks and balances designed to minimize their impact on our constitutional rights and other privacy interests, the more likely courts will find them to be consistent with the Fourth Amendment.

Third, and perhaps most significantly, once we accept the urgency of FISA reform, we should also appreciate that there are any number of meaningful and responsible ways to get there from here—both with regard to reforming the substance of the government's surveillance authorities and the processes through which they are exercised. Thus, on the substantive front, even if we cannot all agree on whether the controversial collection authorities should be scaled back in the abstract, Congress could certainly move to *codify* baseline minimization requirements for each content-based surveillance program, rather than leaving them up to the discretion of the Executive Branch and FISA Court—to better limit how the government is allowed to *use* the information it is collecting. Congress might then also provide stiffer penalties for violations of these rules as a means of giving the minimization requirements teeth that, for now, they're quite demonstrably lacking.

With regard to process, I also believe that there is much to commend proposals for some kind of “special advocate” to participate in at least some proceedings before the FISA Court in order to present adversarial briefing and

4. *See* Am. Civil Liberties Union v. Clapper, No. 13-civ-3994 (S.D.N.Y. filed June 11, 2013).

5. *See In re Elec. Privacy Info. Ctr.*, No. 13-58 (U.S. filed July 8, 2013).

argument—and then object in cases in which he believes the FISA Court has erred. There’s also plenty of room for Congress to bolster the existing notice requirements for cases in which the government seeks to use FISA-derived evidence in criminal prosecutions, and to otherwise exert pressure on the FISA Court to publicize its decisions to the maximum extent practicable.

As significantly, such reforms should not just focus on responding to the controversies of the moment—*i.e.*, the 215 and 702 programs. If we’ve learned nothing else from this summer, hopefully we’ve learned the value and importance of meaningful public discourse and debate on these sets of issues—and, along with that, the costs to the government of having to defend these programs only after damaging disclosures concerning their scope and substance.

Ultimately, regardless of which specific path Congress chooses to take, the critical point for present purposes is that it’s a false dichotomy to suggest, as some have, that the choice is between preserving the status quo and undermining the efficacy of these programs. Simply put, sufficiently careful and comprehensive FISA reform will only further our national security while better protecting our civil liberties.

I. LEGISLATING INTO GAPS: THE FOURTH AMENDMENT QUESTIONS

As is now well-known, FISA was enacted at least largely to provide legal underpinnings (and constraints) on government surveillance that had previously been conducted solely under the auspices of the Executive Branch.⁶ Although the Supreme Court had held in the *Keith* case that there is no “domestic intelligence surveillance” exception to the Fourth Amendment’s Warrant Clause,⁷ the possible existence of a *foreign* intelligence surveillance exception, and the lower courts’ varied and complex answers to that question,⁸ underscored the need for a statute both authorizing and circumscribing such surveillance activities—in lieu of constitutional doctrine. In other words, FISA itself was meant to occupy an unsettled area of Fourth Amendment law.

6. *See generally* 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS §§ 2:1 to 3:9, at 37–113 (2d ed. 2012).

7. *See* United States v. U.S. Dist. Ct., 407 U.S. 297 (1972).

8. *See, e.g.*, Steve Vladeck, *More on Clapper and the Foreign Intelligence Surveillance Exception*, LAWFARE, May 23, 2012 (3:32 p.m.), <http://www.lawfareblog.com/2012/05/more-on-clapper/>.

The same can be said of section 215 of the USA PATRIOT Act and section 702 of FISA. Section 215, which authorizes the government to obtain—without a warrant—certain “tangible things” held by businesses deemed to be “relevant” to an ongoing terrorism investigation,⁹ capitalizes upon the so-called “third-party” doctrine. That doctrine, which traces its origins in principal part to the Supreme Court’s 1979 decision in *Smith v. Maryland*,¹⁰ holds that individuals do not have an expectation of privacy in personal information that they voluntarily provide to a third party where the third party uses such information as part of its ordinary course of business—and so the government does not violate the Fourth Amendment when they obtain such information *from* such third-parties without the individuals’ consent.¹¹ At least thus far, the FISA Court opinions that have analyzed the Fourth Amendment questions raised by the bulk telephony metadata program have held them to be squarely settled by *Smith*—because the metadata is all being collected from telecom providers who use the information for business purposes, and is therefore information in which individuals are said to have no legitimate expectation of privacy.¹²

Likewise with regard to section 702 (along with surveillance carried out pursuant to Executive Order 12,333): Insofar as these authorities contemplate sweeping, warrantless interceptions of communications where the targets are reasonably believed to be non-citizens outside the territorial United States,¹³ the provision thereby occupies territory left open after the Supreme Court’s 1990 decision in *United States v. Verdugo-Urquidez*, which suggested that non-citizens outside the territorial United States categorically lack Fourth Amendment rights.¹⁴ And insofar as surveillance conducted pursuant to these authorities might incidentally result in the interception of communications by individuals *with* Fourth Amendment rights, for which the government would usually need a warrant, the “incidental overhears” doctrine suggests that there’s no Fourth Amendment

9. 50 U.S.C. § 1861(a)(1).

10. 442 U.S. 735 (1979).

11. *See id.* at 742–45.

12. *See, e.g., In re Application of the FBI for an Order Requiring the Production of Tangible Things From [REDACTED]*, No. BR-13-109, slip op. at 6–9 (FISA Ct. Aug. 29, 2013) [hereinafter Eagan Opinion].

13. *See, e.g.,* 50 U.S.C. § 1881a(a)(1).

14. 494 U.S. 259 (1990).

violation so long as the government was not specifically *targeting* such communications.¹⁵

But even if it *appears* that these programs are therefore free of constitutional defects, the doctrines are not as settled as many may like to believe, potentially leaving these surveillance programs, in their current form, vulnerable to judicial intervention. For example, five different Justices expressed varying degrees of skepticism with the continuing scope of the third-party doctrine in the Supreme Court’s January 2012 decision in *United States v. Jones*,¹⁶ and even on its own terms, one could argue that there’s a difference between information *obtained* by a third-party and information *aggregated* by the government in a manner that is necessarily unavailable to any private entity.¹⁷

One might also quibble with the extent to which *Verdugo-Urquidez* settled the inapplicability of the Fourth Amendment to non-citizens overseas, especially since Justice Kennedy (whose vote was necessary to the result) appeared uncomfortable with such a categorical rejection of constitutional protections—as opposed to a case-by-case analysis.¹⁸ To similar effect, there is also reason to question the FISA Court of Review’s 2008 endorsement of a categorical “foreign intelligence surveillance” exception to the Fourth Amendment’s Warrant Clause.¹⁹ But far more significantly, there are strong arguments against application of the “incidental overhears” doctrine to communications by U.S. persons obtained under section 702, both because (1) such communications are obtained on a massive scale;

15. See, e.g., *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280–81 (S.D.N.Y. 2000).

16. See 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring in the judgment).

17. That is to say, although individuals may not retain an expectation of privacy in specific data streams they provide to individual third parties (e.g., phone companies; financial institutions; etc.), individuals *may* retain an expectation of privacy in the aggregation of those streams, which, at least in theory, is a capability possessed solely by the government. *Cf.* *Kyllo v. United States*, 533 U.S. 27 (2001) (holding that individuals retain an expectation of privacy from “plain-view” technologies that can only be deployed by the government, as opposed to other private parties).

18. See, e.g., *Verdugo-Urquidez*, 494 U.S. at 275–78 (Kennedy, J., concurring); see also Michael Bahar, *As Necessity Creates the Rule: Eisentrager, Boumediene, and the Enemy—How Strategic Realities Can Constitutionally Require Greater Rights for Detainees in the Wars of the Twenty-First Century*, 11 U. PA. J. CONST. L. 277, 315 (2009) (observing that Justice Kennedy’s concurrence in *Verdugo-Urquidez* is widely viewed as the controlling opinion on the issue of extraterritoriality application of the Fourth Amendment).

19. See *In re Directives* [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). *But see* Vladeck, *supra* note 8.

and (2) the government is well aware that such communications are likely to be intercepted.²⁰

To be clear, my point is not that the 215 and 702 programs, in their current forms, *violate* the Fourth Amendment. I mean only to underscore the open constitutional questions *surrounding* these programs—questions that, in my view, are not nearly as well settled by existing doctrine as the some may believe.

II. THE INEVITABILITY OF FULL-SCALE JUDICIAL REVIEW

The fact that these Fourth Amendment questions are not fully settled is also reinforced *by* those opinions of the FISA Court to which the public has now become privy. Even though we now have the benefit of a series of decisions by the FISA Court explaining why these programs are both consistent with their underlying statutes and the Fourth Amendment,²¹ those opinions leave a lot to be desired. Indeed, not only have criticisms of the FISA Court’s analyses come from all sides,²² but the Justice Department’s defense of the legality of the metadata program, at least, has focused on arguments largely *distinct* from those endorsed by the FISA Court.²³

I don’t mean to criticize the FISA judges themselves, for in many respects, they’ve been handed a loaded deck.²⁴ Virtually all of the proceedings before the FISA Court thus far have been *ex parte*, without the benefit of adversarial briefing or argument. It is true that there is a robust *internal* review process within the FISC, and that the NSA appears to have *self-reported* its errors; but that may not be enough, especially when dealing with such complex and massive programs. We now know, for example, that there have been a series of instances in which the

20. *See, e.g.*, United States v. Bin Laden, 126 F. Supp. 2d 264, 280–82 (S.D.N.Y. 2000); *see also* [REDACTED], 2011 WL 10945618, at *26–27 & n.67 (FISA Ct. Oct. 3, 2011) [hereinafter Bates Opinion].

21. *See, e.g.*, Eagan Opinion, *supra* note 12.

22. *See, e.g.*, Orin Kerr, *My (Mostly Critical) Thoughts on the August 2013 FISC Opinion on Section 215, THE VOLOKH CONSPIRACY*, Sept. 17, 2013 (7:39 p.m.), <http://www.volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/>.

23. *See, e.g.*, Defendants’ Memorandum of Law in Support of Motion To Dismiss the Complaint at 19–31, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. filed Aug. 26, 2013), *available at* https://www.aclu.org/files/assets/govt_motion_to_dismiss.pdf.

24. *See* James G. Carr, *A Better Secret Court*, N.Y. TIMES, July 23, 2013, at A21.

government, according to the FISA Court, *misled* the court about the nature of its surveillance programs and/or its interpretation of the relevant statutory authorities.²⁵

The upshot of these points is the conclusion that the open questions I've described above will not receive a full judicial airing before the FISA Court itself. And that fact has a lot to say about why I believe it's likely that these programs will receive more sweeping judicial review sooner or later. Indeed, the U.S. District Court for the Southern District of New York will hear oral argument late next month on the ACLU's lawsuit challenging the bulk metadata program on statutory and constitutional grounds,²⁶ and the Supreme Court is also soon set to consider an application for extraordinary relief from the Electronic Privacy and Information Center (EPIC) raising analogous challenges to the FISA Court's orders at the heart of the bulk metadata program.²⁷ We also learned late Friday that the government has also now notified a federal criminal defendant in Colorado of its intent to introduce evidence obtained under section 702 against him in his criminal trial,²⁸ which will undoubtedly spawn litigation over the constitutional question there.

Thus, regardless of *which* of these judicial proceedings gets there first, it is only a matter of time before the federal courts are asked to provide full-fledged answers to the statutory and constitutional questions surrounding the 215 and 702 programs. And it stands to reason that, if and when that time comes, meaningful statutory reforms will go a long way toward insulating the programs from judicial invalidation.

Take the metadata program as an example: Whether or not the program in its current form *is* consistent with Congress's intent when it enacted and amended section 215—and when it enacted another law expressly *prohibiting* telephony service providers from turning over customer records except pursuant to authorities

25. See Bates Opinion, *supra* note 20, at *5 n.14.

26. See *supra* note 4.

27. See *supra* note 5.

28. See Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES, Oct. 27, 2013, at A21; see also Second Notice of Intent To Use Foreign Intelligence Surveillance Act Information, United States v. Muhtorov, No. 12-cr-00033 (D. Colo. filed Oct. 25, 2013), available at <https://www.documentcloud.org/documents/810241-faa-notice.html>.

other than section 215²⁹—is a question on which reasonable minds have vigorously disagreed.³⁰ But what seems beyond dispute is that the program today is operated on terms far broader than what some Members of Congress who initially drafted section 215 contemplated.³¹ And so, as between judicial review of a program that seems increasingly divorced from its statutory underpinnings, and judicial review of a surveillance scheme that hews fairly closely to statutory text, it seems clear which is more likely to survive. And the more Congress is specifically trying to prevent the government from misusing or otherwise abusing its authorities to obtain information and/or communications for which it lacks a legal basis, the more likely that the programs will withstand *constitutional* scrutiny, as well.

My point is fairly straightforward, to be sure; but insofar as the government’s surveillance authorities under FISA operate in a constitutional shadow, the longer that shadow becomes, the more likely these authorities will be carefully scrutinized by the federal courts—scrutiny that meaningful statutory reform could go a long way toward satisfying.

Finally, and perhaps most significantly, it bears emphasizing that this discussion should hardly be limited to those issues currently on the front lines of American discourse. Although the 215 and 702 programs have excited the most public opinion in recent months, Congress should also ask whether similar reforms might be appropriate for *other* surveillance programs—including those programs the existence and/or scope of which are still classified. For as much as we have learned this summer about bulk metadata collection and PRISM, it only seems fair to assume that there are a number of additional programs to which the American public is *not* privy—and yet which may be in at least as much need of the same kinds of reforms. Put another way, reforms should be structural, and not just at the visible margins.

29. *See, e.g.*, 18 U.S.C. § 2702(b)(2) (not including section 215 among the authorities listed as “exceptions” to statutory bar on disclosure of records by electronic communications service providers).

30. *See, e.g.*, sources cited *supra* note 3.

31. *See, e.g.*, Letter from Hon. F. James Sensenbrenner, Jr., to Hon. Eric H. Holder, Jr. (Sept. 6, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

III. SOME THOUGHTS ON REFORMS

Of course, not all reforms are equal—and no one reform is a magic bullet. Thus, I don't mean to take sides as between the various proposals for FISA reform currently percolating in Congress. I must also confess that I am profoundly ambivalent about whether reform should prohibit the bulk *collection* of information on a mass, suspicionless scale—not because I don't have strong views on the matter, but because I fear that too many of the arguments *justifying* such government surveillance are based on considerations that cannot adequately be publicized.³²

Instead, I think it would be far more productive to briefly outline a few potential reforms that strike me as especially attractive even (if not especially) in the absence of new, front-end collection restrictions:

On the substantive side, Congress might start by clarifying which collections are permitted on such a wholesale, suspicionless scale, and which aren't. For example, is there a meaningful distinction between telephony metadata and, *e.g.*, internet metadata? Is PRISM consistent with what Congress meant when it initially enacted section 702? Are there other specific collection authorities that are being used to conduct surveillance that Congress never intended to—and still would not—authorize? Regardless of what one thinks the scope of the government's surveillance authorities *should* be, greater public transparency concerning what they *are* (and are *not*) seems an important starting point for any serious reform discussion.

Additionally, two obvious places for non-collection reforms involve the minimization requirements that apply to content-based surveillance programs. Although the *existence* of minimization requirements is mandated by statute,³³ the statutes have very little to say about the *substance* of those requirements. And although it may not be ideal for Congress to provide comprehensive requirements by statute on a program-by-program basis, it does seem to me to be obvious that Congress should prescribe a much more detailed statutory minimization *baseline*—

32. Without a full appreciation of the government's technological capabilities, it is difficult to assess the efficacy of alternatives to those surveillance methods that have been disclosed, and, as such, difficult to assess whether such bulk collection is truly "necessary" as compared to less-restrictive alternatives such as a query-based approach. Of course, this Committee is not saddled with the same lack of information.

33. *See, e.g.*, 50 U.S.C. § 1881a(e); *see also id.* § 1801(h) (providing minimal definition of "minimization procedures").

basic use restrictions that are a matter of statutory command, and not just Executive Branch or FISA Court discretion. To that end, it is certainly worth considering whether any and all post-collection querying of information involving U.S. persons must always be based upon reasonable, articulable suspicion (“RAS”). Congress might also consider clearer and harsher *penalties* for minimization violations—both when the violation appears to be authorized (as in the circumstances in which the FISA Court noted that government had misled it), or when it arises from the *ultra vires* conduct of individual government employees. Even without scaling back the government’s substantive collection reforms, such amendments could dramatically help to improve checks and balances *within* these programs.

On the process side, it does seem like an especially good idea to allow for greater adversarial engagement before the FISA Court—especially in those cases raising new questions of legal interpretation. Whether called a “special advocate” who nominally represents the public, or a security-cleared counsel specifically representing the putative targets of government surveillance, it seems to me obvious (as it did to two of the court’s former judges)³⁴ that the FISA Court would better be able to discharge its duties with the assistance of able counsel from more than just the government’s perspective.³⁵

Congress might also consider ramping up the FISA Court’s transparency—not by requiring publication of all of its work, but by at least creating a default (albeit *rebuttable*) presumption in favor of publication,³⁶ along with more rigorous

34. *See, e.g., Carr, supra* note 24.

35. To be sure, a complex series of Article III standing issues might arise if and when the special advocate were empowered to *appeal* an adverse decision by the FISA Court to the FISA Court of Review. *See, e.g., Hollingsworth v. Perry*, 133 S. Ct. 2652 (2013) (holding that defenders of state ballot proposition—as opposed to state itself—had no standing to appeal its invalidation by a district court because they had no “direct stake” in the outcome of their appeal). But however his responsibilities are defined, the participation of a “special advocate” before the FISA Court *itself* raises no such concerns since the only party that needs standing before that tribunal is the plaintiff—*i.e.*, the government. Thus, so long as proceedings before the FISA Court *presently* satisfy Article III’s adversity requirement, *see, e.g., In re Sealed Case*, 310 F.3d 717, 732 & n.19 (FISA Ct. Rev. 2002), no *new* Article III problems would be created by the participation of an additional party, on almost any terms, in the FISA Court.

36. There is no present statutory rule regarding publication of FISA Court opinions. That court’s own rules leave publication to the discretion of the individual judge. *See* U.S. For. Intel. Surv. Ct. Rules of Proc. R. 62(a) (2010). And although mandatory publication might raise constitutional concerns, it should follow that a rebuttable publication presumption would not interfere with any indefeasible constitutional authority that it might be argued the President possesses in this field.

reporting requirements both to Congress (and not just the intelligence committees), and, in some cases, to the public as well. After all, for as much as we now know about the 215 and 702 programs, there is also the prospect of additional current or future secret government surveillance programs to which we have not been, or otherwise will not become, privy. And if we've learned nothing else from the past few months, hopefully we now appreciate the significance of meaningful public understanding, awareness, and opportunity to engage on the substance of those activities the government carries out in our name—especially those that end up directly affecting United States persons.

* * *

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