

S. HRG. 113-334

STRENGTHENING PRIVACY RIGHTS AND NATIONAL SECURITY: OVERSIGHT OF FISA SURVEILLANCE PROGRAMS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

—————
JULY 31, 2013
—————

Serial No. J-113-25

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

88-671 PDF

WASHINGTON : 2014

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California

CHUCK SCHUMER, New York

DICK DURBIN, Illinois

SHELDON WHITEHOUSE, Rhode Island

AMY KLOBUCHAR, Minnesota

AL FRANKEN, Minnesota

CHRISTOPHER A. COONS, Delaware

RICHARD BLUMENTHAL, Connecticut

MAZIE HIRONO, Hawaii

CHUCK GRASSLEY, Iowa, *Ranking Member*

ORRIN G. HATCH, Utah

JEFF SESSIONS, Alabama

LINDSEY GRAHAM, South Carolina

JOHN CORNYN, Texas

MICHAEL S. LEE, Utah

TED CRUZ, Texas

JEFF FLAKE, Arizona

KRISTINE LUCIUS, *Chief Staff Director*

KOLAN DAVIS, *Republican Chief Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	47
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa	3

WITNESSES

Witness List	45
Cole, Hon. James M., Deputy Attorney General, U.S. Department of Justice, Washington, DC [with adjunct testimony from John C. Inglis, Deputy Director, National Security Agency, Washington, DC; Robert S. Litt, General Counsel, Office of the Director of National Intelligence, Washington, DC; and Sean M. Joyce, Deputy Director, Federal Bureau of Investigation, Washington, DC]	5
prepared statement	49
Inglis, John C., Deputy Director, National Security Agency, Washington, DC, prepared statement	54
Carr, Hon. James G., Senior Judge, U.S. District Court for the Northern District of Ohio, Toledo, Ohio	34
prepared statement	60
Jaffer, Jameel, Deputy Legal Director, American Civil Liberties Union Founda- tion, New York, New York	36
prepared statement	62
Baker, Stewart A., Partner, Steptoe & Johnson LLP, Washington, DC	37
prepared statement	85

QUESTIONS

Questions submitted by Senator Leahy for James M. Cole	101
Questions submitted by Senator Leahy for John C. Inglis	102
Questions submitted by Senator Leahy for Jameel Jaffer	104
Questions submitted by Senator Grassley for James M. Cole	105
Questions submitted by Senator Grassley for John C. Inglis	107
Questions submitted by Senator Grassley for Robert S. Litt	109
Questions submitted by Senator Grassley for Sean M. Joyce	111
Questions submitted by Senator Grassley for James G. Carr	114
Questions submitted by Senator Grassley for Jameel Jaffer	115
Questions submitted by Senator Grassley for Stewart Baker	118

QUESTIONS AND ANSWERS

Responses of James M. Cole to questions submitted by Senators Leahy and Grassley [NOTE: Some responses of James M. Cole are classified and therefore not printed as a part of this hearing.]	121
Responses of John C. Inglis to questions submitted by Senators Leahy and Grassley [NOTE: The responses of John C. Inglis are classified and there- fore not printed as a part of this hearing.]	125
Responses of Robert S. Litt to questions submitted by Senator Grassley	126
Responses of Sean M. Joyce to questions submitted by Senator Grassley	127
Responses of James G. Carr to questions submitted by Senator Grassley	131
Responses of Jameel Jaffer to questions submitted by Senators Leahy and Grassley	137
Responses of Stewart Baker to questions submitted by Senator Grassley	149

IV

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

	Page
Op Ed, "A Better Secret Court", <i>New York Times</i> , James G. Carr, July 22, 2013	159
Walton, Reggie B., Presiding Judge, U.S. Foreign Intelligence Surveillance Court, Washington, DC, July 29, 2013, letter	162
Group Coalition letter, July 30, 2013	192
Joint transparency letter, July 16, 2013	196
Zwillinger, Marc J., Founder, ZwillGen PLLC, statement	199
The Constitution Project, Virginia E. Sloan, President, July 30, 2013, letter	206
U.S. Department of Justice, February 2, 2011, letter	208
U.S. Department of Justice, December 14, 2009, letter	210

STRENGTHENING PRIVACY RIGHTS AND NATIONAL SECURITY: OVERSIGHT OF FISA SURVEILLANCE PROGRAMS

WEDNESDAY, JULY 31, 2013

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 9 a.m., in Room SH-216, Hart Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Feinstein, Durbin, Whitehouse, Klobuchar, Franken, Blumenthal, Grassley, Sessions, Cornyn, Lee, and Flake.

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

Chairman LEAHY. Good morning. Today, the Judiciary Committee will scrutinize Government surveillance programs conducted under the Foreign Intelligence Surveillance Act, or FISA. In the years since September 11th, Congress has repeatedly expanded the scope of FISA and has given the Government sweeping new powers to collect information on law-abiding Americans, and we must carefully consider now whether those laws may have gone too far.

Last month, many Americans learned for the first time that one of these authorities—Section 215 of the USA PATRIOT Act—has for years been secretly interpreted—secretly interpreted—to authorize the collection of Americans' phone records on an unprecedented scale. Information was also leaked about Section 702 of FISA, which authorizes the NSA to collect the communications of foreigners overseas.

Now, first, let me make it very clear. I do not condone the way these and other highly classified programs were disclosed, and I am concerned about the potential damage to our intelligence-gathering capabilities and national security. It is appropriate to hold people accountable for allowing such a massive leak to occur. We need to examine how to prevent this type of breach in the future.

In the wake of these leaks, the President said that this is an opportunity to have an open and thoughtful debate about these issues. And I welcome that statement because this is a debate that several of us on this Committee in both parties have been trying to have for years. Like so many others, I will get the classified briefings, but then, of course, you cannot talk about them. There are a lot of these things that should be and can be discussed. And

if we are going to have the debate that the President called for, the executive branch has to be a full partner. We need straightforward answers, and I am concerned that we are not getting them.

Just recently, the Director of National Intelligence acknowledged that he provided false testimony about the NSA surveillance programs during a Senate hearing in March, and his office had to remove a fact sheet from its website after concerns were raised about its accuracy. And I appreciate that it is difficult to talk about classified programs in public settings, but the American people expect and deserve honest answers.

It also has been far too difficult to get a straight answer about the effectiveness of the Section 215 phone records program. Whether this program is a critical national security tool is a key question for Congress as we consider possible changes to the law. Some supporters of this program have repeatedly conflated the efficacy of the Section 215 bulk metadata collection program with that of Section 702 of FISA, even though they are entirely different. Now, I do not think that is a coincidence when we have people in Government make that comparison, but it needs to stop. I think the patience of the American people is beginning to wear thin, but what has to be of more concern in a democracy is the trust of the American people is wearing thin.

I asked General Alexander—and I understand he cannot be here today because he is at a convention in Las Vegas, I guess for hackers. But I asked General Alexander about the effectiveness of the Section 215 phone records program at an Appropriations Committee hearing last month, and he agreed to provide a classified list of terrorist events that Section 215 helped to prevent, and I have reviewed that list. Although I agree that it speaks to the value of the overseas content collection implemented under Section 702, it does not do the same for Section 215. The list simply does not reflect dozens or even several terrorist plots that Section 215 helped thwart or prevent—let alone 54, as some have suggested.

These facts matter. This bulk collection program has massive privacy implications. The phone records of all of us in this room—all of us in this room—reside in an NSA database. I have said repeatedly that just because we have the ability to collect huge amounts of data does not mean that we should be doing so. In fact, it has been reported that the bulk collection of Internet metadata was shut down because it failed to produce meaningful intelligence. We need to take an equally close look at the phone records program. If this program is not effective, it has to end. And so far I am not convinced by what I have seen.

I am sure that we will hear from witnesses today who will say that these programs are critical in helping to identify and connect the so-called dots. But there are always going to be dots to collect, analyze, and try to connect. The Government is already collecting data on millions of innocent Americans on a daily basis based on a secret legal interpretation of a statute that does not on its face appear to authorize this kind of bulk collection. So what is going to be next? And when is enough enough?

I think Congress has to carefully consider the powerful surveillance tools that we grant to the Government. We have to ensure that there is stringent oversight, accountability, and transparency.

This debate should not be limited to those surveillance programs about which information was leaked. That is why I have introduced a bill that addresses not only Section 215 and Section 702, but also national security letters, roving wiretaps, and other authorities under the PATRIOT Act. As we have seen in the case of ECPA reform, the protection of Americans' privacy is not a partisan issue. I thank Senator Lee of Utah and others for their support of my FISA bill, and I hope other Senators will join that effort.

So I look forward to the testimony of the Government witnesses. I am particularly grateful for the participation of Judge Carr, a current member of the judiciary and a former judge of the FISA Court. I hope this will give us an opportunity for an open debate about the law, the policy, and the FISA Court process that led us to this position.

I yield first, of course, to Senator Grassley, and then we will call on the first panel with James Cole. We will put General Inglis' statement in the record. It did not arrive in time to be given, so his statement will be made part of the record and he will answer questions.

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

Chairman LEAHY. Senator Grassley.

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

Senator GRASSLEY. Mr. Chairman, I thank you for holding this hearing, and I think it is very important that Congress do its oversight work, which this hearing is part of. But it is even more important, the more secret a program, the more oversight that Congress has. And as you said, probably more about this program could be told to the public, and the more that could be told, maybe more understanding and less questioning on the part of the public.

The Foreign Intelligence Surveillance Act provides the statutory framework for electronic surveillance in the context of the foreign intelligence gathering. Investigating threats to our national security gives rise to a tension between the protections of citizens' privacy rights and the Government's legitimate national security interests. Congress through this legislation has sought—and I hope successfully—to strike a balance in this sensitive area, but whether it is the right balance, of course, is one of the reasons we are having this hearing.

The reports in the media have raised important questions regarding exactly what information about American citizens is being collected by the Government, whether the programs are being conducted as Congress intended, and whether there are sufficient safeguards to ensure that they cannot be abused by this or any future administration. In short, the reports have raised questions about whether the proper balance has been struck.

We need to look no further than the recent IRS scandal to see what can happen when an unchecked executive branch bureaucracy with immense power targets political opponents. These actions trampled many citizens' most basic rights to fully participate in our democratic process. This kind of abuse cannot be permitted to occur

in our national security agencies as well, and maybe even more importantly.

Oversight by Congress will play an important role as we move forward in evaluating the wisdom and value of the intelligence programs. However, Congress needs accurate information in order to conduct oversight responsibilities that the Constitution demands that we do under our checks and balances of Government. That is why it was especially disturbing to see that the Director of National Intelligence was forced to apologize for inaccurate statements he made last March before the Senate Intelligence Committee. Those statements concerned one of the very important programs that we will be hearing about this very day. Nothing can excuse this kind of behavior from a senior administration official of any administration, especially on matters of such grave importance.

We have a constitutional duty to protect Americans' privacy. That is a given. We also have an equal constitutional responsibility to ensure that the Government provides a strong national defense. That is a given. Intelligence gathering is, of course, a necessary and vital part of that defense. We have a duty to ensure that the men and women of our military, our intelligence, and our counterterrorism communities have the tools that they need to get the job done.

I understand officials contend that the programs authorized under FISA that we will discuss today are critical tools that have assisted them in disrupting attacks both here and abroad. To the extent that possible in this unclassified setting, I look forward to hearing how these programs have made our Nation safer.

I want to emphasize that this is an equally important part of the balance that we have to strike. And as we consider whether reform of these intelligence programs is necessary or desirable, we must also make sure that we do not overreact and repeat the mistakes of the past.

We know that before 9/11 there was a wall erected under the Clinton administration between intelligence gathering and law enforcement. That wall contributed to our failure to be able to connect the dots and prevent 9/11. None of the reforms that we consider should effectively rebuild that wall.

Additionally, while the intelligence and the law enforcement communities need to share information in a lawful way, any reform we consider should not confuse the differences between these two contacts.

For example, no reform should be based on the misguided legal theory that foreign terrorists on foreign soil are entitled to the same constitutional rights that Americans expect here at home.

Finally, increased transparency is a worthy goal in general, and as I suggested before, whenever we can talk about these programs, I think there are less questions out there in the minds of people, and we have probably created some public relations problems for us and for this program and for our national security community because maybe we have not made enough information available. I say that understanding that we cannot tell our enemies what tools we use.

But if we consider any reform that may bring more transparency to the FISA process, we should keep in mind then that every piece of information we make available to the public will be read by a determined adversary, and that adversary has already demonstrated the capacity to kill thousands of Americans even on our own soil.

I welcome the panel witnesses and look forward to engaging them as we seek to strike the difficult and sensitive balance between privacy and security.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Our first witness will be James Cole. He first joined the Department of Justice in 1979. He served for 13 years in the Criminal Division, later becoming the Deputy Chief of the Division's Public Integrity Section. He went into private practice, sworn in as Deputy Attorney General on January 3, 2011. Of course, Mr. Cole is no stranger to this Committee.

Please go ahead, sir.

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

Mr. COLE. Thank you, Mr. Chairman, Mr. Ranking Member, and Members of the Committee, for inviting us here today to speak about the 215 business records program and Section 702 of FISA. With these programs and other intelligence activities, we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties. We believe these two programs have achieved the right balance.

First of all, both programs are conducted under public statutes passed and later reauthorized by Congress. Neither is a program that has been hidden away or off the books. In fact, all three branches of Government play a significant role in the oversight of these programs. The judiciary—through the Foreign Intelligence Surveillance Court—plays a role in authorizing the programs and overseeing compliance; the executive branch conducts extensive internal reviews to ensure compliance; and Congress passes the laws, oversees our implementation of those laws, and determines whether or not the current laws should be reauthorized and in what form.

Let me explain how this has worked in the context of the 215 program. The 215 program involves the collection of metadata from telephone calls. These are telephone records maintained by the phone companies. They include the number the call was dialed from, the number the call was dialed to, the date and time of the call, and the length of the call. The records do not include the names or other personal identifying information, they do not include cell site or other location information, and they do not include the content of any phone calls. These are the kinds of records that under longstanding Supreme Court precedent are not protected by the Fourth Amendment.

The short court order that you have seen published in the newspapers only allows the Government to acquire the phone records; it does not allow the Government to access or use them. The terms

under which the Government may access or use the records is covered by another, more detailed court order that the DNI declassified and released today. That other court order, called the “primary order,” provides that the Government can only search the data if it has a “reasonable, articulable suspicion” that the phone number being searched is associated with certain terrorist organizations. The order also imposes numerous other restrictions on NSA to ensure that only properly trained analysts may access the data and that they can only access it when the reasonable, articulable suspicion predicate has been met and documented. The documentation of the analyst’s justification is important so that it can be reviewed by supervisors before the search and audited afterwards to ensure compliance.

In the criminal context, the Government could obtain the same types of records with a grand jury subpoena, without going to the court. But here, we go to the court every 90 days to seek the court’s authorization to collect the records. In fact, since 2006, the court has authorized the program on 34 separate occasions by 14 different judges. As part of that renewal process, we inform the court whether there have been any compliance problems, and if there have been, the court will take a very hard look and make sure we have corrected those problems. As we have explained before, the 11 judges on the FISA Court are far from a rubber stamp; instead, they review all of our pleadings thoroughly, they question us, and they do not approve an order until they are satisfied that we have met all statutory and constitutional requirements.

In addition to the judiciary, Congress also plays a significant role in this program. The classified details of this program have been extensively briefed to both the Judiciary and Intelligence Committees and their staffs on numerous occasions. If there are any significant issues that arise with the 215 program, we would report those to the two Committees right away. Any significant interpretations by the FISA Court would likewise be reported to the Committees under our statutory obligations, including opinions of any significant interpretation, along with any of the court orders that go with that.

In addition, Congress plays a role in reauthorizing the provision under which the Government carries out this program and has done so since 2006. Section 215 of the PATRIOT Act has been renewed several times since the program was initiated—including most recently for an additional 4 years in 2011. In connection with those recent renewals, the Government provided a classified briefing paper to the House and Senate Intelligence Committees to be made available to all Members of Congress. The briefing paper and a second updated version of it set out the operation of the programs in detail, explained that the Government and the FISA Court had interpreted the Section 215 authorization to authorize the bulk collection of telephone metadata, and stated that the Government was, in fact, collecting such information. The DNI also declassified and released those two papers today.

We also made offers to brief any member on the 215 program, and the availability of the paper and the opportunity for oral briefings were communicated through “Dear Colleague” letters issued by the Chairs of the Intelligence Committees to all Members of

Congress. Thus, although we could not talk publicly about the program at the time—since it was properly classified—the executive branch took all reasonably available steps to ensure that Members of Congress were appropriately informed about the programs when they renewed it.

I understand that there have been recent proposals to amend Section 215 authority to limit the bulk collection of telephone metadata. As the President has said, we welcome a public debate about how best to safeguard both our national security and the privacy of our citizens. Indeed, we will be considering in the coming days and weeks further steps to declassify information and help facilitate that debate, just as we have done this morning in releasing the primary order and the congressional briefing papers. In the meantime, however, we look forward to working with the Congress to determine in a careful and deliberate way what tools can best be structured and secured to secure the Nation and at the same time protect our privacy and civil liberties.

Thank you, Mr. Chairman.

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

Chairman LEAHY. I think we can—the debate you speak of is starting now. The administration did declassify a FISC order. Of course, it does not contain any real legal analysis or discussion of the 215 relevance standard, so that will be part of our questions. But first I want to ask Deputy Director Inglis a question before we even go into the legality and usefulness of this.

We had a huge security breach, I think we will all agree, committed by Edward Snowden. And a few years ago, Bradley Manning downloaded hundreds of thousands of classified and sensitive documents and passed them on to WikiLeaks.

Now, if two data breaches of this magnitude had occurred in the private sector, somebody would have been held accountable by now. There is a lot of material kept in the private sector, trade secrets and so on. If they allowed this kind of leaking going on, in most companies somebody would be held accountable.

Who at the NSA has taken responsibility for allowing this incredibly damaging security breach to occur?

Mr. INGLIS. Well, sir, that accountability must be considered at at least two levels: one, at the individual level, we have to take a hard look to see whether individuals exercised their responsibilities appropriately, whether they exercised due diligence in the exercise of those responsibilities—

Chairman LEAHY. Well, obviously there was not. I mean, if a 29-year-old school dropout could come in and take out massive, massive amounts of data, it is obvious there were not adequate controls. Has anybody been fired?

Mr. INGLIS. No, sir, not yet.

Chairman LEAHY. Has anybody been admonished?

Mr. INGLIS. Sir, those investigations are underway. When those investigations are complete, we will have a full accounting within the executive branch and to the Congress of individual and systemic accountability. I think that at the end of the day we will have to look to see whether people exercised the responsibilities ap-

propriately, whether they essentially exercised the trust that is accorded to them.

In our system we extend top secret SCI, special compartmented intelligence clearances to a range of people and expect that they will then exercise that trust as the American people intended. And we will make a full accounting of that.

Chairman LEAHY. I remember President Reagan made up a statement, which many of us use, about trust, but verify. Don't you have—I realize you have to act with a certain amount of trust, but don't you have people double-checking what somebody is doing?

Mr. INGLIS. We do, sir. And—

Chairman LEAHY. Who double-checked Mr. Snowden?

Mr. INGLIS. Well, there are checks at multiple levels. There are checks in terms of what an individual might be doing at any moment in time. There are—

Chairman LEAHY. They obviously failed.

Mr. INGLIS. In this case, I think we can say that they failed, but we do not yet know where.

Chairman LEAHY. You “think” you can say they failed. I mean, he is sitting over at the airport in Russia with millions of items.

Mr. INGLIS. I would say that with the benefit of what we now know, they did fail.

Chairman LEAHY. Okay.

Mr. INGLIS. But we do not yet know where precisely they failed, and we may find that they failed at multiple points in the system, either in the exercise of individual responsibility or in the design of the system in the first place.

Chairman LEAHY. Has anybody offered—been asked to resign or offered to resign because of this failure?

Mr. INGLIS. No one has offered to resign. Everyone is working hard to understand what happened and to put in place the necessary mechanisms to—

Chairman LEAHY. How soon will we know who screwed up?

Mr. INGLIS. I think that we will know over weeks and months precisely what happened and who should then be held accountable, and we will hold them accountable.

Chairman LEAHY. Are you taking any steps now to make sure such a screw-up does not happen again?

Mr. INGLIS. We are, sir. We have instituted a range of mechanisms, not simply one, to ensure that we would understand and immediately be able to catch someone who tried to repeat precisely what Mr. Snowden did. But we also have to be creative and thoughtful enough to understand that there are many other ways somebody might try to beat the system.

Chairman LEAHY. You can understand why some people would use that old expression, “locking the door after the horse has been stolen.”

Mr. INGLIS. I can, sir.

Chairman LEAHY. Okay. Thank you. I appreciate your candor. And I realize General Alexander is in Las Vegas, but I will ask you this question: Last month, he promised to provide me with specific examples of terrorism cases where Section 215 phone records collections had been used. I was led to believe by his answer that there were dozens of cases where Section 215 authority has been

critical to the discovery and disruption of terrorist plots. I have now reviewed all the classified material that the NSA sent, and I am far from convinced. The document is classified, but what was said in open testimony is that Section 215 helped to thwart or prevent 54 terrorist plots. Not by any stretch can you get 54 terrorist plots.

In how many cases was Section 215 bulk phone records collection critical to preventing a terrorist plot?

Mr. INGLIS. Sir, I might answer in open session and then offer to provide follow-up details in a classified session.

I would say that the administration has disclosed that there were 54 plots that were disrupted over the life of these two programs—

Chairman LEAHY. Section 215 was critical to preventing—

Mr. INGLIS. No, sir. And of those—

Chairman LEAHY [continuing]. Fifty-four plots?

Mr. INGLIS. And of those plots, 13 of those had a homeland nexus. The others had essentially plots that would have come to fruition in Europe, Asia, other places around the world.

Chairman LEAHY. How many of those—

Mr. INGLIS. Of the 13—

Mr. INGLIS. Of the 13—

Chairman LEAHY. How many of those 13 were plots to harm Americans?

Mr. INGLIS. Of the 13 that would have had a homeland nexus, in 12 of those 215 made a contribution. The question you have asked, though, is more precise in the sense of is there a “but for” case to be made, that but for 215 those plots would have been disrupted. That is a very difficult question to answer inasmuch as that is not necessarily how these programs work. That is actually not how these programs work.

What happens is that you essentially have a range of tools at your disposal. One or more of these tools might tip you to a plot. Others of these tools might then give you an exposure as to what the nature of that plot is. And, finally, the exercise of multiple instruments of power, to include law enforcement power, ultimately completes the picture and allows you to interdict that plot.

There is an example amongst those 13 that comes close to a “but for” example, and that is the case of Basaaly Moalin.

Chairman LEAHY. I have read that. I have read the material on that. It would be safe to say there are not 54 “but fors”?

Mr. INGLIS. It is safe to say that, sir.

Chairman LEAHY. That is not right—

Mr. INGLIS. This capability, the 215 collection of metadata, is focused on the homeland. It is focused on detecting plots that cross the foreign to homeland domain.

Chairman LEAHY. But it was not—

Mr. INGLIS. Given that only 13 of those plots—

Chairman LEAHY. But it was not a “but for” in 54 cases?

Mr. INGLIS. It was not, sir.

Chairman LEAHY. Thank you.

Mr. INGLIS. Given that only 13 of those plots had a homeland nexus, it, therefore, only had its principal opportunity to make a contribution in 13 or less. In fact, it made a contribution to a plot

that was disrupted overseas. I think that shows that this actually is looking not simply at the homeland, but it is looking at the foreign-homeland nexus.

Chairman LEAHY. And I hope we are not mixing up 215 with other sections.

Mr. INGLIS. We try hard not to do that, sir. They are distinguished but complementary tools.

Mr. JOYCE. Mr. Chairman, if I might add some insight to the value of 215?

Chairman LEAHY. My time is up, but go ahead. If that is okay with you?

Senator FEINSTEIN. Can't they make statements?

Chairman LEAHY. Go ahead, Mr. Joyce. No, they are just here to help.

Go ahead, Mr. Joyce.

Mr. JOYCE. I just want to add, as you mentioned before, you know, how many dots do we need? I think we need to frame this by understanding who the adversary is and what they are trying to do. And they are trying to harm America. They are trying to strike America. And what we need is we need all these tools.

So you mentioned the value of 702 versus the value of business records 215. They are different. And I make the analogy like a baseball team. You have your most valuable player, but you also have the players that hit singles every day.

Chairman LEAHY. Mr. Joyce—

Mr. JOYCE. I just want to relate to the homeland plots. So in Najibullah Zazi, in the plot to bomb the New York subway system, business record 215 played a role. It identified specifically a number we did not previously know of—

Chairman LEAHY. It was a critical role?

Mr. JOYCE. What I am saying, it plays a different—

Chairman LEAHY. Wasn't it some undercover work that took place in there?

Mr. JOYCE. Yes, there was some undercover work. But what I am saying, each tool plays a different role, Mr. Chairman. I am not saying that it is—

Chairman LEAHY. Wasn't the FBI—

Mr. JOYCE [continuing]. The most important tool—

Chairman LEAHY. Wasn't the FBI already aware of the individual in contact with Zazi?

Mr. JOYCE. Yes, we were, but we were not aware of that specific telephone number, which NSA provided us.

Chairman LEAHY. The only reason I go down this, you know, if we did everything, for example, we could have more security if we strip-searched everybody who came into every building in America. We are not going to do that. We would have more security if we closed our borders completely to everybody. We are not going to do that. If we put a wiretap on everybody's cell phone in America, if we search everybody's home—but there are certain things, certain areas of our own privacy that we Americans expect. And at some point you have to know where the balance is. But I have gone into other people's time. Senator Grassley.

Senator GRASSLEY. Would you, Mr. Chairman, clarify for me the process? We have had the testimony now, so we—

Chairman LEAHY. Yes.

Senator GRASSLEY [continuing]. Ask questions of all the people?

Chairman LEAHY. That is right—well, we were going to have questions of Mr. Cole and Mr. Inglis, but Mr. Litt and Mr. Joyce are here to be able to add if anything is necessary.

Senator GRASSLEY. Sure. Okay.

Chairman LEAHY. Thank you.

Senator GRASSLEY. I will start out with Mr. Cole, and my questions are kind of to emphasize, to inform, and to even be repetitive, because I think the public needs a greater understanding of what we are up to here.

There are two legal authorities that we are discussing here: one, Section 702 authority. That one I am going to lay aside. The other authority is Section 215. Many Americans are concerned about the scope there. They fear that the Government is spying on them and prying into their personal lives. I ask questions to make absolutely sure that I understand the scope of 215.

The first question: What information does the Government collect under this program? And specifically is anyone's name, address, Social Security number, or location collected?

Mr. COLE. Senator Grassley, first, to answer the second part, name, address, location, Social Security number is not collected under the 215 program at all.

Senator GRASSLEY. Okay.

Mr. COLE. Never has been, never will be.

Second, the nature of the collection is really very dependent on this reasonable, articulable suspicion. While a lot of metadata does exist in a database, it cannot be accessed unless you go through the procedures of documenting that there is reasonable, articulable suspicion that the phone number you want to ask about is associated with terrorists. Unless you get that step made, you cannot enter that database and make a query and access any of those data.

Senator GRASSLEY. Okay. Again, for emphasis, is the Government listening in on any American phone calls through this program? And let me say that I just heard within the last week on some news media that somebody is declaring that any bureaucrat someplace in some intelligence agency can pick up the phone and listen to the conversation.

Mr. COLE. Nobody is listening to anybody's conversations through this program, and through this program nobody could. No information like that is being collected through this program.

Senator GRASSLEY. Mr. Litt, Section 215 contains a requirement that records collected under the program provision be "relevant to an authorized investigation." As a legal matter, how can you justify the assertion that phone records of millions of Americans who have nothing to do with terrorism are relevant to an authorized investigation under Section 215?

Mr. LITT. So I would begin by noting that a number of judges repeatedly over the years have found that these records are, in fact, relevant. The reason is that the standard of relevance that we are talking about here is not the kind of relevance that you think about in the Perry Mason sense of a criminal trial. It is a much broader standard of relevance, and in a number of circumstances in the

law, such as grand jury subpoenas or civil discovery, it is a well-accepted concept that if you need to get a large group of records in order to find a smaller group of records that actually provides the information you need to move forward, the larger group of records can be relevant. That is particularly true in this case because of the kinds of controls that the Deputy Attorney General mentioned, the fact that the queries are limited, the access to the data is limited, and for that reason the FISA Court has repeatedly found that these records are relevant.

Senator GRASSLEY. Is there any legal precedent that supports such a broad definition of relevance to an investigation?

Mr. LITT. I would actually defer that to the Deputy Attorney General.

Senator GRASSLEY. Okay.

Mr. COLE. Well, the legal precedent comes from the history of all the orders that have been issued, the courts having looked at this under the FISA law and under the provisions of 215 and making sure that under the provisions and the ability to get these records relevant to a criminal—or, rather, a foreign intelligence—investigation, they have gone through, the law that Mr. Litt has described on, as I said, I believe 34 different occasions to do this analysis. So that legal precedent is there.

Senator GRASSLEY. Okay. Mr. Joyce, one part of the balance that we have to strike protecting privacy of Americans, the other part national security. Thankfully, until the Boston bombing we had prevented large-scale terrorist attacks on American soil. I have a few questions about how valuable the role of Section 215 and 702 programs have played in predicting our national security, two questions, and then I will have to stop and go to our colleagues.

Can you describe any specific situations where Section 215 and Section 702 authorities helped disrupt a terrorist attack or identify individuals planning to attack, the number of times? And then, second, if you did not have the authority to collect phone records in the way that they are now under Section 215, how would you have effected those investigations?

Mr. JOYCE. So your first question, Senator, as far as a specific example of when we have utilized both of these programs is one I first mentioned, the first al Qaeda-directed plot since 9/11 in September 2009 when Najibullah Zazi and others conspired to plot to bomb the New York subway system. We initially found out about Zazi through an NSA 702 coverage, and he was actually talking to an al Qaeda courier who was—he was asking for his help to perfect an explosives recipe. So but for that, we would not have known about the plot. We followed that up with legal process and then had FISA coverage on him and others as we fully investigated the plot.

Business records 215 was also involved, as I had previously mentioned, where we also through legal process were submitting legal process for telephone numbers and other e-mail addresses, other selectors, but NSA also provided another number we were unaware of a co-conspirator, Adis Medunjanin. So that is an instance where a very serious plot to attack America on U.S. soil that we used both these programs.

But I say, as Chairman Leahy mentioned, there is a difference in the utility of the programs. But what I say to you is that each and every program and tool is valuable. There were gaps prior to 9/11, and what we have collectively tried to do, the members of the committee, other members of the other oversight committees, the executive branch, and the intelligence community, is we have tried to close those gaps and close those seams. And the business record 215 is one of those programs that we have closed those seams.

So I respectfully say to the Chairman that the utility of that specific program initially is not as valuable. I say you are right. But what I say is it plays a crucial role in closing the gaps and seams that we fought hard to gain after the 9/11 attacks.

As you mentioned, another instance when we used the business record 215 program, as Chairman Leahy mentioned, Basaaly Moalin. So initially the FBI opened a case in 2003 based on a tip. We investigated that tip. We found no nexus to terrorism and closed the case.

In 2007, the NSA advised us through the business record 215 program that a number in San Diego was in contact with an Al-Shabaab, an al Qaeda East Africa member in Somalia. We served legal process to identify that unidentified phone number. We identified Basaaly Moalin. Through further investigation we identified additional co-conspirators, and Moalin and three other individuals have been convicted and some pled guilty to material support to terrorism.

So I go back to we need to remember what happened in 9/11, and everyone in this room remembers where they were and what happened—

Chairman LEAHY. Mr. Joyce, you are stating the obvious there. Be specific to it because we are going to have votes on the floor, and it is going to take us out of here. We would like to keep somewhat close to the time.

Mr. JOYCE. All I will say, Mr. Chairman, is, respectfully, you mentioned about the dots. We must have the dots to connect the dots.

Chairman LEAHY. Thank you. One of the advantages of this Committee, the members on both sides of the aisle bring a lot of different abilities and various areas of expertise.

The next witness is the Chair of the Senate Intelligence Committee.

Senator FEINSTEIN. Am I a witness here?

Chairman LEAHY. The next witness? The next questioner is the Chair of the Senate Intelligence Committee, Senator Feinstein, and it is a great advantage to us to have her on this Committee.

Senator FEINSTEIN. Well, thank you very much. Thank you very much, Mr. Chairman.

I would like to begin by putting a couple of letters in the record. These have just been declassified. The first is a letter to myself and Senator Chambliss on February 2, 2011, before this program came up before the Senate, explaining it, making the information available. The second is that same letter to the House, so we have before 2010 and 2011. I would also—

Chairman LEAHY. Without objection, they will be made part of the record.

Senator FEINSTEIN. Thank you.

[The letters appear as a submission for the record.]

Senator FEINSTEIN. I would also like to—I just realized that I believe Mr. Inglis' statement makes public for the first time a fact, and it is an important fact. It is on page 4 of his letter, and what he points out I think Mr. Cole described, that the query, which is the search of the database, can only be done on reasonable, articulable suspicion and only 22 people have access to that, trained and vetted analysts at the NSA.

If the numbers are run and it looks like there is a problem, the report is made to the FBI. And the FBI looks at it, and if they want to collect content, they must get a probable cause warrant from the Foreign Intelligence Surveillance Court.

Let me quote: “. . . in 2012, based on those fewer than 300 selectors”—that is, queries, which actually were 288 for Americans—“we provided a total of 12 reports to FBI, which altogether ‘tipped’ less than 500 numbers.”

So what you are saying, if I understand it, Mr. Inglis, is that, maximum, there were 12 probable cause warrants. Is that correct?

Mr. INGLIS. I think in truth, any one of the numbers that were tipped could have led the FBI to develop probable cause on more than 12. But there were only 12 reports provided to the FBI across 2012, and there were less than 500 numbers in those reports collectively that were tipped to the FBI in 2012.

Senator FEINSTEIN. Let me ask Mr. Joyce this question. Can you tell us how many orders—how many probable cause warrants were issued by the FBI in 2012?

Mr. JOYCE. I cannot off the top of my head, Senator. I can get you those numbers, though, following the hearing.

Senator FEINSTEIN. Well, I think we would appreciate that. I think—

Mr. JOYCE. I would just add, though, you make a very good point. Whether it is the 702 program or the business record 215, once that information is passed to us involving anyone in the United States, we must go to the FISC, the Foreign Intelligence Surveillance Court, and show probable cause on the FISC warrant basically to provide content or whatever as far as overhears for that specific individual.

Senator FEINSTEIN. Good.

[The information referred to appears as a submission for the record.]

Senator FEINSTEIN. Now, the NSA has produced and declassified a chart, which I would like to make available to all members. It has the 54 total events. It includes Section 702 authority and Section 215 authority, which essentially work together. And it shows the events disrupted based on a combination of these two programs: 13 in the homeland, 25 in Europe, 5 in Africa, and 11 in Asia.

Now, I remember, I was on the Intelligence Committee before 9/11, and I remember how little information we had. And the great criticism of the Government because of these stovepipes, the inability to share intelligence, the inability to collect intelligence, we had no program that could have possibly caught two people in San Diego before the event took place.

I support this program. I think based on what I know, they will come after us, and I think we need to prevent an attack wherever we can from happening. That does not mean that we cannot make some changes.

Yesterday at the Intelligence Committee, I outlined some changes that we might consider as part of our authorization bill, and let me quickly run through them: the number of American phone numbers submitted as queries on a regular basis annually from the database; the number of referrals made to the FBI each year based on those queries, and how many times the FBI obtains probable cause warrants to collect the content of a call, which we now know is very few times, relatively; the number of times that a company—this is at their request from the high-tech companies—that any company is required to provide data pursuant to FISA’s business records provision.

As you know, the companies who provide information are seeking to be able to speak more publicly about this, and I think we should. There are some changes we can make to the business records section. We are looking at reducing the 5-year retention period that NSA keeps phone records in its database down to 2 or 3 years. It is my understanding that the usefulness of it tails off as the years go on. We have to determine that point and then consider it.

And requiring the NSA to send to the FISA Court for its review the records of each query of the database as soon as it is practicable so the Court can determine the propriety of the query under the law.

These are things that can be done to increase transparency, but not to stop the program. I believe based on what I have seen—and I read intelligence regularly—that we would place this Nation in jeopardy if we eliminated these two programs.

Thank you, Mr. Chairman.

Mr. LITT. Mr. Chairman, may I just offer a brief response to that?

Chairman LEAHY. Just a moment, and then I will. Would you also include reporting how often NSA or anybody else goes into an individual’s browsing history or their e-mails or social media activity?

Senator FEINSTEIN. Sure, right. And we could do that in the private sector, too, how often this happens.

Chairman LEAHY. I was just looking at this article in the Guardian today, which may or may not be accurate.

Mr. Litt, you wanted to say something?

Mr. LITT. Yes, thank you. I just wanted to say that I think that this administration is more or less in the same place that Senator Feinstein is. We are open to reevaluating this program in ways that can perhaps provide greater confidence and public trust that this is, in fact, a program that achieves both privacy protections and national security. And, in fact, the White House has directed the Director of National Intelligence to make recommendations in that area. So we will be looking forward to working with your Committee and this Committee to see whether there are changes that can be made that are consistent with preserving the essence of the program and yet provide greater public confidence.

Chairman LEAHY. Thank you. Senator Cornyn? Again, speaking of the diversity we have, Senator Cornyn, of course, is the Deputy Republican Leader, and we appreciate the amount of time he spends in this Committee.

Senator CORNYN. Mr. Chairman, thank you for having this hearing, and thanks to each of the witnesses for your service to our country.

Those of us who have been here for a little while and through the evolution of these programs have, I think, learned more than the public generally knows about how they operate, and I think that has helped give us confidence in what is occurring. But I am also sensitive to Senator Feinstein, the distinguished Chair of the Senate Intelligence Committee, some of her observations—and Mr. Litt I think reiterated that, too—about the importance of maintaining public confidence in classified programs, which is a tough thing to do.

But I think I am also reminded of the fact that, since 2007, we have 43 new members of the U.S. Senate, and so there have been some people who have come to the Senate in recent years who perhaps have not been able to observe through their regular work some of the development of these programs, and so I think a hearing like this and the other hearings that you have participated in that I have attended have been very important to giving everyone a foundation of information where they can have confidence on behalf of the people we represent.

But I would like to ask, maybe starting with Mr. Cole and go down the line, to get your reaction to the criticism made of the operations of the Foreign Intelligence Surveillance Court made by former Intelligence Surveillance Court Judge James Robertson. And this really has to do with the nature of essentially *ex parte* proceedings before the Court. I know that when it comes to individualized, particularized warrants, it is common in our system to have essentially *ex parte* proceedings. But here, when the Foreign Intelligence Surveillance Court is authorizing a program, according to Judge Robertson, under this expanded jurisdiction, it has turned the Court into something of an administrative agency. And, of course, talking again about public confidence in the oversight of the Court, which I think is an important part of maintaining that confidence, whether you think there might be some advantage, as Senator Blumenthal and I have discussed informally, having more of an adversarial process. My experience and I trust your experience with the adversarial process in our courts is it usually produces more information that allows the judge to make a better decision. And I would just like to get your reaction, Mr. Cole, and perhaps go down the line.

Mr. COLE. Thank you, Senator. First of all, I can tell you from the practice we have before the FISA Court that it is far more than just another administrative agency. They push back hard, and they make sure that they are the guardians of the law and the Constitution.

The topic of having an adversary—that is one that we are in the process of discussing and I know is being discussed in the Senate and in the House, and it is one of those areas that I think is part of the debate that we should be having on how best to do this.

There are obviously issues we will have to work through as to clearances and classifications and who would be there and what their role would be and things of that nature if there is going to be a practical way to do it. But those are the kinds of discussions I think we do need to have.

As you pointed out, it is not the usual course, and in the criminal law context we have many search warrants, Title III surveillance warrants that come in, that are not done in an adversary way. But this is certainly part of what we would like to be talking about and see if this has some utility.

Senator CORNYN. Thank you.

Mr. Inglis, do you have anything to add?

Mr. INGLIS. My background is largely operational, not in the training of the law, but that said, I am more than mindful of the absolute obligation to ensure that these things are done fully consistent with the Constitution. We welcome any and all hard questions. Whether that comes from an adversarial process or the process we enjoy, we think that we should be held accountable to answer those questions and ensure that the authorities that we are granted supports the whole of the Constitution, not just the defense of national security but the defense of civil liberties.

Senator CORNYN. Thank you.

Mr. Litt.

Mr. LITT. The only point that I would like to make from the perspective of the intelligence community is to note that we already—this is an unusual process to have the Court involved in an essentially executive branch activity, conduct of foreign intelligence. I do not know of any other nation in the world that has the degree of judicial supervision of intelligence activities that this country has already. And I think that to some extent people have a—make a mistaken analogy when they hear the term “court” and they think of this as an adversary proceeding, like a criminal trial or a civil trial. The question is: What is the best way to ensure that our intelligence programs are conducted in compliance with the law and with adequate protection for people’s privacy and civil liberties? And if it would help to have some sort of adversary process built into that, I think that would be entirely appropriate. But we should not be trying to make this mimic a criminal trial because it is a very different process.

Senator CORNYN. Mr. Joyce, do you have anything to add?

Mr. JOYCE. No. My background is operational, so I would defer to my lead attorney, the Deputy Attorney General.

Senator CORNYN. Okay. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

I hope, Mr. Litt, you are not saying that we have something that is very unusual, that we have something that can collect data on U.S. citizens, that you are not saying the Court should not be involved.

Mr. LITT. No, no. I am not saying that.

Chairman LEAHY. I just want to make sure.

Mr. LITT. I am not saying that at all.

Chairman LEAHY. Thank you.

Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you to our witnesses. As a former prosecutor, I have long believed that our laws must strike the right balance between protecting our civil liberties and protecting our national security.

I think most Americans, I will say, did not expect the sweeping nature of the surveillance programs, and for that reason I think this opportunity to reexamine these programs to see if there are ways we can ensure that they are more transparent and accountable without sacrificing the benefits they provide to national security is very important. And I just got this order, the Court order, Mr. Cole, that was just hot off the presses here. And could you—you said in your earlier testimony, you talked about the metadata, which I assume is just the collected data we have been hearing about on domestic phone calls, which is not the phone conversation itself. And then you go down to a Category 2, which must be when you are investigating parts of that metadata, which is based on this order; and then Category 3—this is how I am thinking of it in terms of circles—would be when you would actually get a court order to start investigating a person. Is that a fair way to look at this?

Mr. COLE. I think that is a very good way of looking at it—and the word you used I think is important here, the surveillance that is being done—because the only thing we are actually involved in surveiling are these much smaller groups that we have reasonable, articulable suspicion for. We are not surveiling everything that is in the database. You have to go through some very specific requirements that are contained in that order before you can surveil.

Senator KLOBUCHAR. In this order—and you said it would be—there has to be a reasonable suspicion that it is a terrorist. That is what you said earlier?

Mr. COLE. Reasonable suspicion that is relevant to an investigation of certain terrorist organizations.

Senator KLOBUCHAR. Okay. And so is there a percentage of that data that, you know, you look at when you get to the big metadata, then you go down to the next category, what percentage of the metadata is the next category that is based on this order?

Mr. COLE. I think it is hard to really quantify. I have heard numbers anywhere from 0.0001 percent of that metadata. It is a very, very tiny fraction of the metadata that actually is accessed and—

Senator KLOBUCHAR. And then when you go down to the part there where you are actually investigating someone or you get a special court order to look into it, what percentage is that?

Mr. COLE. That is then even smaller, because we then have to have probable cause to believe that those people are falling within the requirements of the Foreign Intelligence Surveillance Act.

Senator KLOBUCHAR. Okay. So given how small this is, is there no way of limiting the breadth of the data and information collected under the program that would not have adverse effects on our ability to effectively monitor national security threats?

Mr. COLE. Well, this is what we are looking at right now and trying to work through. As Chairman Feinstein had noted, she has made some recommendations. We are in the process of looking through that process to see if there are other ways to go about doing this where we still preserve the effectiveness of the operation

and try to limit whatever kind of privacy and civil liberties intrusions that come from that.

Senator KLOBUCHAR. Very good. And I know one idea that General Alexander suggested is that he is open to the idea of telecommunications companies holding the records rather than having the NSA collect them, although we know we still have that issue of telephone immunity anyway, as long as the Government could get access.

Mr. Inglis, do you want to testify about that and answer that? Do you think that is a viable alternative? It seems to me that we may have to do more than that.

Mr. INGLIS. So I think there are multiple implementations that could work. I think that we need to score all of those implementations against a set of criteria, which would include at the top that they do provide protections for privacy and civil liberties, but they also need to have sufficient breadth to your question, that if you ask a question of this database, let us say you have the situation we had with Basaaly Moalin, we have a number from East Africa al Qaeda that we have reasonable suspicion is associated with a plot against the homeland, you want to check to see whether there is, in fact, a connection into the homeland. You need sufficient breadth in the database that you are about to query to have confidence that if you come away with no response, that you can take that as confidence there is not a plot; or that if you get a response, you have found it, whether it is in any particular location in the world. So the breadth is important.

But I think that we can take a look at whether this is stored at the provider so long as you have some confidence you can do this in a timely way. We need to sometimes disrupt an operation that is in play, that is in progress, and so seconds, hours matter.

There might be other situations where you have the time to perhaps take more time, but we will have to think our way through whether the providers can meet that standard. I think there are technical architectures where they can.

Finally, to the question that Senator Feinstein has asked, a very thoughtful question, do we need to hold these records for 5 years? Our experience has shown that intelligence, writ large, tends to have a significant tail-off at 5 years, but there is a knee in the curve that might live at 2 years or 3 years. We need to base it upon data with a rearward look, take a hard look at that and determine how long these things really are necessary and beyond that how long they are valuable.

Senator KLOBUCHAR. And one quick question at the end here, Mr. Cole. Now that this Court order has been declassified, is there effort underway to declassify some of the legal rationale behind it?

Mr. COLE. We are still working on trying to declassify a number of things in this area. We are trying to get as much as we can out, obviously balancing the national security concerns with those released. But our goal is to try and get out as much information as we can to provide transparency on this.

Senator KLOBUCHAR. Thank you very much.

Chairman LEAHY. Senator Sessions.

Senator SESSIONS. Thank you all very, very much. Let me ask this, Mr. Litt. With regard to Mr. Joyce's comments about a certain

case that they were able to interdict and stop, dealing with the subway matter, he said that the collection of data under this program played a role in the successful culmination of that case.

Just fundamentally, you were Deputy Attorney General under Janet Reno for 6 years in the Department of Justice. You were a member of the ABA's Criminal Justice Committee. You have studied these issues and are required to make sure that laws are followed. But is this what was done in that case? Does it violate the Constitution in any way as defined by U.S. case law and the words of the Constitution itself?

Mr. LITT. So, first, I thank you for the promotion, but I never actually served as Deputy Attorney General. I had a couple of positions in the Department, but—

Senator SESSIONS. You were Deputy Assistant—

Mr. LITT. Deputy Assistant Attorney General.

Senator SESSIONS. We have to get all these Assistant Deputies and Deputy Assistants straight. Excuse me.

Chairman LEAHY. I think we can all agree he is highly qualified.

Senator SESSIONS. Well, you are experienced in these matters, and I just want to raise a certain point, if you will give me a brief answer on that.

Mr. LITT. I think the answer is quite clear under the controlling case law that a collection of this kind of telephone metadata from the telephone companies is not a violation of anyone's constitutional rights.

Senator SESSIONS. And when I was a federal prosecutor—and, Mr. Cole, you were a prosecutor—virtually every complex case resulted in a subpoena to phone companies to get people's phone records. Is that correct?

Mr. COLE. I would say the vast majority involved getting phone records in a case.

Senator SESSIONS. And when you do that, you obtain their name, a lot of details about the call, but not the contents of the case.

Mr. COLE. That is right. Many times you can get subscriber information—who owns the phone, what their billing address is, things of that nature—which we do not get under this program.

Senator SESSIONS. So this haystack of information that you have is only numbers. It does not even have the name of the person connected to that number, the subscriber of that number. Is that correct?

Mr. COLE. That is correct. If we find a chain that we think is important, we then have to do another investigation to find out who actually belongs to those numbers.

Senator SESSIONS. Well, Chairman Leahy and others—and we talked when the PATRIOT Act passed, we went into great, great detail about all these issues. And I would say that balancing the constitutional rights of danger versus constitutional rights is not the right way to phrase this. I believe everything in the PATRIOT Act that we passed was consistent in principle to the very things that have been done by law enforcement for years and decades in terms of the ability to issue subpoenas and obtain records. Maybe a few new applications of it to new technologies, but essentially the principles were maintained. Would you agree, Mr. Cole?

Mr. COLE. Yes, Senator. As I said at the beginning, I think we have struck the balance properly here, but there is always room for discussion and getting people's input. And times sometimes do change, and it is good to come back and revisit these things and make sure we have the balance right.

Senator SESSIONS. Well, I agree with that. I think the questions that have been raised require us to look at that.

Now, the data, this haystack of phone numbers, there is no ability to go back and listen to any of those conversations that occurred at a previous time, is there?

Mr. COLE. No. We do not even capture through this any conversations, so there is no ability, no possibility of listening to conversations through what we get in this program.

Senator SESSIONS. And, Mr. Litt, as an intel lawyer here, if you have the ability to tap a terrorist's phone call in Europe or Yemen, let us say, and that person calls to the United States, by definition of a lawful wiretap you listen to the persons that the individual calls. Is that right? So, I mean, a wiretap by definition is to listen to the conversations that the bad guy has with whoever he calls?

Mr. LITT. That is correct, and under FISA the Court requires us to have minimization procedures to ensure that we do not retain or disseminate communications of Americans unless those are valid foreign intelligence or evidence of a crime.

Senator SESSIONS. But if you want to tap a terrorist you have identified in the United States, you have to have a warrant with probable cause, do you not?

Mr. LITT. That is correct.

Senator SESSIONS. And so if you identify a person by surveiling a foreign terrorist, you identify phone calls to the United States, you would still have to have information sufficient to get a court to give you a Title III warrant to listen to that person's phone calls?

Mr. LITT. It could be a Title III warrant. It could be an individual warrant under Title I of FISA. But either way there is a probable cause standard that has to be met.

Senator SESSIONS. And it requires Court approval.

Mr. LITT. Yes.

Senator SESSIONS. Mr. Chairman, I know this Committee has worked hard on this. We tried to make sure that every provision in the Act was consistent with our constitutional and legal heritage. But we will listen to the concerns that are being raised, and if we made a mistake, I am willing to change it. But I am inclined to think all of these actions are consistent with the Constitution and laws of the United States.

Chairman LEAHY. One of the reasons we are having the hearing is that there are going to be some proposals for changes in the law, and I want to make sure that we have as much information as possible for it.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman. I also want to thank all the witnesses here, Mr. Cole, Mr. Inglis, Mr. Litt, and Mr. Joyce, for your service to the country.

I want to be clear at the outset. I think that these programs protect our country and have saved lives. But I do think there is a

critical problem at the center of this debate, and that is the lack of transparency around these programs. The Government has to give proper weight to both keeping America safe from terrorists and protecting Americans' privacy. But when almost everything about these programs is secret and when the companies involved are under strict gag orders, the American public has no way of knowing whether we are getting that balance right. I think that is bad for privacy and bad for democracy.

Tomorrow I am introducing a bill to address this, to fix this. It will force the Government to disclose how many Americans have had their information collected under key authorities in the Foreign Intelligence Surveillance Act, and it will give force—it will also force the Government to disclose how many Americans have had their information actually reviewed by federal agents.

My bill would also allow private companies to disclose aggregate figures about the number of FISA orders that they are receiving and the number of their users that these orders have affected.

Two weeks ago, a broad coalition of 63 Internet companies and bipartisan civil liberties groups sent a letter to the President asking for the reforms that my bill would make law. I am proud to say that I am introducing my bill with the support of Chairman Leahy, Senator Blumenthal, and a number of other Senators who are not on the Judiciary Committee. From what I just heard from Senator Feinstein, there may be some overlaps in our approaches, and I would be happy to work with her.

I would like to focus my questions on the subject of transparency. Mr. Litt, in the weeks after Mr. Snowden's leaks, the Office of the Director of National Intelligence decided to declassify the fact that, in 2012, only 300 queries were run on the database of telephone records compiled under Section 215 of the PATRIOT Act. Can you tell me why the ODNI decided to declassify that fact?

Mr. LITT. So, first, to be clear, what was declassified was the fact that there were fewer than 300 telephone numbers approved for queries. There can be more than one query based on the same telephone number if, for example, over time you want to check and see whether there have been any additional communications. So the number that was declassified was the number of selectors as to which reasonable, articulable suspicion had been established so that they could be the basis for a query.

Senator FRANKEN. Why did you decide to declassify the fact, and then?

Mr. LITT. You know, what we are doing is we are looking at all of the information surrounding these programs, at what has already been revealed, because fundamentally these programs were classified in toto to begin with because of the feeling that revealing our capabilities would give our adversaries an edge in how to avoid those capabilities. Once the fact of the program became public, we began to look at all the details surrounding the program, such as the orders that we have released today and the number you mentioned there, and we are making an assessment as to each one of them as to whether it is in the public interest to release that particular fact that has previously been classified.

Senator FRANKEN. I think that I do not want the public to take our word for it always, and I think there is a balance here, and

transparency is part of that balance. And I do not want a situation where the Government is transparent only when it is convenient for the Government. About an hour ago, ODNI declassified a FISA Court order under Section 215. That is a good thing. But ODNI has known for weeks that this hearing was coming, and yet ODNI releases material just a few minutes before the hearing began.

You know, again, it is a step forward, but you get the feeling, when it is ad hoc transparency, that is not—that does not engender trust, I do not think.

Mr. LITT. I could not agree with you more. I think we have an obligation to go through and look at the bad as well as the good and declassify what can be declassified without danger. We did actually have a discussion yesterday within the executive branch about whether we should release these documents this morning or not, because it is generally not a good idea to release things on the morning of a hearing. And I think we came to the conclusion that once we have made the determination that the documents should be declassified, there was no justification for holding them up any longer. And so that was—

Senator FRANKEN. Did you just start thinking about that decision like yesterday?

Mr. LITT. No, but it—

Senator FRANKEN. When did you—I mean, you have known this for a long time. You might have been—you might have thought about this weeks ago and said, you know, maybe not the day of.

Mr. LITT. We have been thinking about this for some time, and we have been processing these as quickly as we can. You will note that the documents that were released contain some redactions of information that remains classified.

Senator FRANKEN. Of course.

Mr. LITT. It is a rather time-consuming interagency process to reach consensus on what can safely be released.

Senator FRANKEN. Well, my time is up, but I think we should create a strong permanent set of public reporting requirements that will empower the public to reach their own conclusions about the merits of these programs, and that is what the bill I am working on would accomplish. Again, I would love to work with Senator Feinstein and, Mr. Litt, I would love if you would work with me to make sure we get the reporting requirements right as we move forward with the bill. Would you do that?

Mr. LITT. Absolutely. We would be glad to do that, sir.

Senator FRANKEN. Thank you.

Thank you, Mr. Chairman.

Chairman LEAHY. Incidentally, we are going to go next to Senator Flake, but I do want to compliment all four of the witnesses who are here for their candor, and I might want to single out General Inglis—or “Mr. Inglis” I guess you go by now. And I have been advised and I understand from others that you have always been very direct, very clear, very straightforward. Often that is in classified sessions, but you have been the same way in open session, and I appreciate that.

Senator Flake.

Senator FLAKE. Thank you, Mr. Chairman, and thank you, and I am sorry I was not here to hear your testimony. I know that you

have all noted in your written testimony that there are significant checks in the FISA system. Do you believe that there are insufficient checks to outweigh the concerns that some have about the appointment of an independent counsel? If you have touched on this in earlier questions, I apologize, but, General Cole, you mentioned that with regard to an independent counsel, do you think that there—in the second panel, Mr. Baker raises some issues and problems with independent counsel. Can you give me your thoughts on whether you think that is needed or not?

Mr. COLE. Certainly, Senator. This is a topic that is being discussed both in the administration and in the Congress as one avenue that might be available. Traditionally, when you issue search warrants, when you issue wiretaps and things like that, in the criminal law you do not have an adversary process that takes place. There is not somebody on the other side. So there is a legal tradition that the way we have been doing it is certainly one that we have done in other contexts.

We also have the Court that is involved, and that is unusual, as Mr. Litt had pointed out, particularly in a foreign intelligence context, to have the courts involved at all.

But this is something that I think we are open to having discussions about as to what the utility would be, what the role would be, how it would work. The devil can many times be in the details, but we think all of these things are worth discussing to figure out how to make this the best program it can be.

Senator FLAKE. If there were an independent counsel involved, can you foresee problems in terms of timeliness to have a lawyer staff cleared in time to review the sensitive information? If anybody else wants to address that as well.

Mr. COLE. I will just start. It may be a little bit, but the Court pushes back a lot itself, and there is an enormous process that takes place with the Court itself to make sure that we have satisfied all the requirements under the law and under the Constitution. So if there is somebody on the other side doing it, I would imagine they would be doing the same thing on roughly the same schedule.

Mr. LITT. If I can just add to that, there is a letter that the Chief Judge of the Foreign Intelligence Surveillance Court has written to the Chairman that I think is available on the Internet that outlines in some detail the procedures that the Court follows and I think gives a good sense for the care and thoroughness that the FISA Court exercises today.

Senator FLAKE. There has been some criticism in that the process that we have for the selection of these judges may lead to more Republican judges being appointed than Democratic—or more Republicans appointing judges than Democrats appointing judges. Do you sense or see any difference in your experience, all of you, with—is that an issue that somebody ought to be concerned about? Or have you seen any difference in decisions rendered?

Mr. COLE. From my experience I have not seen any decisions of the judges or judges in there being guided by the law and not necessarily by politics. But that is certainly a topic we would leave to the sound discretion of the Congress.

Senator FLAKE. Any other thoughts from anybody else? Do you see any problems with that process, selection of judges? Mr. Litt.

Mr. LITT. No, I was just going to say it is very hard to tell how another judge would have rendered a decision because you only have the one judge rendering the decision.

Senator FLAKE. All right. Thank you, Mr. Chairman.

Chairman LEAHY. Senator Durbin.

Senator DURBIN. Thank you, Mr. Chairman.

I am a liberal arts lawyer. I took some math courses, but it has been a long time ago, so I am going to ask the panelists, maybe Mr. Litt, Mr. Inglis, or whoever, to help me do some math here.

In 2012, there were 300 queries that resulted in a search of records, and we are told that there were three hops. In other words, if I was the subject matter of this search and I called Senator Feinstein, they would accumulate all of the records of my telephone calls to her and others, and then all of the records of Senator Feinstein's telephone calls, which may have included Chairman Leahy, and now you have included all of his records as well.

Mr. Jaffer of the ACLU will testify, at least speculate later, that if I had an average of 40 contacts, that would mean that for my name, my query, you would accumulate 2 million phone records—2 million for that one inquiry. Now multiply that in the year 2012 by 300. So we are talking about 600 million phone records. Now multiply that times 7 years.

So what has been described as a discrete program to go after people who would cause us harm, when you look at the reach of this program, it envelops a substantial number of Americans.

So can somebody help me with the math here, if I have missed something along the way or perhaps should minimize that number?

Mr. INGLIS. Sir, if I could start, and apologizing for the format, the unclassified format, I will be discreet in my remarks but happy to follow up in any detail that you would prefer, either here or at NSA.

First and foremost, the analysts are charged to provide information that is truly useful to the Federal Bureau of Investigation, and so in that regard they try to be judicious about choosing when to do a second hop or under the Court's authorization a third hop. Those are not always exercised. They do not always exercise a second hop for all numbers that might be pointed to by the first hop. And so while theoretically 40 times 40 times 40 gets you to a large number, that is not typically what takes place.

If an analyst were to see, for example, at the second hop that there are very significant numbers associated with one of those numbers, they would have to come to some deduction as to what that means. That could be that what you have kind of glommed onto is a pizza delivery man. You do not want to pursue that. That is not useful.

If on that second hop you see that that has hopped to a foreign number already known to the intelligence community because it is a known terrorist, you would want to make the third hop to understand what is beyond that.

Senator DURBIN. I understand that part of it where you are trying not to waste the time or resources of our Government in protecting our Nation?

Mr. INGLIS. Yes, sir.

Senator DURBIN. But the potential reach of this, when we say 300, goes way beyond 300.

Mr. INGLIS. So I think that is a very important question. We have to compare the theory to the practice. We try to be very, very judicious in the use of this very narrowly focused authority. And so the reason that we declassified the numbers is to show that we are, in fact, judicious. Less than 300 times did we approve a query for selection—or a selector for query in 2012, and provided less than 500 numbers in 12 reports to the FBI in all of 2012.

Mr. LITT. If I can just add one thing to that, it is important to remember that all that we are getting out of this is numbers—nobody's name, nobody's address, the content of no communications. These are all—this is nothing but a tool to try to identify telephone numbers that warrant further inquiry.

Senator DURBIN. I understand that. And here is the point, that I have offered an amendment before this Committee which garnered a grand total of four votes a few years ago on this very subject because most of the members were not aware of this program, the 215 program and its detail. I knew a little bit more than some, but obviously did not know as much as I am learning today. And there was a genuine concern today expressed. At that time because of the limited knowledge of the members, I got four votes.

So here is the question I get down to, and it is asked over and over again. If my cell phone is in area code 217, which it is, and I am a suspect, I certainly think it is appropriate and I encourage our Government to find out who I am talking to. That is important. I still cannot get to the point of requiring every person with a 217 area code to have their records collected in terms of their telephone conversations.

Now multiply that times every area code across America, and look at the potential reach. It seems to me that what is being described as a narrow program is really a very broad program in terms of the metadata collection on the front end. What I would like to ask—people have said, I have heard it from members of this panel, you know, we have saved lives with this. The 215 program has saved lives, stopped terrorism. Good. That is what we want our Government to do.

Could you have also saved the same number of lives and had the same impact if, knowing my telephone number as a suspect, you could search my records as opposed to collecting everyone's records in my area code?

Mr. INGLIS. So if I could go back to a case in point, perhaps that might be the best way to tease this out. I think that is a great question. The Basaaly Moalin case, what we knew at the time when we made that query was we knew a number that we had reasonable suspicion was affiliated with a terrorist group plotting against the homeland. That number was in Somalia. It was associated with Al-Shabaab. We had reasonable suspicion it was associated with something in the United States. We had no idea what it might have been associated with, and so we need to do a query. We did not know whether it would be associated with a 217 area code or a 303 area code, what of the grand set of possibilities was it associated with.

In order to find the needle that matched up against that number, we needed the haystack. That is what the premise is in this case. And in that point, if just before somebody had made that query you had said this is going to connect to a number in San Diego, that would have been as surprising as if you had said that number is connected to someplace in Yemen.

Senator DURBIN. But, Mr. Inglis, I guess what it gets down to is this: Once establishing that number with Al-Shabaab, this operative from Al-Shabaab, you could certainly go after that person's telephone records and all of the contacts that that person has made. The basic question we are faced with is: Do you need to collect 5 years' worth of data on everyone in America and their telephone records so that the haystack, which is pretty big—

Mr. INGLIS. That is a fair question. So the question would be: Is it enough to look prospectively, in the future, right, at that particular number? It may well be that the plotting you are looking for occurred in the past. And if you do not have that person's records in the past, then you cannot determine—

Senator DURBIN. And a point that has been raised repeatedly, if we required the phone companies to retain the records for 5 years—

Mr. INGLIS. That is a very fair point, and that is possible.

Senator DURBIN. It would not be in the grasp of the Government, but accessed by the Government.

Mr. INGLIS. I agree, sir.

Senator DURBIN. Which serves the same purpose, does it not?

Mr. INGLIS. I agree. But under the current legal framing, the phone companies are not required to retain that for the benefit of the Government.

Senator DURBIN. How hard would that be?

Mr. INGLIS. I think it would require a legal change. I do not think that is hard.

Senator DURBIN. I do not think so either.

Mr. INGLIS. I think that you can get there from here. You have to then think about the rest of the attributes that are necessary to make this a useful venture.

Senator DURBIN. Senator Feinstein said: "Ask him about the expense."

Mr. INGLIS. I would say in a classified session I could give you chapter and verse on the expense. The expenses are different depending upon whether you choose the current implementation or you choose an implementation where you leave it at the providers. The Government, if it requires the providers to retain those records, should bear that expense.

Senator DURBIN. Thank you.

Chairman LEAHY. Senator Lee.

Senator LEE. Thank you, Mr. Chairman.

As I understand it, the NSA's collection of metadata, the kind of metadata that we have been discussing today, is accomplished pursuant to Section 215 of the PATRIOT Act. Now, Section 215(b)(2)(A) of the PATRIOT Act places an important limitation on that collection in that it limits the Government's ability to collect that metadata to circumstances where the data in question is "relevant to an authorized investigation."

At some point—you know, relevance is a concept that is difficult to define in the abstract. It is a somewhat fluid concept, and it is one of those things that some jurist might say, “I know it when I see it, but I struggle to define it.”

Yet regardless of how difficult it might be to define in the abstract what relevance is, don’t you think we have left the station of relevance long before we get to the point of collecting metadata on potentially 300 million Americans and their cell phone usage? How can one get one’s mind around the concept of that volume of information, metadata or otherwise, all being relevant to an ongoing investigation?

Mr. COLE. Well, Senator, Mr. Litt—and he can chime in—had noted a little bit earlier how broad, as you noted yourself, the concept of relevance is in civil discovery, in many different kinds of legal contexts. It can be things that will lead you to things that you need as a concept for relevance.

Senator LEE. Right. I understand Mr. Litt’s very broad conception of relevance, and as he recently explained in his comments at the Brookings Institution. But I assure you, as a recovering lawyer myself, there is no context in civil discovery or otherwise in which one may define “relevance” broadly enough to take in information regarding each and every single American who owns a telephone.

Mr. COLE. The answer I would give to that, Senator, is that we are not really accessing or getting into all of that metadata that is stored in that database. We do not actually get to roam around in it. We do not get to look at it to our heart’s content and then say, well, this is relevant and that is relevant, so let us take that.

You have to look at it in the context of the primary order which was declassified and issued today that says the only way you can access it is if you have reasonable, articulable suspicion that the number you are going to query off of is, in fact, related to specific terrorist groups. And that has to be documented. And if you do not have that, you cannot get into this.

So the surveillance concept I think is very important here. You cannot surveil this without that gate being checked through.

Senator LEE. And that gate is not controlled by a warrant. I mean, if you want to access that, you do not have to go to court to get a warrant to access that. Those are controlled by internal procedures, correct?

Mr. COLE. That is correct. But they are controlled by the Court order, and they are controlled by compliance audits that are done both by the executive branch and the Court looking at how it is implemented on a periodic basis.

Senator LEE. Okay. Mr. Litt, do you have something to add?

Mr. LITT. Yes, just very briefly. I just want to make clear that the standard of relevance that I articulated in the speech is not mine alone. This is one that has been approved by the judges of the FISA Court and was known to members of this Committee and the Intelligence Committee at the time that the Section 215 authority was renewed.

Senator LEE. Well, I understand that. I understand that, and that has been part of the problem we have had, is that until recently most people did not have any idea about those, and we have significant constraints that limited our ability to explain why some

of us had concerns with the PATRIOT Act, why some of us on both sides of the aisle voted against reauthorizing the PATRIOT Act. We were unable to speak about this publicly because we have secret procedures being undertaken pursuant to secret law, and it has been a bit of a problem.

Now, what would you say, then, getting back to you, Mr. Cole, to my constituents? I understand what you are saying, that, "We are collecting all of it but we are not looking at it. We are collecting it, but we are closing our eyes, so do not worry about it." What would you say to my constituents who say, "I do not want the Government having that information. It is not the Government's information." It still does not make it relevant under the law. It still does not meet what many of my constituents believe to be well within their reasonable expectation of privacy for the Government to collect that much information, potentially information about 300 million Americans.

Mr. COLE. Well, I would say two things. First of all, we have had 34 separate times a court say that it does meet the standard of relevance, to have it all and then have the restrictions. But the further thing that I would say, which I think is very important, is what we are doing here today, which is it is worth having a debate about is there a better way to do it. It is worth having a debate about where we are going to strike that balance between security for the Nation and making sure that people's privacy and civil liberty rights are being honored. And that is a tough balance to find, but it is a balance worth talking about, and it is the process that we are welcoming and engaging in right now.

Senator LEE. Okay. Thank you. I see my time has expired. I just want to comment that I appreciate your insight on this. I do think it is worth discussing publicly, and I think it is also something that we need to consider from a constitutional standpoint. We have been relying on a 34-year-old Supreme Court case, *Smith v. Maryland*, to get at this idea that metadata is somehow beyond the reach of the Fourth Amendment. But we have to remember that *Smith* did not involve collection on hundreds of millions of Americans. It involved collection on a single target. It involved collection in a manner that is completely archaic by today's standards and that by today's standards would involve a minuscule amount of information.

I think at some point when you collect that much data on that many people—whether it is that much data on one person, that might create some problem. That much data on hundreds of millions of people creates an even bigger problem and one that I think was not considered by the Supreme Court of the United States in *Maryland v. Smith*—

Chairman LEAHY. Thank you.

Senator LEE [continuing]. One that we need to revisit. Thank you, Chairman.

Chairman LEAHY. Thank you, Senator Lee.

Senator Whitehouse, again, showing the expertise here, you served both on this Committee and the Intelligence Committee. I appreciate you being here.

Senator WHITEHOUSE. Thank you, Chairman.

Mr. Cole, you just said it is worth having a debate on these issues, and I think you are right about that. But I also hope that

the executive branch takes a lesson from this experience about the value of classification or what I would consider overclassification. I have seen this over and over now. When we were fighting with the Bush administration about the torture program, the executive branch got to tell its side of the story because the executive branch were the declassifiers, and we were stuck with facts that we knew that blew up the argument that was being made by the executive branch, but that we could not articulate because they were classified.

We have seen it on cyber where so much of the American public is unaware of the cyber threat that we are facing. Now, thankfully, we are becoming more aware, but for a long time we were just in the dark about what was going on because in the private sector companies did not want to talk about it for fear of aggravating their regulators, their consumers, their clients, even giving their competitors advantage, and the Government just wildly overclassified everything.

Now we have, I think, a terrific article that Senator Feinstein wrote. We have, I think, very good testimony by Bob Mueller. We have a lot of good information out there that helps the American public understand these programs. But it all came out late. It all came out in response to a leaker. There was no organized plan for how we rationally declassify this so that the American people can participate in the debate.

I think there is an executive branch reaction toward classification. I think that reaction is in part because of the advantage it gives the executive branch relative to the legislative branch, which cannot declassify. And I think over and over again we have found that, looking back, we are worse off for that effort in the first instance.

So I would really urge you to take a look at this and, you know, when this thing burst, there is this old saying—I am not going to get it exactly right, but there is something about the rumor is all the way across town before the truth could even get its boots on. You have lived that experience in the last couple of months. I hope this has an effect on you, because this is a recurring problem and we really need to be balancing much more carefully the value of declassification against the value of classification.

I think you guys are terribly one-sided in favor of classification, and then something like this comes and, pow, you are still trying to get your boots on because you never took the appropriate steps to put news out about this program that would have avoided, I think, a lot of this. And I would like to have you have a chance to react to that.

Mr. COLE. I think you make very valid points, Senator Whitehouse, that these are all topics that we need to debate. They are not easy topics because they involve, again, that same balancing—the same balancing that we are trying to do between national security and civil liberties. And what kinds of programs we put into place to gain intelligence information is the same kind of debate we need to have about what is classified and what is not classified and what secrets we let out.

If it was easy, we would be having these left and right. I do not think, at least from what I have seen, that the executive branch

is doing it to disadvantage the legislative branch, but I think that may be—

Senator WHITEHOUSE. But it does have that effect.

Mr. COLE. It may have that effect, and I would concede that. I think it is done because people are cautious, and it is easier to overclassify than to underclassify. It is safer to overclassify than to underclassify. And now we are having to get into the hard work of finding just where that line is, and that is a difficult job to do. But it is worth doing.

Mr. LITT. Senator, could I just add—

Senator WHITEHOUSE. So something like this happens or the torture program gets exposed or we have a significant cyber attack, or something happens that shows that that short-term decision that it was easier to classify was actually the wrong decision.

Mr. LITT. I just want to add on this—and I know you are familiar with what I am about to say, but we are having a public debate now, but that public debate is not without cost. The information that has been leaked is going to do damage to our ability to protect the Nation. We are going to lose capabilities. People are paying attention to this.

The way that typically the Congress, both through the legislation it passes and through its own internal rules, has historically sought to achieve the balance between appropriate oversight of intelligence activities and the need to protect sources and methods is through primarily the Intelligence Committees but also some other committees of Congress—this Committee, the Armed Services Committee, the Appropriations Committees. And typically that is the forum that has been used to strike this balance. It may be—

Senator WHITEHOUSE. I get that, and my time has expired, so let me just jump in and say we all get that. My point is that the American public is an important part of this debate, and we would probably be better off if there was not such a strong instinct in favor of classifying and keeping things classified and we developed information for the American public in a way that minimized that intelligence collection loss and allowed us to have this debate.

Thank you.

Chairman LEAHY. Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman. I want to join in thanking the Chairman for this hearing and for his legislative proposal, which I have joined, and to each of you for your extraordinary contribution to our Nation but also to the thousands of others in the intelligence community and special operations who have thwarted and stopped terrorist threats to this country and which all too often I believe have been ignored because the efforts to stop them have been so successful, and the debate, as Mr. Cole has termed it, is one that is very appropriate in a free society that is trying to protect itself from terrorism by using search and surveillance, which have a role, and what we are grappling to do here is to define how to reconcile the secrecy of search and surveillance, which necessarily have to be so, with privacy and civil liberties and all the other constitutional guarantees that make us unique among the nations in the world and, in fact, the greatest Nation in the history of the world.

You know, I have been a litigator for close to 40 years. I have never doubted that the scores of judges that I have litigated before have a commitment to rights of privacy and all the constitutional rights. And I have no doubt about the FISA judges pushing back and having a commitment to the rule of law. But in appearance, this system is failing, and failing fast, to maintain the trust and credibility of the American people who want to be protected from terrorist threats, but at the same time also protected from the degradation of their constitutional rights.

So I am introducing a bill that would change the appointment and selection procedure so that the appearance and the reality of diversity of view and aggressive protection of constitutional rights is maintained and enhanced. And I will be introducing that bill tomorrow that would involve the circuit court judges on our courts of appeals, chief judges, in the appointment process, with the continued involvement of the Chief Justice, and change also the FISA Court of Reviews selection process.

I have found in my years that one of a judge's worst nightmares is incompetent counsel, and the reason is, especially in a criminal trial, that incompetent counsel or lack of counsel for the defendant means that the record on appeal is weaker, that the test and clash of litigation is diminished in quality, and that is the basic principle that I think should be involved in some way in the FISA Court as well.

And so a second bill that I am proposing is for a special advocate to be involved not necessarily in the ex parte proceedings on every single warrant or surveillance or search, but at some point where there are significant issues of law so that different sides are presented, challenges are made, and the judge or panel has the benefit of that contention that is at the core of our court process. Our courts not only insist on but thrive on the clash and testing of different points of view. Whether it is debate on a legal issue or cross-examination, that is at the essence of our litigation process.

So I think in appearance, if not reality, the current design of the FISA Court stacks the deck against the protection of our civil liberties and can be improved and enhanced without sacrificing either speed or security, because those special advocates can be cleared beforehand for security purposes, they can be involved after the fact, if necessary, on appeal in effect to the FISA Court of Review or to the U.S. Supreme Court. And I hope—and this is to lead to the question—I hope, Mr. Cole and Mr. Litt, that you will join in this process of trying to improve the current FISA Court structure. And I would like to know whether there is active consideration of changes in the selection procedure and the involvement of potentially a special advocate or independent counsel of some kind in this process.

Mr. COLE. Senator, I think at this point there is active consideration of a range of issues just to get at the kinds of things you are talking about, to make sure that the process works as well as it can, to balance both of those important issues of national security and civil liberties and privacy, and to make sure that it is transparent enough so that we maintain credibility with the American people about this program.

It is a difficult issue, as we have discussed today for several hours, to find the right balance. But, yes, it is definitely something under consideration and active discussion in the administration.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Chairman LEAHY. Mr. Cole, I have a question. As I understand it, the Government believes that every single domestic phone record is relevant to terrorism investigation and can be obtained using Section 215 of the PATRIOT Act. And I understand the FISA Court agrees with that interpretation, but you then place restrictions on how it can be used once you have collected it. But I do not understand what limits there might be under this theory. Couldn't you invoke under this—couldn't you invoke Section 215 to obtain virtually all available commercial data? If Americans' phone records are relevant, how about our credit card records, what sites we go on on the Internet, what we may bookmark, our medical records, if we have it on the computer, or firearms records, we keep a list of what firearms we hold? Are all those things available?

Mr. COLE. Well, I think there are two important points here, Mr. Chairman.

Number one is that the only way the Court finds these relevant is in the context of the restrictions and in the context of what it is you are looking for. So you have to take all of those features of this phone record process into account of how can it be done, how reasonably can it be done, what is the need for speed, what is the need to integrate all the different records that are coming together, and finds only when you look at that entire mix that this kind of program, with these restrictions—

Chairman LEAHY. I understand—

Mr. COLE. To your question, you would have to make that same showing for those other kinds of records as to the need for that breadth and the need for those restrictions.

Chairman LEAHY. But if our phone records are relevant, why wouldn't our credit card records be—wouldn't you like to know if somebody is buying the fertilizer used in bombs?

Mr. COLE. I may not need to collect everybody's credit card records in order to do that because, again, these are—we are not collecting all their phone records so that we can wander through them. And it is only the phone records that are being used to look at the connections. If somebody is buying things that could be used to make bombs, of course, we would like to know that, but we may not need to do it in this fashion.

Chairman LEAHY. Well, Director Clapper said NSA would notify Congress before obtaining cell phone location information under this program. Is there any legal impediment to you expanding the program for cell phone location?

Mr. COLE. I do not believe there would be a legal impediment, and yesterday the Fifth Circuit issued a ruling that goes to that issue. But the legal impediments are not the only issues that you take into account here.

Chairman LEAHY. I understand. Well, I want to put several items in the hearing record:

Written testimony from Mark Zwillinger who represented Yahoo! in its challenge to a directive received under the PROTECT Amer-

ica Act; he is one of the few non-Government lawyers to appear before the FISA Court, so that is important insight;

A letter from Judge Reggie Walton, presiding judge of the Foreign Intelligence Surveillance Court, responding to questions from Senator Grassley and myself;

A letter from a coalition of communications companies and advocacy groups regarding transparency;

A letter from a coalition of privacy and civil liberties groups recommending staff—a letter from the Constitution Project supporting S. 1215, the FISA Accountability and Privacy Protection Act.

Those will all be placed in the record.

[The information referred to appears as a submission for the record.]

Chairman LEAHY. If there are no further questions for this panel, and if there are not, I would thank all four of you. I know you have spent a lot of time preparing for this. I thank you all for being here. I know you have a lot of other things you should be doing and can be doing, but thank you for taking this time.

We will start on the next panel. If we are interrupted by a vote, we will then stop until 12:30 when Senator Blumenthal has offered to come back and preside, but we would call up Judge Carr, James Carr, U.S. District Court for the Northern District of Ohio; Jameel Jaffer, the deputy legal director, American Civil Liberties Union; and Stewart Baker, a partner at Steptoe & Johnson. I thank you all very much.

[Pause.]

Chairman LEAHY. I thank the witnesses who are here, and I apologize in advance if we end up having to recess for a period of time and come back. But, Judge Carr, why don't we begin with you, and thank you for coming here.

STATEMENT OF THE HONORABLE JAMES G. CARR, SENIOR JUDGE, U.S. DISTRICT COURT FOR THE NORTHERN DISTRICT OF OHIO, TOLEDO, OHIO

Judge CARR. Thank you, Senator. It is my pleasure to be here. I served on the Foreign Intelligence Surveillance Court from 2002 to 2008. I have been a United States district judge since 1994 and before that a magistrate judge since 1979. I am the author of a two-volume treatise on the law of electronic surveillance, which I suspect played a role in the decision to appoint me to the Court.

I want to make clear, as I hope I did in my brief prepared remarks, that I am here solely on my own behalf. I am not here on behalf of the Judicial Conference, the Administrative Office, the judiciary generally, or the Foreign Intelligence Surveillance Court. And actually I think why I am here today is because by coincidence I happened to have an op-ed piece published a week ago in the *New York Times* in which I made a proposal that I am glad to be able to make in front of this Committee in a somewhat more public fashion.

Chairman LEAHY. And that op-ed piece will be made part of the record.

Judge CARR. Thank you.

[The op-ed appears as a submission for the record.]

Judge CARR. Very simply put, what I propose is that Congress amend the Foreign Intelligence Surveillance Act simply to give, sort of officially give the discretion to the individual judges of the Foreign Intelligence Surveillance Court, or if they sit en banc, the ability to appoint a security-cleared attorney to represent the interests of the public and interject to some extent the adversary process at the level of the Foreign Intelligence Surveillance Court.

I listened with interest to Senator Blumenthal's suggestion about an advocate who would become engaged at the level of the Court of Review. Speaking, again, solely on my own behalf, the origin of this thought comes from my experience as a member of that Court for that period.

There were a couple of occasions—I cannot count them but fewer than the fingers on one hand, I am sure—in which I felt as a district judge that it would have been useful, when the Government proposed some new program some new method or means of acquisition, that it would have been useful to have somebody speak in opposition to the request and to hear the other side. That would, it seems to me, accomplish two things, and if that discretion were available to members of the Court, particularly when issues arose under Rule 11 of the current Rules of Procedure, which require that the Government notify the judge when something new or novel is being proposed. That is what they did when we were there, and that was always very useful. But in any event, I think my proposal would have two very beneficial consequences.

One, as I believe Senator Blumenthal already alluded to, it would provide us with the opportunity as judges to reach more informed decisions, because we would have heard two points of view. That is what we do day in and day out in our chambers and in our courtrooms. We are accustomed to that, and we are comfortable with that.

Second, it would create a mechanism which I think is very important for in instances when the Government prevails, in which the Foreign Intelligence Surveillance Court judge approves the new and novel request, because there was a lawyer engaged at the outset, that lawyer could seek review before the Foreign Intelligence Surveillance Court of Review and in turn before the U.S. Supreme Court.

Today, of course, only the Government can appeal, and the Government has done so I believe on a couple of occasions. I am familiar with one. But there was nobody there on behalf of the other side, as it were. And as I say, I think that my proposal is fairly simple, straightforward, economical, and I think it would be very useful.

Thank you for hearing me out, and I welcome your questions as to what I have to say.

[The prepared statement of Judge Carr appears as a submission for the record.]

Chairman LEAHY. Thank you very much, Judge. And I should note you were on the FISA Court from 2002 to 2008.

Judge CARR. Right.

Chairman LEAHY. I believe Chief Justice Rehnquist, a part-time Vermonter, rest his soul, was the one who appointed you.

Jameel Jaffer is the deputy legal director at the American Civil Liberties Union, director of the ACLU's Center for Democracy, currently counsel to the plaintiffs in *ACLU v. Clapper*, challenging the NSA's phone records program. He has litigated several cases concerning the PATRIOT Act and FISA Amendments Act.

Please go ahead.

**STATEMENT OF JAMEEL JAFFER, DEPUTY LEGAL DIRECTOR,
AMERICAN CIVIL LIBERTIES UNION FOUNDATION, NEW
YORK, NEW YORK**

Mr. JAFFER. Thanks. Thank you for the invitation to testify.

Over the last 2 months, it has become clear that the NSA is engaged in far-reaching, intrusive, and unlawful surveillance of Americans' telephone calls and electronic communications. The surveillance programs we are talking about this morning are the product of both defects in the law and defects in the current oversight system. FISA affords the Government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the Government's surveillance activities. The ordinary federal courts have improperly used procedural doctrines to place the NSA's activities beyond the reach of the Constitution. And structural features of the FISA Court have prevented that Court from serving as an effective guardian of individual rights.

Surveillance supposedly undertaken to protect our democracy now presents a threat to it. It is not simply that this surveillance has dramatic implications for individual privacy, though plainly it does. Pervasive surveillance is also poisonous for free speech and free association. People who know the Government could be monitoring their every move, their every phone call, or their every Google search will comport themselves differently. They will hesitate before visiting controversial websites. They will hesitate before joining controversial advocacy groups. And they will hesitate before exercising rights that the Constitution guarantees.

Now, individually those hesitations may appear to be inconsequential, but the accumulation of those hesitations over time will alter the nature of our democracy. It will alter citizens' relationship to one another, and it will alter their relationship to their Government. That much is clear from the history of many other countries. And it is what the Church Committee warned of more than 30 years ago. That warning should have even more resonance today because in recent decades the intelligence agencies' resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. But should take certain steps right away.

First, it should amend FISA to prohibit "dragnet" monitoring of Americans' communications. Amendments of that kind should be made to the FISA Amendments Act, to FISA's so-called business

records provision—that is, Section 215—and to the national security letter authorities.

Second, Congress should end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the Government to publish basic statistical information about the Government's use of foreign intelligence authorities. It should ensure that the gag orders associated with national security letters are limited in scope and duration and imposed only when absolutely necessary. And it should require the publication of FISA Court opinions that evaluate the meaning, scope, or constitutionality of the foreign intelligence laws.

Finally, Congress should ensure that the Government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge Government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC, in the FISA Court, when the Government's surveillance applications raise those kinds of novel issues of statutory or constitutional interpretation. And it should enact legislation to ensure that the state secrets privilege is not used to place the Government's surveillance activities beyond the reach of the courts.

Thank you again for the opportunity to testify.

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

Chairman LEAHY. Thank you very much.

Mr. Baker, you are a partner, I understand, in the law firm of Steptoe & Johnson, but you were originally general counsel of the National Security Agency. You were the first Assistant Secretary for Policy at the Department of Homeland Security. We are happy to have you here, sir. Please go ahead.

STATEMENT OF STEWART A. BAKER, PARTNER, STEPTOE & JOHNSON LLP, WASHINGTON, DC

Mr. BAKER. Thank you, Mr. Chairman. It is a pleasure to appear before you and the other members of the Committee again. Just two points about this program I think are important to begin with.

First, the kind of information that is being gathered here—phone numbers, phone records, billing records, in essence—is the sort of information for which a million subpoenas a year are served by law enforcement on phone companies today. This is not data that is kept out of the hands of Government by existing procedures and not the kind of data that has been abused in obvious ways since they have been doing this since the beginning of billing records almost a century ago. So this is not extraordinarily sensitive information.

And neither is this an unchecked program. I think, having looked at the order that was declassified this morning and having heard the procedures that have been described in the past, it is pretty clear that the people who are reviewing these records are subject to more scrutiny, more checks, more discipline than any of the other law enforcement agencies that have subpoenaed a million records from the phone companies each year.

The problem, obviously, from the discussion here is that the Government gathered the information and put it in a database first,

and that is an unusual step. The question is: What could we do other than that? If we leave this with the phone companies and try to gather the information from the phone companies, first, they will get rid of this information when they choose to, when it is no longer of interest to them, which would be in a matter of months. We have no guarantee it will be there when we need it. We have no ability to search across the records of each of those phone companies to do the kind of analysis that we need to do to find the folks that have been found with this program.

And, finally, I suppose we could pay them to put it in a format and keep it for a period of time that we thought was necessary to run this program, but then you have created a database that every divorce lawyer in America is going to say, "Well, that is AT&T's data. I am just going to subpoena it." This is not something that we really want to do. Who is going to search it? Is the phone company going to search it? Are we going to ask China Mobile to do searches for national security targets on the data that they are storing? Or are we going to give the Government access to the servers? Which is, of course, what caused the flap over the 702 program in the first place.

So I think there are real problems with leaving this in the hands of the private companies, and that is why as a practical matter the Government chose the route that it did.

The other problem obviously is that this has been kept secret, and I have to say the fact is—and I have spent a lifetime doing this—you cannot do intelligence in public because the targets are the most interested in how you do it and what the limitations you have imposed on yourself may be. And, therefore, disclosing the limitations, arguing about exactly how we are going to do this reveals to the people we are trying to gather intelligence on, who in many cases are trying to kill us, exactly what it is that we are trying to do. So there is a big cost to doing this in public and to having the kinds of disclosures that we are having.

Last thought, and I have heard Senator Blumenthal's proposal and Judge Carr's proposal. I have to express some doubts about the idea of appointing a counsel from outside the Government to represent—I do not know—well, that is the first question. Who or what is this person supposed to be representing? Are they representing the terrorists? Are they representing the Court? Are they representing some abstract interest in civil liberties? Or are we just going to let them decide?

You know, we got rid of the independent counsel law precisely because we were uneasy about having private parties just make up their own public policy without any check from political decision-makers or without any client. And I fear we are getting into the same situation if we start appointing counsel to represent something in the context of these cases.

I will stop there and be glad to answer questions.

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

Chairman LEAHY. Thank you, and we are going to wrap up because the vote is going to start. But, Judge Carr, what about that? Your proposal was not to have counsel in every single case but where there were special legal issues raised. Is that correct?

Judge CARR. Absolutely. It would be a probably very infrequently invoked opportunity that I am asking you to put in the hands of the individual judges when they encounter new and novel questions.

Chairman LEAHY. Thank you.

Judge CARR. And if I may speak to the issue of who is the client, obviously there is no client in the conventional sense. This is, admittedly, an unorthodox procedure. In the op-ed and my remarks, I tried to indicate why it is important, even though we do not have it in Title III applications or search warrants.

I think ultimately that the individual represents—that lawyer that I am talking about, precleared by security, set to go—would represent the interests of the public generally in seeing to it that the balance between constitutional rights, the Fourth Amendment, and the President's authority to conduct our foreign affairs is maintained and upheld and not tilted one way or the other. And to some extent, I would hope that if this process were in place, it would enhance public confidence in the results reached, regardless of what they were, and particularly those when they favored the Government, because the public would know somebody was in there speaking on its behalf generally and broadly but in opposition to the Government's request.

Chairman LEAHY. Thank you very much.

Senator Blumenthal, I am going to turn it over to you, and then when the vote starts, we can recess. I thank you very much.

Senator BLUMENTHAL [presiding]. Thank you, Mr. Chairman. I think that the proposal that I will be making in my legislation is very similar to the suggestion you have made, and I want to thank, Judge Carr, for the thought that you and Judge Robertson have devoted to this subject and the very insightful ideas that you have suggested. And there are other instances, as we all know as lawyers, where the court essentially appoints counsel from time to time in both civil and criminal proceedings to represent, in essence, the public interest or some perhaps non-identifiable individual who might at some point in the future have an interest in the proceedings. And, indeed, in this instance what I proposed is an Office of Special Advocate whose attorneys would be precleared and whose security credentials would be on a par with, in effect, the prosecutors or the Government, and on those novel or significant issues of law that arise from time to time could represent in essence an opposing point of view, a different side, as Judge Robertson has put it. The basic idea is that judges are accustomed to hearing two sides of an argument, as you have articulated so well.

So I think some of the practical objections are easily addressed, and what I would like to ask you is whether there are, in fact, significant and novel issues of law that do arise from time to time where you think either before the FISA Court or on review ultimately the development of the law would be enhanced by having an opposing point of view represented.

Judge CARR. I do, and I think to some extent you can look at Rule 11 of the Foreign Intelligence Surveillance Court Rules of Procedure, which requires the Government to call the judge's attention to something that is new and novel. So you already have in place sort of a flagging mechanism, and that actually codified the way

things worked in any event when I was a member of the Court. The Government really was an honest broker and said, "Judge, looking at paragraph 73 to 78, that is something you have not seen before." And there were times when that happened, when simply to hear another side, I wished or hoped or desired that there is somebody else picking up and giving me a different view.

Let me say, Senator, I find your proposal interesting and very worthwhile. I would only suggest bring it down to the level of the FISC itself. In other words, do not wait for an appeal because that way you will have a fully developed record, the agencies would have been laid out, the judge would have reached hopefully a reasoned and informed decision, and written an opinion with reasons that then whoever is unhappy with it can be taken for appellate review. That is the way it works normally. That is the way it should work in the foreign intelligence surveillance context.

Senator BLUMENTHAL. And to some extent, you have already anticipated my proposal because it would, in fact, enable representation of two sides in the FISA Court as well as the Court of Review because, as you well know, a record is essential often to determining an issue of law simply to clarify what factual issues are at stake.

And I think the important point for people to understand—and this really goes to perhaps some of the objections to the proposal. In the criminal context, when a warrant is issued, it is almost always *ex parte*—

Judge CARR. Always.

Senator BLUMENTHAL. Always *ex parte*, except sometimes in a grand jury if in very exceptional cases opposing counsel is present. But then at some point, the question of admissibility arises to the evidence that is garnered as a result of the warrant or surveillance or other means of activity by the Government. And at that point there is a public hearing.

Judge CARR. And also keep in mind, certainly with an ordinary search, the subject learns immediately, comes home, the door has been broken, knocked down. But if indicted, he can file a motion to suppress. Even if not indicted, the subject can file a motion under Rule 41 for return of property: Give me my money back, give me my whatever it is back. But there are mechanisms that are available to question and to raise and to challenge the legitimacy of what the Government has done. And that is why I proposed—that is one of the purposes of my proposal, is to enable the opportunity to test the legitimacy of what the Government has done.

Day in and day out, something I want to emphasize, the applications that the Foreign Intelligence Surveillance Court reviews, they are fact based. They have a very low standard of probable cause, and properly so, because as another witness mentioned, or one of the Senators, this represents what I consider to be a brilliant—the FISA represents a brilliant compromise reached by the legislative branch in a constitutionally uncertain area. I mean, where in Article II does it say that a court has anything to do with the President's conduct of foreign affairs? On the other hand, the Fourth Amendment applies to the President. And nobody knows how far either of those reach, and that is why the FISA is so useful and I think effective.

Senator BLUMENTHAL. And this proposal, while it might lend itself to greater transparency, would still keep secret the FISA Court proceeding at a stage when secrecy is paramount for the search and surveillance activity. It would simply enable—and I think you have used the key word—the “testing” of the Government’s claim that the surveillance or search is both legal and necessary.

Judge CARR. Well, actually, if I can say, Senator, we do not consider—I am speaking in the past tense. I did not consider and I do not think the judges do consider the necessity for the surveillance. I think that is quite clear under the Act. We look at only probable cause, agent of a foreign government, active on behalf of foreign terrorist-based organization, that is it. We do not second-guess and say, gee, how come you are spending money on this instead of that?

Senator BLUMENTHAL. Mr. Baker, let me ask you, does any of this discussion between Judge Carr and myself allay some of your concerns?

Mr. BAKER. Some of the concerns, yes. Obviously if you have got a full audience, full office ready to go and you are focused on the Court of Review where the issues are teed up, it is easier to justify having a special counsel appointed.

I do have to say that I question the assumption that creating this office will make people feel better about the functioning of the Court and the national security apparatus in general because it will necessarily be secret. And I have watched as the General Counsel of the National Security Agency tried to act as an advocate for the public interest, as the Inspector General of the National Security Agency was put forward as an advocate for the national interest. As the Office of Intelligence at the Justice Department said, “We will represent the public interest. We are not in bed with the intelligence community. We will ride herd on them.” And yet every time there is a fuss—well, and even the clerks who serve the FISA Court act as a kind of institutional second voice, and none of that matters at the end of the day when a scandal of this sort blows up.

So I question whether people will not simply say, “Oh, well, sure, this person was representing the public interest, but he got his security clearance from the Government, he might be paid, his staff is paid by the Government. It is really just a sham.” So I fear that this will not have the effect that you are hoping it will.

Senator BLUMENTHAL. Well, hopefully it will improve and enhance the process, which, at the end of the day, gives people the trust and credibility in the system. And maybe I should ask that question of Mr. Jaffer. Would you and others with your very commendable and admirable commitment to civil rights and civil liberties be somewhat reassured—I am not saying that you would give it a gold star necessarily, but would it provide some reassurance?

Mr. JAFFER. Absolutely. I do think it would provide some reassurance. I think it is important that there be some form of adversarial process, especially when these issues raise questions of constitutional interpretation or statutory interpretation that are new. And I think that one of the important roles for the special advocate is to press for transparency where transparency is appropriate and

possible. So I think it would be a very significant improvement to the system.

Now, I do not think it is enough. I think it has to be paired with some other reforms, including reforms relating to transparency and a narrowing of the substantive standards that the FISA Court is applying. But I absolutely do think that this would be a step in the right direction.

Senator BLUMENTHAL. And I would agree with you that some greater degree of transparency on the orders and opinions so that the public has some greater access to rulings of law at the very least, with sensitivity to the need for redacting details that security may require, as well as—I do not know whether you were here earlier, but I have a proposal to change the method of selecting the members of the FISA Court that would, in essence, give the chief judges of the courts of appeal a role in designating the individuals so that the Chief Justice of the U.S. Supreme Court would not be the sole source of those appointees.

But I think moving in this direction would not only be good for the credibility of the Court, but good for the ultimate justice of the outcome and protecting rights and liberties.

Mr. JAFFER. Just on the transparency point, Mr. Baker said earlier that we cannot expect the Government to do intelligence in public, and I think that is a fair point. But I think it is crucial to remember the distinction between law and policy on one hand and sources and methods on the other. The public has a right to know what the Government's policies are and what the legal basis is for those policies. And that is all anyone is asking for. Nobody is suggesting that the factual basis for the Government surveillance should be disclosed or that the surveillance targets' names should be disclosed while the Government is engaged in the surveillance. The debate is not about that. The debate is about, should the public know what the Government's policies are? And I think in a democracy that should not really be a debate at all.

Judge CARR. Senator, if I may, I was appointed, in effect, by the chief judge of our circuit, Boris Martin. The way it worked with me is I was one of the judges appointed to the four positions created in the PATRIOT Act. Judge Martin had been well aware of my interest because of the work I had done in publication with regard to electronic surveillance generally. It is my understanding the Chief Justice called upon Ralph Mecham to reach out to propose somebody. It happened to be the Sixth Circuit's turn apparently, and Judge Martin called me and said, "Jim, I got this call from Ralph Mecham. I am forwarding your name."

So at least when I was appointed 10 or more years ago, it seems to me that might be codifying the practice.

Senator BLUMENTHAL. It may be, Judge Carr, but we have no idea, do we?

Judge CARR. Right.

Senator BLUMENTHAL. Because the process is so secretive and the effort to formalize what happens behind closed doors or behind the veils of the Chief Justice's office may enhance some confidence, at least cannot hurt.

Judge CARR. Well, also, one other point on the issue. A role for the advocate, however you want to call it, in urging that portions

or complete opinions both of the FISC and the Court of Review become public, I think that individual could—I had not thought about that, but I think that individual could also perform that role in urging the Government to be diligent and thorough and see to it that, to the extent that anything can be disclosed, that it is.

Senator BLUMENTHAL. Unfortunately, I have got to—I am probably the only Senator at this point who has not voted, and I have to apologetically excuse myself to do so. I think I have authority to close this hearing.

The record will remain open for 1 week. I want to thank each of you for being here. Your testimony has been remarkably helpful and effective, and I will be calling on you again in the course of my work on this issue personally. I am sorry that more of my colleagues were not here to hear you themselves, but I am sure they will review the record of what you had to say.

So thank you very much. This hearing is adjourned.

[Whereupon, at 11:22 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Witness List

Hearing before the
Senate Committee on the Judiciary

On

“Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs”

Wednesday, July 31, 2013
Dirksen Senate Office Building, Room 226
10:00 a.m.

Panel I

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

John C. Inglis
Deputy Director
National Security Agency
Washington, DC

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

Sean M. Joyce
Deputy Director
Federal Bureau of Investigation
Washington, DC

Panel II

The Honorable James G. Carr
Senior Judge
U.S. District Court for the Northern District of Ohio
Toledo, OH

Jameel Jaffer
Deputy Legal Director

American Civil Liberties Union
New York, NY

Stewart Baker
Partner
Stephoe & Johnson LLP
Washington, DC

PREPARED STATEMENT OF HON. PATRICK LEAHY

**Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing on “Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs”
July 31, 2013**

Today, the Judiciary Committee will scrutinize government surveillance programs conducted under the Foreign Intelligence Surveillance Act, or FISA. In the years since September 11th, Congress has repeatedly expanded the scope of FISA, and given the Government sweeping new powers to collect information on law-abiding Americans – and we must carefully consider now whether those laws have gone too far.

Last month, many Americans learned for the first time that one of these authorities – Section 215 of the USA PATRIOT Act – has for years been secretly interpreted to authorize the collection of Americans’ phone records on an unprecedented scale. Information was also leaked about Section 702 of FISA, which authorizes NSA to collect the communications of foreigners overseas.

Let me make clear that I do not condone the way these and other highly classified programs were disclosed, and I am concerned about the potential damage to our intelligence-gathering capabilities and national security. We need to hold people accountable for allowing such a massive leak to occur, and we need to examine how to prevent this type of breach in the future.

In the wake of these leaks, the President said that this is an opportunity to have an open and thoughtful debate about these issues. I welcome that statement, because this is a debate that several of us on this Committee have been trying to have for years. And if we are going to have the debate that the President called for, the executive branch must be a full partner. We need straightforward answers and I am concerned that we are not getting them.

Just recently, the Director of National Intelligence acknowledged that he provided false testimony about the NSA surveillance programs during a Senate hearing in March, and his office had to remove a fact sheet from its website after concerns were raised about its accuracy. I appreciate that it is difficult to talk about classified programs in public settings, but the American people expect and deserve honest answers.

It also has been far too difficult to get a straight answer about the *effectiveness* of the Section 215 phone records program. Whether this program is a critical national security tool is a key question for Congress as we consider possible changes to the law. Some supporters of this program have repeatedly conflated the efficacy of the Section 215 bulk metadata collection program with that of Section 702 of FISA. I do not think this is a coincidence, and it needs to stop. The patience and trust of the American people is starting to wear thin.

I asked General Alexander about the effectiveness of the Section 215 phone records program at an Appropriations Committee hearing last month, and he agreed to provide a classified list of terrorist events that Section 215 helped to prevent. I have reviewed that list. Although I agree that it speaks to the value of the overseas content collection implemented under Section 702, it

does not do the same with for Section 215. The list simply does not reflect dozens or even several terrorist plots that Section 215 helped thwart or prevent -- let alone 54, as some have suggested.

These facts matter. This bulk collection program has massive privacy implications. The phone records of all of us in this room reside in an NSA database. I have said repeatedly that just because we have the ability to collect huge amounts of data does not mean that we *should* be doing so. In fact, it has been reported that the bulk collection of Internet metadata was shut down because it failed to produce meaningful intelligence. We need to take an equally close look at the phone records program. If this program is not effective, it must end. And so far, I am not convinced by what I have seen.

I am sure that we will hear from witnesses today who will say that these programs are critical in helping to identify and connect the so-called "dots." But there will always be more "dots" to collect, analyze, and try to connect. The Government is already collecting data on millions of innocent Americans on a daily basis, based on a secret legal interpretation of a statute that does not on its face appear to authorize this type of bulk collection. What will be next? And when is enough, enough?

Congress must carefully consider the powerful surveillance tools that we grant to the Government, and ensure that there is stringent oversight, accountability, and transparency. This debate should not be limited to those surveillance programs about which information was leaked. That is why I have introduced a bill that addresses not only Section 215 and Section 702, but also National Security Letters, roving wiretaps, and other authorities under the PATRIOT Act. As we have seen in the case of ECPA reform, the protection of Americans' privacy is not a partisan issue. I thank Senator Lee and others for their support of my FISA bill, and hope that other Senators will join our efforts.

Today, I look forward to the testimony of the Government witnesses and outside experts. I am particularly grateful for the participation of Judge Carr, a current member of the judiciary and a former judge of the FISA Court. I hope that today's hearing will provide an opportunity for an open debate about the law, the policy, and the FISA Court process that led us to this point. We must do all that we can to ensure our nation's security while protecting the fundamental liberties that make this country great.

#####

PREPARED STATEMENT OF JAMES M. COLE

**Opening Statement of Deputy Attorney General James M. Cole
Before the Senate Judiciary Committee, July 31, 2013, 9:00am**

Thank you, Mr. Chairman, Mr. Ranking Member and members of the committee, for inviting us here to speak about the 215 business records program and section 702 of FISA. With these programs and other intelligence activities, we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties. We believe these two programs have achieved the right balance.

First of all, both programs are conducted under public statutes passed and later reauthorized by Congress. Neither is a program that has been hidden away or off the books. In fact, all three branches of government play a significant role in the oversight of these programs. The Judiciary – through the Foreign Intelligence Surveillance Court – plays a role in authorizing the programs and overseeing compliance; the Executive Branch conducts extensive internal reviews to ensure compliance; and Congress passes the laws, oversees our implementation of those laws, and determines whether or not the current laws should be reauthorized and in what form.

Let me explain how this has worked in the context of the 215 program. The 215 program involves the collection of metadata from telephone calls. These are

telephone records maintained by the phone companies. They include the number a call was dialed from, the number the call was dialed to, the date and time of the call, and the length of the call. The records do not include names or other personal identifying information, they do not include cell site or other location information, and they do not include the content of any phone calls. These are the kinds of records that under longstanding Supreme Court precedent are not protected by the Fourth Amendment.

The short court order you have seen published in the newspapers only allows the government to acquire the phone records; it does not allow the government to access or use them. The terms under which the government may access or use the records is covered by another, more detailed court order. That other court order provides that the government can only search the data if it has a “reasonable, articulable suspicion” that the phone number being searched is associated with certain terrorist organizations. The order also imposes numerous other restrictions on NSA to ensure that only properly trained analysts may access the data, and that they can only access it when the reasonable, articulable suspicion predicate has been met and documented. The documentation of the analyst’s justification is important so that it can be reviewed by supervisors before the search and audited afterwards to ensure compliance.

In the criminal context, the government could obtain the same types of records with a grand jury subpoena, without going to court. But here, we go to the court approximately every 90 days to seek the court's authorization to collect the records. In fact, since 2006, the court has authorized the program on 34 separate occasions by 14 different judges. As part of that renewal process, we inform the court whether there have been any compliance problems, and if there have been, the court will take a very hard look and make sure we have corrected these problems. As we have explained before, the 11 judges on the FISC are far from a rubber stamp; instead, they review all of our pleadings thoroughly, they question us, and they don't approve the order until they are satisfied that we have met all statutory and constitutional requirements.

In addition to the Judiciary, Congress also plays a significant role in this program. The classified details of this program have been extensively briefed to both the Judiciary and Intelligence Committees and their staffs on numerous occasions. If there are any significant issues that arise with the 215 program, those would be reported to the two committees right away. Any significant interpretations of FISA by the Court would likewise be reported to the committees under our statutory obligation to provide copies of any FISC opinion or order that includes a significant interpretation of FISA, along with the accompanying court

documents. All of this reporting is designed to assist the two committees in performing their oversight role with respect to the program.

In addition, Congress plays a role in reauthorizing the provision under which the government has carried out this program since 2006. Section 215 of the PATRIOT Act has been renewed several times since the program was initiated – including most recently for an additional four years in 2011. In connection with the recent renewals of 215 authority, the government provided a classified briefing paper to the House and Senate Intelligence Committees to be made available to all Members of Congress. That briefing paper set out the operation of the program in detail, explained that the government and the FISC had interpreted section 215 to authorize the bulk collection of telephone metadata, and stated that the government was collecting such information. We also made offers to brief any member on the 215 program. The availability of the briefing paper and opportunity of an oral briefing were communicated through letters sent by the Chairs of the Intelligence Committees to all Members of Congress. Thus, although we could not talk publicly about the program at the time – since its existence was properly classified – the Executive Branch took all reasonably available steps to ensure that members of Congress were appropriately informed about the program when they renewed the 215 authority.

I understand that there have been recent proposals to amend section 215 authority to limit the bulk collection of telephone metadata. As the President has said, we welcome a public debate about how best to safeguard both our national security and the privacy of our citizens. Indeed, we will be considering in the coming days and weeks further steps to declassify information and help facilitate that debate. In the meantime, however, we look forward to working with the Congress to determine in a careful and deliberate way what tools can best secure the nation while also protecting our privacy interests.

Although my opening remarks have focused on the 215 program, we stand ready to take your questions on the 702 program. Thank you.

PREPARED STATEMENT OF JOHN C. INGLIS

UNCLASSIFIED

**NSA OPENING STATEMENT
SENATE JUDICIARY COMMITTEE
OPEN HEARING ON MEDIA LEAKS
31 JULY 2013**

Introduction

Mr. Chairman, Mr. Ranking member, members of the committee, thank you for the opportunity to join with my colleagues to brief the committee on issues you've identified in your invitation and opening remarks. I am privileged today to represent the work of thousands of NSA, intelligence community and law enforcement personnel who employ the authorities provided by the combined efforts of the Congress, Federal Courts and the Executive Branch.

For its part, NSA is necessarily focused on the generation of foreign intelligence but we have worked hard and long with counterparts across the US government and allies to ensure that we "discover and connect the dots" -- exercising only those authorities explicitly granted to us and taking care to ensure the protection of civil liberties and privacy.

Per your request, I will briefly describe how NSA implements the two NSA programs leaked to the media almost two months ago, to include their purpose and the controls imposed on their use -- the so-called PRISM program authorized under section 702 of the FISA amendment act (FAA) and the so-called 215 program which authorizes the collection of telephone metadata.

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

I'll start with **Section 702 of the FISA**, which authorizes the targeting of non-U.S. persons abroad for foreign intelligence purposes such as counter-terrorism and counter-proliferation.

- Specifically, Section 702 authorizes the collection of communications for the purpose of Foreign Intelligence with the compelled assistance of an electronic communication service provider.
- Under this authority NSA can collect communications for foreign intelligence purposes only when the person who is the target of our collection is a foreigner who is reasonably believed to be outside the US.
- Section 702 cannot be used to intentionally target:

UNCLASSIFIED

UNCLASSIFIED

- o any US citizen or other US person,
- o any person known to be in the US,
- o OR a person outside the United States if the purpose is to target a person inside the United States

This program is also key to our counterterrorism efforts; information used in greater than 90% of the 54 disrupted terrorism events we have previously cited in public testimony was gained from section 702 authorities.

As one example, we've discussed the case of Najibullah Zazi. NSA analysts, leveraging section 702 to target the email of a Pakistan-based al-Qaida terrorist, discovered that he was communicating with someone about a plot involving explosives. NSA tipped this exchange to the FBI who confirmed that the communicant was actually Denver-based Zazi, who we know now was planning an imminent attack on the New York subway system. Without the tip from FAA 702, the plot may never have been uncovered.

The second program, which we undertake through court orders under **Section 215 of the Patriot Act**, authorizes the collection of telephone metadata only.

- It does not allow the government to listen to anyone's phone calls.
- This program was specifically developed to allow the USG to detect communications between known or suspected terrorists who are operating outside the U.S. who are communicating with potential operatives inside the U.S., a gap highlighted by the attacks of 9/11. *In a phrase this program is focused on detecting terrorist plots that cross the seam between foreign terrorist organizations and the US homeland.* We have previously cited in public testimony, that section 215 made a contribution to 12 of the 13 terror plots with a US nexus, amongst the 54 world-wide plots cited earlier.

On operational value:

In considering operational value, it is important to begin with an understanding of the problem the government is trying to solve.

- It is simply this: If we have intelligence indicating that a foreign-based terrorist organization is plotting an act of terror against the homeland, how would we determine whether there is, in fact, a connection between persons operating overseas and operatives within the US?
- Many will recall that the inability of the US intelligence community to make such a connection between 9/11 hijacker Al Midhar operating in California and an Al Qaeda safe house in Yemen, which was discussed by the 9/11 commission report.

UNCLASSIFIED

UNCLASSIFIED

- NSA had in fact collected the Yemen end of their communications but due to the nature of our collection, had no way of determining the number or the location of Al Midhar on the other end.

So the problem becomes, if you have one telephone number for a person you reasonably believe is plotting an act of terror against the homeland, how do you find possible connections to that number crossing the seam between the homeland and overseas?

In simple terms, you are looking for a needle, *in this case a number*, in a haystack. But not just any number. You want to make a focused query against a body of data that returns only those numbers that are connected to the one you have reasonable suspicion is connected to a terrorist group.

But unless you have the haystack – in this case all the records of who called whom – you cannot answer the question. The confidence you will have in any answers returned by your query is necessarily tied to whether the haystack constitutes a reasonably complete set of records and whether those records look back a reasonable amount of time to enable you to discover a connection between conspirators who might plan and coordinate across several years.

Hence “all” the records are necessary to connect the dots of an ongoing plot, sometimes in a time sensitive situation, even if only an extremely small fraction of them is ever determined to be the match you’re looking for.

The authorities work in concert

As I mentioned at the outset, these authorities work together to enable our support to counter-terrorism. A counter-terrorism investigation is the product of many leads, a handful of which may prove to be decisive. It is impossible to know which tool is going to generate the decisive lead in any particular case. In some cases, the leads may corroborate a lead FBI is already following; in others, it may help them prioritize leads for further investigation; in still others it may yield a number that was previously unknown to them. These leads results in threat assessments, preliminary investigations and full investigations; in some cases, the data from the program yields no results, helping to disprove leads and conserve investigative resources. This is the way we would want these programs to work: adding dots, affirming them, connecting them, and in so doing contributing key pieces to the larger intelligence picture.

Using the Zazi case, once FBI confirmed Zazi’s identity, they passed NSA his phone number, for which NSA then made a determination of “Reasonable Articulate Suspicion”, and used the number to search the 215 database. Based on that search NSA analysts discovered a previously unknown number in communication with Zazi for a man named Adis Medunjanin. While FBI had previously been aware of Medunjanin, the direct and recent connection to Zazi as well as another us-based extremist focused

UNCLASSIFIED

UNCLASSIFIED

the FBI's attention on him as a key lead in the plot. as you know, both Zazi and Medunjanin have been convicted for their role in the plot.

Controls and Limitations:

The limitations and controls imposed on the use of both of these programs are significant.

For the 215 metadata these controls are laid out in the FISA court's "primary order" which the executive branch has declassified this morning so that it might provide context for the court's "secondary order", leaked earlier in the press, but which only dealt with the collection of the data.

Under rules imposed by the Primary Order:

- The metadata acquired and stored under the 215 authority may be queried only when there is a reasonable suspicion based on specific facts that a "selector"—which is typically a phone number—is associated with specific foreign terrorist organizations.
- Under rules approved by the court, only 22 people at NSA are allowed to approve the selectors used to initiate a search in this data base; all queries are audited; only seven positions at NSA (a total of 11 people) are authorized to release query results that are believed to be associated with persons in the US.
- Reports are filed with the court every 30 days that specify the number of selectors approved, and disseminations made to the FBI that contain numbers believed to be in the US.
- And, while the data acquired under this authority might theoretically be useful in other intelligence activities or law enforcement investigations, its use for any other purpose than that which I've described is prohibited.

With this capability, we are very mindful that we must use it conservatively and judiciously, in close concert with our law enforcement colleagues and focused on the seam between foreign terrorist groups and potential domestic actors.

- During 2012, we only initiated queries for information in this dataset using fewer than 300 unique selectors. The information returned from these queries only included phone numbers, not the content, identity, or location of the called or calling party. And in 2012, based on those fewer than 300 selectors, we provided a total of 12 reports to FBI, which altogether 'tipped' less than 500 numbers.

The 702 program operates under equally strict controls that, while ensuring our efforts are focused on the collection of foreign intelligence, specifically address how analysts should handle incidentally collected US person communications.

UNCLASSIFIED

UNCLASSIFIED

When NSA targets a terrorist overseas, they may sometimes communicate with persons in the US (anyone in the US, a US citizen or foreign person, is considered a US person). That's what we call "incidental collection."

If the case of a communication involving a US person, we have court approved minimization procedures that we must follow.

- This was the case with Najibullah Zazi. As I mentioned, we intercepted that communication using 702 collection by focusing on the Pakistani based al-Qa'ida terrorist.
- While it was not completely clear from the communication who Zazi was or where he was located, NSA analysts immediately tipped this exchange to the FBI who confirmed that Zazi was in fact in Denver and subsequently acquired a warrant to target and access the content of his communications.
- Without that initial 702 tip from NSA, which came as a result of targeting an al-Qa'ida terrorist located overseas, the plot may never have been discovered.
- This tip was handled in complete accordance with the applicable minimization procedures which authorized NSA to disseminate information of or concerning a US person if the US person information is necessary to understand or assess foreign intelligence information.
- Finally, NSA cannot reverse target, i.e. target a foreign person overseas if the intent is to target the communications of a person in the US.

We do of course have tools that allow analysts to conduct focused searches of our holdings and listen to the content of legally acquired collection concerning foreign intelligence targets. Given that these communications have been shown to bear on our foreign intelligence mission, we must and do review them. But the purpose is to glean foreign intelligence and the rules for protecting the identities and communications of US persons are both clear and followed.

Looking forward:

Policy makers across the executive and legislative branches will ultimately decide whether we want to sustain or dispense with a tool designed to detect terrorist plots across the seam between foreign and domestic domains. Different implementations of the program can address the need, but each should be scored against several key attributes:

- Privacy concerns must be addressed through controls and accountability;
- It should be possible to make queries in a timely manner so that, in the most demanding case, results can support disruption of imminent plots;
- The database must be reasonably complete across providers and time to yield so that we can have confidence in the answers it yields about whether there is, or is not, a terrorist plot in play; and

UNCLASSIFIED

UNCLASSIFIED

- The data architecture is constructed in a manner that allows efficient follow-up queries to any selector that shows connections to other numbers of legitimate relevance to an ongoing plot.

Conclusion

Our primary responsibility is to defend the Nation. The programs we are discussing today are a core part of those efforts. We use them to protect the lives of Americans and our allies and partners worldwide.

Over 100 nations are capable of collecting Signals Intelligence or operating a lawful intercept capability that enable them to monitor communications.

- I think our Nation is amongst the best at protecting our privacy and civil liberties.
- We look forward to the discussions here and, if necessary, at classified sessions to more fully explore your questions BUT I note that the leaks that have taken place thus far will cause serious damage to our intelligence capabilities.
- More to the point, the irresponsible release of classified information will have a long-term detrimental impact on the Intelligence Community's ability to detect and help deter future attacks.
- The men and women of NSA are committed to compliance with the law and the protection of privacy and civil liberties. The solutions they develop and the actions they take defend the Constitution and the American people, both their physical safety and their right to privacy. We train them from their first day at work and throughout their career.
- This is also true of contractors. The actions of one contractor should not tarnish all the contractors because they do great work for our nation, as well.
- Allegations that low level analysts at NSA can exercise independent discretion beyond these controls to target communications is simply wrong.

Finally, whatever further choices the Nation makes on this matter in consultation and collaboration across the three branches of government, NSA will faithfully implement them – in both spirit and mechanism. To do otherwise would be to fail in the only oath we take – to support and defend the Constitution of the United States – to include protection of both National Security and Civil Liberties.

UNCLASSIFIED

PREPARED STATEMENT OF JAMES G. CARR

**Senate Judiciary Committee Hearing
“Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs”
July 31, 2013**

**Prepared Remarks of James G. Carr,
Sr. U.S. District Judge
N.D. Ohio**

Having been asked to appear here following the publication in the *New York Times* on July 23, 2013, of an op-ed article suggesting an amendment to the Foreign Intelligence Act, I do so with the caveat that whatever I say – or have written – on the subject of the op-ed expresses my views alone. I do not mean to bypass the normal process by which the Judiciary proposes legislation. I speak for myself and no one else.

The proposal I made in the op-ed piece is whether it would be worthwhile for the judges of the Foreign Intelligence Surveillance, when a government FISA application raises a new or novel issue of constitutional or statutory interpretation, to have discretion to designate a previously security-cleared attorney to challenge the government’s request.

Such appointment would not be frequent, and would not occur in the routine kind of cases making up the day in, day out docket of the Foreign Intelligence Surveillance Court (FISC). Rarely does a FISA application present any challenging issues under the statute. The probable cause standard is much lower than for a conventional search warrant. Once the government meets that standard, judges must issue the FISA order.

Once in a very great while, however, a FISA application raises a novel, substantial, and very difficult issue of law. In such circumstances, the FISC judge (or judges, sitting en banc) may desire to hear not just the government’s views in support of the request, but reasons from an independent attorney as to why the court should not issue the order in whole or part.

This process would give the court the benefit of the give and take that is the hallmark of the adversarial process.

In addition, review by the Foreign Intelligence Court of Review would occur, as it does not now, where the government had prevailed before the FISC. Today, only the government, as the only party before the FISC, is in a position to appeal, which it is not likely to do where the FISC has granted its request.

Where such review were available and pursued, public concern about the decisions of the FISC should moderate. This would be so, whether or not the opinion of the Court of Review became public.

If implemented, my recommendation about appointment of counsel would also make possible ultimate review by the Supreme Court.

I can foresee at least one objection to what I propose. Namely, no one besides the government appears when the government seeks an ordinary search warrant in a conventional criminal investigation. But the subject of a conventional Fourth Amendment search warrant knows of its execution, can challenge its lawfulness if indicted, and can, even if not indicted, seek to recover seized property or possibly sue for damages.

In contrast, except in very, very rare instances, suppression or other means of challenging the lawfulness of a FISA order is simply not available to the subject of a FISA order. Even on the infrequent occasion when a FISA target becomes charged in a criminal case, he will, as a result of the procedures mandated in the Classified Information Procedures Act almost never have the opportunity to challenge the FISA order.

Thus, although all conventional search warrants issue *ex parte*, their execution informs the subject of the warrant's issuance. Once the subject knows of the warrant, the law gives that subject several ways in which to challenge the lawfulness of the warrant and search. This is not so with a FISA order.

Another concern would arise where the FISC must, due to emergency circumstances, act immediately. The FISA already authorizes the government to act without a FISA order in emergency circumstances. In such cases, it must still seek *post hoc* FISC approval for the surveillance. In such circumstances, the FISC judge could designate counsel at that stage. In any event, new constitutional issues probably would not arise in emergency circumstances.

My recommendation, while offering some substantial potential benefits to the court's processes and public generally, is very modest. It would not affect the court's day to day operations. It would remain for an individual judge to determine whether to invoke this option on the infrequent occasion that the judge concluded doing so would be useful.

Finally, I emphasize again that these comments, and anything that I may say in response to the Committee's questions, express my views alone, not those of the Federal Judiciary, any other judge, or any one else. While I think what I ask the Committee to consider is worthwhile, only time can tell whether others do as well.

Thank you for this opportunity to submit these Remarks and the attached copy of the op-ed piece which is the occasion for my being here.

###

PREPARED STATEMENT OF JAMEEL JAFFER



Testimony of

Jameel Jaffer

Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy

Director, Washington Legislative Office
American Civil Liberties Union

Before

The Senate Judiciary Committee

Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs

July 31, 2013

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting the ACLU to testify before the Committee.

Over the last two months it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans' telephone calls and electronic communications. These unconstitutional surveillance programs are the product of defects both in the law itself and in the current oversight system. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government's surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly

used procedural doctrines to place the NSA's activities beyond the reach of the Constitution.

To say that the NSA's activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance "threaten[ed] to undermine our democratic society and fundamentally alter its nature." This warning should have even more resonance today, because in recent decades the NSA's resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately.

First, it should amend relevant provisions of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA's so-called "business records" provision, and to the national security letter authorities.

Second, it should end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Third, it should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.

Thank you again for the invitation to testify. We appreciate the Committee's attention to this set of issues.

I. Metadata surveillance under Section 215 of the Patriot Act

On June 5, 2013, *The Guardian* disclosed a previously secret FISC order that compels a Verizon subsidiary, Verizon Business Network Services (VBNS), to supply the government with records relating to every phone call placed on its network between

April 25, 2013 and July 19, 2013.¹ The order directs VBNS to produce to the NSA “on an ongoing daily basis . . . all call detail records or ‘telephony metadata’” relating to its customers’ calls, including those “wholly within the United States.”² As many have noted, the order is breathtaking in its scope. It is as if the government had seized every American’s address book—with annotations detailing which contacts she spoke to, when she spoke with them, for how long, and (possibly) from which locations.

News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans’ call details extends beyond customers of VBNS, encompassing subscribers of the country’s three largest phone companies: Verizon, AT&T, and Sprint.³ Members of the congressional intelligence committees have confirmed that the order issued to VBNS is part of a broader program under which the government has been collecting the telephone records of essentially all Americans for at least seven years.⁴

Intelligence officials have said that the government does not “indiscriminately sift through” the phone-record database. Instead, it queries the database “only when there is reasonable suspicion, based on specific and articulated facts, that an identifier is associated with specific foreign terrorist organizations.”⁵ According to a statement released by the government last month, “less than 300 unique identifiers met this standard and were queried” in 2012.⁶ But even if the government ran queries on only 300 unique identifiers in 2012, those searches implicated the privacy of millions of Americans. Intelligence officials have explained that analysts are permitted to examine the call

¹ See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, June 5, 2013, <http://bit.ly/13jsdlb>.

² Secondary Order, *In Re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Comm’n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), available at <http://bit.ly/11FY393>.

³ See Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, <http://on.wsj.com/11uD0ue> (“The arrangement with Verizon, AT&T and Sprint, the country’s three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total.”); Siobhan Gorman & Jennifer Valentino-DeVries, *Government Is Tracking Verizon Customers’ Records*, Wall St. J., June 6, 2013, <http://on.wsj.com/13mLm7c>.

⁴ Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place ‘Since 2006.’* Guardian, June 6, 2013, <http://bit.ly/13rfdxdu>; *id.* (Senator Saxby Chambliss: “This has been going on for seven years.”).

⁵ See, e.g., *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Intelligence Comm.*, 113th Cong. (June 18, 2013) (testimony of NSA Deputy Director John C. Inglis), <http://bit.ly/15kZ9wh>.

⁶ See, e.g., Ellen Nakashima, *Call Records of Fewer Than 300 People Were Searched in 2012, U.S. Says*, Wash. Post, June 15, 2013, <http://wapo.st/148Z7Wm>.

records of all individuals within three “hops” of a specific target.⁷ As a result, a query yields information not only about the individual thought to be “associated with [a] specific foreign terrorist organization[]” but about all of those separated from that individual by one, two, or three degrees. Even if one assumes, conservatively, that each person has an average of 40 unique contacts, an analyst who accessed the records of everyone within three hops of an initial target would have accessed records concerning more than two million people.⁸ Multiply that figure by the 300 phone numbers the NSA says that it searched in 2012, and by the seven years the program has apparently been in place, and one can quickly see how official efforts to characterize the extent and impact of this program are deeply misleading.

a. The metadata program is not authorized by statute

The metadata program has been implemented under Section 215 of the Patriot Act—sometimes referred to as FISA’s “business records” provision—but this provision does not permit the government to track all Americans’ phone calls, let alone over a period of seven years.

As originally enacted in 1998, FISA’s business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international terrorism investigations by making an application to the FISC. *See* 50 U.S.C. §§ 1861-62 (2000 ed.). Only four types of records could be sought under the statute: records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862 (2000 ed.). Moreover, the FISC could issue an order only if the application contained “specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power.” *Id.*

The business records power was considerably expanded by the Patriot Act.⁹ Section 215 of that Act, now codified in 50 U.S.C. § 1861, permitted the FBI to make an application to the FISC for an order requiring

the production of *any tangible things* (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities

50 U.S.C. § 1861(a)(1) (emphasis added).

⁷ *See* Pete Yost, *Congress Expresses Anger Over NSA Surveillance Program*, Boston Globe, July 18, 2013, <http://b.globe.com/17moqWU>.

⁸ *Id.*

⁹ For ease of reference, this testimony uses “business records provision” to refer to the current version of the law as well as to earlier versions, even though the current version of the law allows the FBI to compel the production of much more than business records, as discussed below.

No longer limited to four discrete categories of business records, the new law authorized the FBI to seek the production of “any tangible things.” *Id.* It also authorized the FBI to obtain orders without demonstrating reason to believe that the target was a foreign power or agent of a foreign power. Instead, it permitted the government to obtain orders where tangible things were “sought for” an authorized investigation. P.L. 107-56, § 215. This language was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b). Under the current version of the business records provision, the FBI must provide “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant*” to a foreign intelligence, international terrorism, or espionage investigation. 50 U.S.C. § 1861(b)(2)(A) (emphasis added).¹⁰

While the Patriot Act considerably expanded the government’s surveillance authority, Section 215 does not authorize the metadata program. First, whatever “relevance” might allow, it does not permit the government to cast a seven-year dragnet over the records of every phone call made or received by any American. Indeed, to say that Section 215 authorizes this surveillance is to deprive the word “relevance” of any meaning. The government’s theory appears to be that some of the information swept up in the dragnet might become relevant to “an authorized investigation” at some point in the future. The statute, however, does not permit the government to collect information on this basis. *Cf.* Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, Guardian, June 9, 2013, <http://bit.ly/18iDA3x> (“[B]ased on the scope of the released order, both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended.”). The statute requires the government to show a connection between the records it seeks and some specific, existing investigation.

Indeed, the changes that Congress made to the statute in 2006 were meant to ensure that the government did not exploit ambiguity in the statute’s language to justify the collection of sensitive information not actually connected to some authorized investigation. As Senator Jon Kyl put it in 2006, “We all know the term ‘relevance.’ It is a term that every court uses. The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation.”¹¹

As Congress recognized in 2006, relevance is a familiar standard in our legal system. It has never been afforded the limitless scope that the executive branch is

¹⁰ Records are presumptively relevant if they pertain to (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This relaxed standard is a significant departure from the original threshold, which, as noted above, required an individualized inquiry.

¹¹ Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court’s Redefinition of ‘Relevant’ Empowered Vast NSA Data-Gathering*, Wall St. J., July 8, 2013, <http://on.wsj.com/13x8QKU>.

affording it now. Indeed, in the past, courts have carefully policed the outer perimeter of “relevance” to ensure that demands for information are not unbounded fishing expeditions. *See, e.g., In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (“What is more troubling is the matter of relevance. The [grand jury] subpoena requires production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.”).¹² The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of “relevance.”¹³

b. The metadata program is unconstitutional

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans’ phone records, it clearly is.

The Supreme Court’s recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual’s location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual’s movements over an extended period allows the government to generate a “precise, comprehensive record” that reflects “a wealth of detail about her familial, political, professional, religious, and sexual associations.” *Id.* (Sotomayor, J., concurring).

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles she reads, whom she corresponds with, and whom *those* people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in *Jones*. In fact, the surveillance held unconstitutional in *Jones* was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in *Jones* was meant to further a specific criminal investigation into a specific crime, and the

¹² *See also Hale v. Henkel*, 201 U.S. 43, 76-77 (1906).

¹³ The metadata program also violates Section 215 because the statute does not authorize the prospective acquisition of business records. The text of the statute contemplates “release” of “tangible things” that can be “fairly identified,” and “allow[s] a reasonable time” for providers to “assemble[.]” those things. 50 U.S.C. § 1861(c)(1)-(2). These terms suggest that Section 215 reaches only business records already in existence.

government collected information about one person's location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Some have defended the metadata program by reference to the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in *Smith*, however, was very primitive—it tracked the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country.

Another argument that has been offered in defense of the metadata program is that, though the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the *collection* of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans' private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans' private papers and communications in the first place.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. *See, e.g., United States v. U.S. District Court*, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to "exacting scrutiny" where they substantially burden First Amendment rights. *See, e.g., Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government's legitimate goals. *See, e.g., Press Release, Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks*, June 7, 2013, <http://1.usa.gov/19Q1Ng1> ("As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.").

c. Congress should amend Section 215 to prohibit suspicionless, dragnet collection of "tangible things"

As explained above, the metadata program is neither authorized by statute nor constitutional. As the government and FISC have apparently found to the contrary, however, the best way for Congress to protect Americans' privacy is to narrow the statute's scope. The ACLU urges Congress to amend Section 215 to provide that the

government may compel the production of records under the provision only where there is a close connection between the records sought and a foreign power or agent of a foreign power. Several bipartisan bills now in the House and Senate should be considered by this Committee and Congress at large. The LIBERT-E Act, H.R. 2399, 113th Cong. (2013), sponsored by Rep. Conyers, Rep. Justin Amash, and forty others, would tighten the relevance requirement, mandating that the government supply “specific and articulable facts showing that there are reasonable grounds to believe that the tangible things sought are relevant and material,” and that the records sought “pertain only to an individual that is the subject of such investigation.” A bill sponsored by Senators Udall and Wyden, and another sponsored by Senator Leahy, would also tighten the required connection between the government’s demand for records and a foreign power or agent of a foreign power. Congress could also consider simply restoring some of the language that was deleted by the Patriot Act—in particular, the language that required the government to show “specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power.”

II. Electronic surveillance under Section 702 of FISA

The metadata program is only one part of the NSA’s domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans’ electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008.¹⁴ Under this program, labeled “PRISM” in NSA documents, the government collects emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.¹⁵ The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it involves surveillance of foreigners outside the United States.¹⁶ This is misleading. The PRISM program involves the collection of Americans’ communications, both international and domestic, and for reasons explained below, the program is unconstitutional.

¹⁴ Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, <http://wapo.st/1888aNr>.

¹⁵ While news reports have generally described PRISM as an NSA “program,” the publicly available documents leave open the possibility that PRISM is instead the name of the NSA database in which content collected from these providers is stored.

¹⁶ James R. Clapper, DNI Statement on Activities Authorized Under Section 702 of FISA, Office of the Director of National Intelligence (June 6, 2013), <http://1.usa.gov/13JJdBE>; *see also* James R. Clapper, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), <http://1.usa.gov/10YY4tp>.

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.¹⁷ While leaving FISA in place for purely domestic communications, the FISA Amendments Act revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications. Under the FISA Amendments Act, the Attorney General and Director of National Intelligence ("DNI") can "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881a(a). The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," *id.* § 1881a(b)(1), but an acquisition authorized under the FISA Amendments Act may nonetheless sweep up the international communications of U.S. citizens and residents.

Before authorizing surveillance under Section 702—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a "mass acquisition order"). *Id.* § 1881a(a), (c)(2). A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year.

To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court "a written certification and any supporting affidavit" attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "targeting procedures" reasonably designed to ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id.* § 1881a(g)(2)(A)(i).

The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "minimization procedures" that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in

¹⁷ A description of electronic surveillance prior to the passage of the FISA Amendments Act, including the warrantless wiretapping program authorized by President Bush beginning in 2001, is available in Mr. Jaffer's earlier testimony to the House Judiciary Committee. See *The FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security*, H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (written testimony of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union Foundation), available at <http://bit.ly/14Q61Bs>.

§ 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that “a significant purpose of the acquisition is to obtain foreign intelligence information.” *Id.* § 1881a(g)(2)(A)(iii)–(vii).

Importantly, Section 702 does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government’s certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. *Id.* § 1881a(g)(4).

Nor does Section 702 place meaningful limits on the government’s retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt “minimization procedures,” *id.* § 1881a, that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons,” *id.* §§ 1801(h)(1), 1821(4)(A). The Act does not, however, prescribe specific minimization procedures. Moreover, the FISA Amendments Act specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is “foreign intelligence information.” *Id.* § 1881a(e) (referring to *id.* §§ 1801(h)(1), 1821(4)(A)). The phrase “foreign intelligence information” is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs. *Id.* § 1801(e).

As the FISA Court has itself acknowledged, its role in authorizing and supervising surveillance under the FISA Amendments Act is “narrowly circumscribed.”¹⁸ The judiciary’s traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FISA Amendments Act is to issue advisory opinions blessing in advance broad parameters and targeting procedures, under which the government is then free to conduct surveillance for up to one year. Under Section 702, the FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not closely supervise the implementation of the government’s targeting or minimization procedures. In short, the role that the FISA Court plays under the FISA Amendments Act bears no resemblance to the role that it has traditionally played under FISA.

¹⁸ *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), available at <http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf>.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.¹⁹ The statute's defects include:

- *Section 702 allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored.*

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

- *Section 702 allows the government to conduct intrusive surveillance without meaningful judicial oversight.*

Under Section 702, the government is authorized to conduct intrusive surveillance without meaningful judicial oversight. The FISA Court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is initiating any particular surveillance program. The FISA Court's role is limited to reviewing the government's "targeting" and "minimization"

¹⁹ The ACLU raised many of these defects in a constitutional challenge to the FISA Amendments Act filed just hours after the Act was signed into law in 2008. The case, *Amnesty v. Clapper*, was filed on behalf of a broad coalition of attorneys and human rights, labor, legal and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and email communications with individuals located outside the United States. In a 5-4 ruling handed down on February 26, 2013, the Supreme Court held that the ACLU's plaintiffs did not have standing to challenge the constitutionality of the Act because they could not show, at the outset, that their communications had been monitored by the government. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). The Court did not reach the merits of plaintiffs' constitutional challenge.

procedures. And even with respect to the procedures, the FISA court's role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time.

- *Section 702 places no meaningful limits on the government's retention and dissemination of information relating to U.S. citizens and residents.*

As a result of the FISA Amendments Act, thousands or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is "targeted" at people abroad. Yet the law fails to place any meaningful limitations on the government's retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt "minimization" procedures—procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." However, these minimization procedures must accommodate the government's need "to obtain, produce, and disseminate foreign intelligence information." In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is "foreign intelligence information." Because "foreign intelligence information" is defined broadly (as discussed below), this is an exception that swallows the rule.

- *Section 702 does not limit government surveillance to communications relating to terrorism.*

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather "foreign intelligence information." There are multiple problems with this. First, under the new law the "foreign intelligence" requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase "foreign intelligence information" has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the "foreign affairs of the United States." Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

b. The NSA's "targeting" and "minimization" procedures do not mitigate the statute's constitutional deficiencies

Since the FISA Amendments Act was enacted in 2008, the government's principal defense of the law has been that "targeting" and "minimization" procedures supply sufficient protection for Americans' privacy. Because the procedures were secret, the government's assertion was impossible to evaluate. Now that the procedures have

been published, however,²⁰ it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans’ communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans’ international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans’ privacy are weak and riddled with exceptions.

- *The NSA’s procedures permit it to monitor Americans’ international communications in the course of surveillance targeted at foreigners abroad.*

While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans’ communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans’ international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans’ communications that contain “foreign intelligence information” or evidence of a crime can be retained forever, and even communications that don’t can be retained for as long as five years. Despite government officials’ claims to the contrary, the NSA is building a growing database of Americans’ international telephone calls and emails.

- *The NSA’s procedures allow the surveillance of Americans by failing to ensure that its surveillance targets are in fact foreigners outside the United States.*

The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA’s procedures fail to ensure that its surveillance targets are *in fact* foreigners outside the United States. This is because the procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

- *The NSA’s procedures permit the government to conduct surveillance that has no real connection to the government’s foreign intelligence interests.*

One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the

²⁰ See Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, Guardian, June 20, 2013, <http://bit.ly/105qb9B>.

FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather “foreign intelligence information.” As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even “the foreign affairs of the United States.” The NSA’s procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner’s address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA’s surveillance.

- *The NSA’s procedures permit the NSA to collect international communications, including Americans’ international communications, in bulk.*

On its face, Section 702 permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the FISA Amendments Act made clear that this was one of its principal purposes, and unsurprisingly, the procedures give effect to that design. While they require the government to identify a “target” outside the country, once the target has been identified the procedures permit the NSA to sweep up the communications of any foreigner who may be communicating “about” the target. The Procedures contemplate that the NSA will do this by “employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas,” by “target[ing] Internet links that terminate in a foreign country,” or by identifying “the country code of the telephone number.” However the NSA does it, the result is the same: millions of communications may be swept up, Americans’ international communications among them.

- *The NSA’s procedures allow the NSA to retain even purely domestic communications.*

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic.²¹ The Act should require the NSA to purge these communications from its databases, but it does not. The procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly.

²¹ Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in “significant and systemic” overcollection of such domestic communications. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, April 15, 2009, <http://nyti.ms/16A1q5O>.

- *The NSA's procedures allow the government to collect and retain communications protected by the attorney-client privilege.*

The procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

c. Congress should amend Section 702 to prohibit suspicionless, dragnet collection of Americans' communications

For the reasons discussed above, the ACLU believes that the FISA Amendments Act is unconstitutional on its face. There are many ways, however, that Congress could provide meaningful protection for privacy while preserving the statute's broad outline. One bill introduced by Senator Wyden during the reauthorization debate last fall would have prohibited the government from searching through information collected under the FISA Amendments Act for the communications of specific, known U.S. persons. Bills submitted during the debate leading up to the passage of the FISA Amendments Act in 2008 would have banned dragnet collection in the first instance or required the government to return to the FISC before searching communications obtained through the FISA Amendments Act for information about U.S. persons. Congress should examine these proposals again and make amendments to the Act that would provide greater protection for individual privacy and mitigate the chilling effect on rights protected by the First Amendment.

III. Excessive secrecy surrounds the government's use of FISA authorities

Amendments to FISA since 2001 have substantially expanded the government's surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of Congress and the public have learned more about domestic surveillance in last two months than in the last several decades combined. While the Judiciary and Intelligence Committees have received some information in classified format, only members of the Senate Select Committee on Intelligence, party leadership, and a handful of Judiciary Committee members have staff with clearance high enough to access the information and advise their principals. Although the Inspectors General and others file regular reports with the Committees of jurisdiction, these reports do not include even basic information such how many Americans' communications are swept up in these programs, or how and when Americans' information is accessed and used.

Nor does the public have access to the FISC decisions that assess the meaning, scope, and constitutionality of the surveillance laws. Aggregate statistics alone would not allow the public to understand the reach of the government's surveillance powers; as we have seen with Section 215, one application may encompass millions of individual records. Public access to the FISA Court's substantive legal reasoning is essential. Without it, some of the government's most far-reaching policies will lack democratic legitimacy. Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.²² Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA's sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such opinions, some close to one hundred pages long.²³ Executive officials testified before Congress several years ago that declassification review was already underway,²⁴ and President Obama directed the DNI to revisit that process in the last few weeks. If the administration refuses to release these opinions, Congress should consider legislation compelling their release.

Congress should also require the release of information about the type and volume of information that is obtained under dragnet surveillance programs. The leaked Verizon order confirms that the government is using Section 215 to collect telephony metadata about every phone call made by VBNS subscribers in the United States. That the government is using Section 215 for this purpose raises the question of what other "tangible things" the government may be collecting through similar dragnets. For reasons discussed above, the ACLU believes that these dragnets are unauthorized by the statute as well as unconstitutional. Whatever their legality, however, the public has a right to know, at least in general terms, what kinds of information the government is collecting about innocent Americans, and on what scale.

IV. National Security Letters

The ACLU has a number of serious concerns with the national security letter (NSL) statutes. In this testimony, we focus on only two. The first is that the NSL statutes allow executive agencies (usually the FBI) to obtain records about people who are not known or even suspected to have done anything wrong. They allow the

²² See, e.g., Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, <http://wapo.st/170VVSu>.

²³ See Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, <http://nyti.ms/12beiA3>.

²⁴ Prehearing Questions for Lisa O. Monaco Upon Her Nomination to be the Assistant Attorney General for National Security, Sen. Select Comm. on Intelligence, 112th Cong., at 12-13, available at <http://bit.ly/10V51on>.

government to collect information, sometimes very sensitive information, not just about suspected terrorists and spies but about innocent people as well. The second concern is that the NSL statutes allow government agencies (again, usually the FBI) to prohibit NSL recipients from disclosing that the government sought or obtained information from them. This authority to impose non-disclosure orders—gag orders—is not subject to meaningful judicial review. Indeed, as discussed below, the review contemplated by the NSL statutes is no more than cosmetic.²⁵

a. The NSL statutes invest the FBI with broad authority to collect constitutionally protected information pertaining to innocent people

Several different statutes give executive agencies the power to issue NSLs.²⁶ Most NSLs, however, are issued by the FBI under 18 U.S.C. § 2709,²⁷ which was originally

²⁵ The ACLU has a number of other concerns with the NSL statutes. First, the statutes do not significantly limit the retention and dissemination of NSL-derived information. *See, e.g.*, 18 U.S.C. § 2709(d) (delegating to the Attorney General the task of determining when, and for what purposes, NSL-derived information can be disseminated). Second, the statutes provide that courts that hear challenges to gag orders must review the government’s submissions *ex parte* and *in camera* “upon request of the government”; this language could be construed to foreclose independent consideration by the court of the constitutional ramifications of denying the NSL recipient access to the evidence that is said to support a gag order. 18 U.S.C. § 3511(e). *But see Doe v. Gonzales*, 500 F. Supp. 2d 379, 423-24 (S.D.N.Y. 2007) (construing statute more narrowly). Third, the statutes provide that courts that hear challenges to gag orders must seal documents and close hearings “to the extent necessary to prevent an unauthorized disclosure of a request for records”; this language could be construed to divest the courts of their constitutional responsibility to decide whether documents should be sealed or hearings should be closed. 18 U.S.C. § 3511(d). *But see Doe*, 500 F. Supp. 2d at 423-24 (finding that statute “in no way displaces the role of the court in determining, in each instance, the extent to which documents need to be sealed or proceedings closed and does not permit the scope of such a decision to be made unilaterally by the government”).

²⁶ For instance, under 12 U.S.C. § 3414(a)(5)(A), the FBI is authorized to compel “financial institutions” to disclose customer financial records. The phrase “financial institutions” is defined very broadly, and encompasses banks, credit unions, thrift institutions, investment banks, pawnbrokers, travel agencies, real estate companies, and casinos. 12 U.S.C. § 3414(d) (adopting definitions in 31 U.S.C. § 5312). Under 15 U.S.C. § 1681u, the FBI is authorized to compel consumer reporting agencies to disclose “the names and addresses of all financial institutions . . . at which a consumer maintains or has maintained an account,” as well as “identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment.” Under 15 U.S.C. § 1681v, executive agencies authorized to conduct intelligence or counterintelligence investigations can compel consumer reporting agencies to disclose “a consumer report of a consumer and all other information in a consumer’s file.” Still another statute, 50 U.S.C. § 436 empowers “any authorized investigative agency” to compel financial institutions and consumer reporting agencies to disclose records about agency employees.

enacted in 1986 as part of the Electronic Communications Privacy Act (“ECPA”).²⁸ Since its enactment, the ECPA NSL statute has been amended several times. In its current incarnation, it authorizes the FBI to issue NSLs compelling “electronic communication service provider[s]” to disclose “subscriber information,” “toll billing records information,” and “electronic communication transactional records.”²⁹ An “electronic communication service” is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”³⁰

Because most NSLs are issued under ECPA, this testimony focuses on that statute. All of the NSL statutes, however, suffer from similar flaws.

The ECPA NSL statute implicates a broad array of information, some of it extremely sensitive. Under the statute, an Internet service provider can be compelled to disclose a subscriber’s name, address, telephone number, account name, e-mail address, and credit card and billing information. It can be compelled to disclose the identities of individuals who have visited a particular website, a list of websites visited by a particular individual, a list of e-mail addresses with which a particular individual has corresponded, or the e-mail address and identity of a person who has posted anonymous speech on a political website. As the *Library Connection* case shows, the ECPA NSL statute can also be used to compel the disclosure of library patron records.³¹ Clearly, all of this information is sensitive. Some of it is protected by the First Amendment.³²

Because NSLs can reach information that is sensitive, Congress originally imposed stringent restrictions on their use. As enacted in 1986, the ECPA NSL statute permitted the FBI to issue an NSL only if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent.³³ Since 1986, however, the reach of the law has been extended dramatically. In 1993, Congress relaxed the individualized suspicion requirement, authorizing the FBI to issue an NSL if it could certify that (i)

²⁷ Dep’t of Justice, Office of Inspector General, *A Review of the FBI’s Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, (March 2008), (hereinafter “2008 OIG Report”), at 107, available at <http://1.usa.gov/17PO5al>.

²⁸ See Pub L. No. 99-508, Title II, § 201(a), 100 Stat. 1848 (Oct. 21, 1986) (codified as amended at 18 U.S.C. § 2510 *et seq.*)

²⁹ 18 U.S.C. §§ 2709(a) & (b)(1).

³⁰ *Id.* § 2510(15).

³¹ See *Library Connection v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

³² Cf. *McIntyre v. Ohio Elections Comm.*, 514 U.S. 334, 341-42 (1995) (“[A]n author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”); *Talley v. California*, 362 U.S. 60, 64 (1960) (“Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names.”).

³³ 18 U.S.C. § 2709 (1988).

the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that *either* (a) the subject of the NSL was a foreign power or foreign agent, *or* (b) the subject had communicated with a person engaged in international terrorism or with a foreign agent or power “under circumstances giving reason to believe that the communication concerned international terrorism.”³⁴ In 2001, Congress removed the individualized suspicion requirement altogether and also extended the FBI’s authority to issue NSLs in terrorism investigations. In its current form, the NSL statute permits the FBI to issue NSLs upon a certification that the records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”³⁵

The relaxation and then removal of the individualized suspicion requirement has resulted in an exponential increase in the number of NSLs issued each year. According to an audit conducted by the Justice Department’s OIG, the FBI’s internal database showed that the FBI issued 8,500 NSL requests in 2000, the year before the Patriot Act eliminated the individualized suspicion requirement.³⁶ By comparison, the FBI issued 39,346 NSL requests in 2003; 56,507 in 2004; 47,221 in 2005; and 49,425 in 2006.³⁷ These numbers, though high, substantially understate the number of NSL requests actually issued, because the FBI has not kept accurate records of its use of NSLs. The OIG sampled 77 FBI case files and found 22 percent more NSL requests in the case files than were recorded in the FBI’s NSL database.³⁸ Since 2007, the public has had only partial information about the FBI’s use of its NSL authorities. Neither the FBI nor the Department of Justice annually publish the total number of NSLs; instead, the Department of Justice reports statistics that omit NSLs concerning non-U.S. persons and NSLs strictly for subscriber information—making a true comparison impossible. These partial statistics indicate that the FBI issued 16,804 NSLs seeking information concerning U.S. persons in 2007; 24,744 in 2008; 14,788 in 2009; 24,287 in 2010; 16,511 in 2011; and 15,229 in 2012.³⁹

The statistics and other public information make clear that the executive branch is now using NSLs not only to investigate people who are known or suspected to present threats but also—and indeed principally—to collect information about innocent

³⁴ Pub. L. 103-142, 107 Stat. 1491 (Nov. 17, 1993).

³⁵ 18 U.S.C. § 2709(a) & (b)(1) (2006).

³⁶ See Dep’t of Justice, Office of Inspector General, *A Review of the Federal Bureau of Investigation’s Use of National Security Letters* (March 2007), (hereinafter “2007 OIG Report”), at xvi, available at <http://bit.ly/16woHoY>.

³⁷ See *id.* at xix; 2008 OIG Report at 9.

³⁸ 2007 OIG Report at 32.

³⁹ See Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Court Orders 1979-2012*, May 4, 2012, <http://bit.ly/cnSWP5> (compiling NSL statistics); Kim Zetter, *Federal Judge Finds National Security Letters Unconstitutional, Bans Them*, *Wired*, Mar. 15, 2013, <http://bit.ly/YzEtgG> (same).

people.⁴⁰ News reports indicate that the FBI has used NSLs “to obtain data not only on individuals it saw as targets but also details on their ‘community of interest’—the network of people that the target was in contact with.”⁴¹ Some of the FBI’s investigations appear to be nothing more than fishing expeditions. In two cases brought the ACLU, the FBI has abandoned its demand for information after the NSL recipient filed suit; that is, the FBI withdrew the NSL rather than try to defend the NSL to a judge.⁴² The agency’s willingness to abandon NSLs that are challenged in court raises obvious questions about the agency’s need for the information in the first place.

The ACLU believes that the current NSL statutes do not appropriately safeguard the privacy of innocent people. Congress should narrow the NSL authorities that allow the FBI to demand information about individuals who are not the targets of any investigation.

b. The NSL statutes allow the FBI to impose gag orders without meaningful judicial review

A second problem with the NSL statutes is that they empower executive agencies to impose gag orders that are not subject to meaningful judicial review.⁴³ Until 2006, the ECPA NSL statute categorically prohibited NSL recipients from disclosing to any person that the FBI had sought or obtained information from them.⁴⁴ Congress amended the statute, however, after a federal district court found it unconstitutional.⁴⁵ Unfortunately, the amendments made in 2006, while addressing some problems with the statute, made the gag provisions even more oppressive. The new statute permits the FBI to decide on a case-by-case basis whether to impose gag orders on NSL recipients but strictly confines the ability of NSL recipients to challenge such orders in court.

As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on

⁴⁰ The statistics also make clear that the FBI is increasingly using NSLs to seek information about U.S. persons. The percentage of NSL requests generated from investigations of U.S. persons increased from approximately 39 percent of NSL requests in 2003 to approximately 57 percent in 2006. 2008 OIG Report at 9.

⁴¹ Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. Times, Sept. 9, 2007; see also Barton Gellman, *The FBI’s Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, Wash. Post, Nov. 6, 2005 (reporting that the FBI apparently used NSLs to collect information about “close to a million” people who had visited Las Vegas).

⁴² See generally *Doe v. Mukasey*, 549 F.3d 861 (2d. Cir. 2008); *Library Connection v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005).

⁴³ All of the NSL statutes authorize the imposition of such gag orders.

⁴⁴ 18 U.S.C. § 2709 (2005).

⁴⁵ *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

any person or entity served with an NSL.⁴⁶ To impose such an order, the Director or his designee must “certify” that, absent the non-disclosure obligation, “there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person.”⁴⁷ If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from “disclos[ing] to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the [FBI] has sought or obtained access to information or records under [the NSL statute].”⁴⁸ Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a “certification” that the gag is necessary, the certification is not examined by anyone outside the executive branch. No judge considers, before the gag order is imposed, whether secrecy is necessary or whether the gag order is narrowly tailored.

The gag provisions permit the recipient of an NSL to petition a court “for an order modifying or setting aside a nondisclosure requirement.”⁴⁹ However, in the case of a petition filed “within one year of the request for records,” the reviewing court may modify or set aside the nondisclosure requirement only if it finds that there is “no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.”⁵⁰ Moreover, if a designated senior government official “certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations,” the certification must be “treated as conclusive unless the court finds that the certification was made in bad faith.”⁵¹

In December 2008, the Second Circuit issued a decision construing the NSL statute (1) to permit a nondisclosure requirement only when senior FBI officials certify that disclosure may result in an enumerated harm that is related to “an authorized investigation to protect against international terrorism or clandestine intelligence

⁴⁶ 18 U.S.C. § 2709(c).

⁴⁷ *Id.* § 2709(c)(1).

⁴⁸ *Id.*

⁴⁹ *Id.* § 3511(b)(1).

⁵⁰ *Id.* § 3511(b)(2).

⁵¹ *Id.* In the case of a petition filed under § 3511(b)(1) “one year or more after the request for records,” the FBI Director or his designee must either terminate the non-disclosure obligation within 90 days or recertify that disclosure may result in one of the enumerated harms. *Id.* § 3511(b)(3). If the FBI recertifies that disclosure may be harmful, however, the reviewing court is required to apply the same extraordinarily deferential standard it is required to apply to petitions filed within one year. *Id.* If the recertification is made by a designated senior official, the certification must be “treated as conclusive unless the court finds that the recertification was made in bad faith.” *Id.*

activities”); (2) to place on the government the burden of showing that a good reason exists to expect that disclosure of receipt of an NSL will risk an enumerated harm; and (3) to require the government, in attempting to satisfy that burden, to adequately demonstrate that disclosure in a particular case may result in an enumerated harm.⁵² The court also invalidated the subsection of the NSL statute that directs the courts to treat as conclusive executive officials’ certifications that disclosure of information may endanger the national security of the United States or interfere with diplomatic relations.⁵³

In addition, the Second Circuit ruled that the NSL statute is unconstitutional to the extent that it imposes a non-disclosure requirement on NSL recipients without placing on the government the burden of initiating judicial review of that requirement.⁵⁴ The court held that this deficiency, however, could be addressed by the adoption of a “reciprocal notice” policy.⁵⁵ Under this policy, the FBI must inform NSL recipients of their right to challenge gag orders. If a recipient indicates its intent to do so, the FBI must initiate court proceedings to establish—before a judge—that the gag order is necessary and consistent with the First Amendment.⁵⁶

Consistent with these judicial rulings, the ACLU supports congressional efforts to ensure that “gag orders” associated with national security letters and other surveillance directives are limited in scope, limited in duration, and imposed only when necessary.

V. Summary of recommendations

For the reasons above, Congress should amend relevant provisions of FISA to prohibit suspicionless, “dragnet” monitoring or tracking of Americans’ communications. Amendments of this kind should be made to the FISA Amendments Act, to FISA’s so-called “business records” provision, and to the national security letter authorities.

Congress should also end the unnecessary and corrosive secrecy that has obstructed congressional and public oversight. It should require the publication of FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should require the government to publish basic statistical information

⁵² *Doe v. Mukasey*, 549 F.3d 861, 883 (2d. Cir. 2008).

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *See id.*

⁵⁶ A district court in the Northern District of California recently issued a similar decision, finding that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and that 18 U.S.C. § 3511(b)(2) and (b)(3) violate the First Amendment and separation of powers principles. *In re Nat’l Sec. Letter*, No. C 11-02173 SI, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013). The court enjoined the government from issuing NSLs under section 2709 or from enforcing the nondisclosure provision in that or any other case. *Id.*

about the government's use of foreign-intelligence authorities. And it should ensure that "gag orders" associated with national security letters and other surveillance directives are limited in scope and duration, and imposed only when necessary.

Finally, Congress should ensure that the government's surveillance activities are subject to meaningful judicial review. It should clarify by statute the circumstances in which individuals can challenge government surveillance in ordinary federal courts. It should provide for open and adversarial proceedings in the FISC when the government's surveillance applications raise novel issues of statutory or constitutional interpretation. It should also pass legislation to ensure that the state secrets privilege is not used to place the government's surveillance activities beyond the reach of the courts.

PREPARED STATEMENT OF STEWART BAKER

Oversight Hearing on FISA Surveillance Programs

Committee on the Judiciary

United States Senate

July 31, 2013

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP

Mr. Chairman, Ranking Member Grassley, members of the Committee, it is an honor to testify before you on such a vitally important topic. The testimony that I give today will reflect my decades of experience in the areas of intelligence, law, and national security. I have practiced national security law as general counsel to the National Security Agency, as general counsel to the Robb-Silberman commission that assessed U.S. intelligence capabilities and failures on weapons of mass destruction, as assistant secretary for policy at the Department of Homeland Security, and in the private practice of law.

To be blunt, one of the reasons I'm here is that I fear we may repeat some of the mistakes we made as a country in the years before September 11, 2001. In those years, a Democratic President serving his second term seemed to inspire deepening suspicion of government and a rebirth of enthusiasm for civil liberties not just on the left but also on the right. The Cato Institute criticized the Clinton Administration's support of warrantless national security searches and expanded government wiretap authority as "dereliction of duty," saying, "[i]f constitutional report cards were handed out to presidents, Bill Clinton would certainly receive an F—an appalling grade for any president—let alone a former professor of constitutional law."¹ The criticism rubbed off on the FISA court, whose chief judge felt obliged to give public interviews and speeches defending against the claim that the court was rubber-stamping the Clinton administration's intercept requests.²

This is where I should insert a joke about the movie "Groundhog Day." But I don't feel like joking, because I know how this movie ends. Faced with civil liberties criticism all across the ideological spectrum, the FISA court imposed aggressive new civil liberties restrictions on government's use of FISA information. As part of its "minimization procedures" for FISA taps, the court required a "wall" between law enforcement and intelligence. And by early 2001, it was enforcing that wall with unprecedented fervor. That was when the court's chief judge harshly disciplined an FBI supervisor for not

¹ Timothy Lynch, *Dereliction Of Duty: The Constitutional Record of President Clinton*, Cato Policy Analysis No. 271 (March 31, 1997), <http://www.cato.org/pubs/pas/pa-271.html>.

² Hon. Royce C. Lamberth, Presiding Judge of the Foreign Intelligence Surveillance Court, Address Before the American Bar Ass'n Standing Comm. on Law and Nat'l Sec. (April 4, 1997), in 19 AMERICAN BAR ASS'N NAT'L SEC. LAW REPORT 2, May 1997, at 1-2.

strictly observing the wall and demanded an investigation that seemed to put the well-regarded agent at risk of a perjury prosecution. A chorus of civil liberties critics and a determined FISA court was sending the FBI a single clear message: the wall must be observed at all costs.

And so, when a law enforcement task force of the FBI found out in August of 2001 that al Qaeda had sent two dangerous operatives to the United States, it did ... nothing. It was told to stand down; it could not go looking for the two al Qaeda operatives because it was on the wrong side of the wall. I believe that FBI task force would have found the hijackers – who weren't hiding – and that the attacks could have been stopped if not for a combination of bad judgment by the FISA court (whose minimization rules were later thrown out on appeal) and a climate in which national security concerns were discounted by civil liberties advocates on both sides of the aisle.

I realize that this story is not widely told, perhaps because it's not an especially welcome story, not in the mainstream media and not on the Internet. But it is true: the parts of my book that describe it are well-grounded in recently declassified government reports.³

More importantly, I lived it. And I never want to live through that particular Groundhog Day again. That's why I'm here.

I am afraid that hyped and distorted press reports orchestrated by Edward Snowden and his allies may cause us – or other nations – to construct new restraints on our intelligence gathering, restraints that will leave us vulnerable to another security disaster.

Intelligence Gathering Under Law

The problem we are discussing today has roots in a uniquely American and fairly recent experiment – writing detailed legal rules to govern the conduct of foreign intelligence. This is new, even for a country that puts great faith in law.

The Americans who fought World War II had a different view; they thought that intelligence couldn't be conducted under any but the most general legal constraints. This may have been a reaction to a failure of law in the run-up to World War II, when U.S. codebreakers were forbidden to intercept Japan's coded radio communications because section 605 of the Federal Communications Act made such intercepts illegal. Finally, in 1939, Gen. George C. Marshall told Navy intelligence officers to ignore the law.⁴ The military successes that followed made the officers look like heroes, not felons.

That view held for nearly forty years, but it broke down in the wake of Watergate, when Congress took a close look at the intelligence community, found abuses, and in 1978

³ STEWART BAKER, *SKATING ON S'ILTS* 66-69 (2010).

⁴ DAVID KAHN, *THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET* 12 (2d ed. 1996).

adopted the first detailed legal regulation of intelligence gathering in history – the Foreign Intelligence Surveillance Act. No other nation has ever tried to regulate intelligence so publicly and so precisely in law.

Forty years later, though, we’re still finding problems with this experiment. One of them is that law changes slowly while technology changes quickly. That usually means Congress has to change the law frequently to keep up. But in the context of intelligence, it’s often hard to explain *why* the law needs to be changed, let alone to write meaningful limits on collection without telling our intelligence targets a lot about our collection techniques. A freewheeling and prolonged debate – and does Congress have any other kind? – will give them enough time and knowledge to move their communications away from technologies we’ve mastered and into technologies that thwart us. The result won’t be intelligence under law; it will be law without intelligence.

Much of what we’ve read in the newspapers lately about the NSA and FISA is the product of this tension. Our intelligence capabilities – and our intelligence gaps – are mostly new since 1978, forcing the government, including Congress, to find ways to update the law without revealing how we gather intelligence.

Section 215 and the Collection-First Model

That provides a useful frame for the most surprising disclosure made by Edward Snowden – that NSA collects telephone metadata (*e.g.*, the called number, calling number, duration of call, etc., but not the call content) for all calls into, out of, or within the United States. Out of context – and Snowden worked hard to make sure it was taken out of context – this is a troubling disclosure. How can all of that data possibly be “relevant to an authorized investigation” as the law requires?

But context is everything here. It turns out that collecting the data isn’t the same as actually looking at it. Robert Litt, General Counsel of the Director for National Intelligence, has made clear that there are court-ordered rules designed to make sure that government officials only look at relevant records: “The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations. And the only purpose for which we can make that query is to identify contacts.”⁵ And in fact these rules have been interpreted so strictly that last year the agency only actually looked at records for 300 subscribers.⁶

Still, isn’t the government “seizing” millions of records without a warrant or probable cause, even if it’s not searching them? “How can that be constitutional?” you might ask.

⁵ Robert Litt, General Counsel, Office of the Director of National Intelligence, Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction (June 26, 2013) (transcript available at <http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction>).

⁶ *Id.*

Very easily, as it happens. The Supreme Court has held that such records are not protected by the Fourth Amendment, since they've already been given to a third party.⁷

And even if the Fourth Amendment applied, at bottom it requires only that seizures be reasonable. The Court has recognized more than half a dozen instances where searches and seizures are reasonable even in the absence of probable cause and a warrant.⁸ They range from drug screening to border searches. There can hardly be doubt that the need to protect national security fits within this doctrine as well, particularly when waiting to conduct a traditional search won't work. Call data doesn't last. If the government doesn't preserve the data now, the government may not be able to search it later, when the need arises.

In short, there's less difference between this "collection first" program and the usual law enforcement data search than first meets the eye. In the standard law enforcement search, the government establishes the relevance of its inquiry and is then allowed to collect and search the data. In the new collection-first model, the government collects the data and then must establish the relevance of each inquiry before it's allowed to conduct a search.

I know it's fashionable to say, "But what if I don't trust the government to follow the rules? Isn't it dangerous to let it collect all that data?" The answer is that the risk of rule-breaking is pretty much the same whether the collection comes first or second. Either way, you have to count on the government to tell the truth to the court, and you have to count on the court to apply the rules. If you don't trust them to do that, then neither model offers much protection against abuses.

But if in fact abuses were common, we'd know it by now. Today, law enforcement agencies collect several hundred thousand telephone billing records a year using nothing

⁷ *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (affirming the Court's previous holdings that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed") (citing *U.S. v. Miller*, 425 U.S. 435, 442 (1976)).

⁸ See, e.g., *O'Connor v. Ortega*, 480 U.S. 709, 720 (1987) (plurality opinion) (concluding that, in limited circumstances, a search unsupported by either warrant or probable cause can be constitutional when "special needs" other than the normal need for law enforcement provide sufficient justification); *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (holding Wisconsin Supreme Court's interpretation of regulation requiring "reasonable grounds" for warrantless search of probationer's residence satisfies the Fourth Amendment reasonableness requirement); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652-653 (1995); *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (asserting that when historical analysis of common law at the time of the Fourth Amendment proves inconclusive as to what protections were envisioned, the Court must "evaluate the search or seizure under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests"); *Packwood v. Senate Select Committee on Ethics*, 510 U.S. 1319, 1321 (1994) (observing the uncontested application of a Fourth Amendment legal standard that "balanced applicant's privacy interests against the importance of the governmental interests. The court concluded that the latter outweighed the former"); *U.S. v. Cantley*, 130 F.3d 1371, 1375 (10th Cir., 1997) (noting that the Supreme Court "has recognized exceptions to the warrant requirement for certain "special needs" of law enforcement, including a state's parole system").

but a subpoena.⁹ That means you're roughly a thousand times more likely to have your telephone calling patterns reviewed by a law enforcement agency than by NSA. (And the chance that law enforcement will look at your records is itself low, around 0.25% in the case of one carrier¹⁰). So it appears that law enforcement has been gaining access to our call metadata for as long as billing records have existed – nearly a century. If this were the road to Orwell's 1984, surely we'd be there by now, and without any help from NSA's 300 searches.

Section 702 and “PRISM”

This brings us to PRISM and the second of the Snowden stories to be released. Without the surprise of the phone metadata order, the PRISM slide show released by Snowden would have been much less newsworthy. Indeed, the parts of the PRISM story that were true aren't actually new and the parts that were new aren't actually true.

Let's start with what's true. Despite the noise around PRISM, the slides tell us very little that the law itself doesn't tell us. Section 702 says that the government may target non-U.S. persons “reasonably believed to be located outside the United States to acquire foreign intelligence information.” It covers activities with a connection to the United States and is therefore subject to greater oversight than foreign intelligence gathered outside the United States. Although the Attorney General and the Director of National Intelligence can authorize collection annually, the collection and use of the data is covered by strict targeting and minimization procedures that are subject to judicial review and aimed at protecting U.S. persons as well as other persons located inside the United States.

That's what the law itself says, and the Snowden slides simply add voyeuristic details about the collection. Everyone already knew that the government had the power to do this because, unlike many countries, we codify these things in law. It should come as no surprise then that the government has been using its power to protect all of us.

There was one surprise in those stories though. That's the part that was new but not true. When the story originally broke, reporters at the *Guardian* and the *Washington Post* made it look as if the NSA had direct, unfettered access to private service providers' networks and that they were downloading materials at will. To be fair, the slides were

⁹ In 2012, Rep. Markey sent letters to a large number of cell phone companies, asking among other things how many law enforcement requests for subscriber records the companies received over the past five years. The three largest carriers alone reported receiving more than a million law enforcement subpoenas a year. *Letters to mobile carriers regarding use of cell phone tracking by law enforcement*, CONGRESSMAN ED MARKEY, <http://markey.house.gov/content/letters-mobile-carriers-reagrding-use-cell-phone-tracking-law-enforcement> (last visited July 15, 2013).

¹⁰ Letter from Timothy P. McKone, Exec. Vice President, AT&T, to Congressman Ed Markey 3 (May 29, 2012), <http://markey.house.gov/sites/markey.house.gov/files/documents/AT%26T%20Response%20to%20Rep.%20Markey.pdf>.

confusing on this point, talking about getting data “directly from the servers” of private companies. But that phrase is at best ambiguous; it could easily mean that NSA serves a lawful order on the companies and the companies search for and provide the data from their servers. In fact, everyone with knowledge, from the DNI to the companies in question, has confirmed that interpretation while denying that NSA has unfettered access to directly search the private servers. In short, it now looks as though the *Washington Post* and the *Guardian* hyped this aspect of their story to spur a public debate about NSA surveillance.

In short, in both section 215 and section 702, the government has found a reasonable way to square intelligence-gathering necessities with changing technology. Now that they’ve been exposed to the light of day, these programs are not at all hard to justify. But we cannot go on exposing every collection technique to the light of day just to satisfy everyone that the programs are appropriate. The exposure itself will diminish their effectiveness. Even a fair debate in the open will cause great harm.

And this was never meant to be a fair debate. Snowden and his allies in the press had copies of the minimization and targeting guidelines; they surely knew that the guidelines made the programs look far more responsible. So they suppressed them, waiting a full two weeks – while the controversy grew and took the shape they preferred – before releasing the documents. Since no self-respecting reporter withholds relevant information from the public, it’s only fair to conclude that this was an act of advocacy, not journalism. Perhaps the reporters lost their bearings; perhaps the timing was controlled by advocates. Either way, the public was manipulated, not informed.

What Next?

Setting aside the half-truths and the hype, what does the current surveillance flap tell us about the fundamental question we’ve faced since 1978 – how to gather intelligence under law? I think the current debate exposes two serious difficulties in using law to regulate intelligence gathering.

1. Regulating Technology – What Works and What Doesn’t

First, since American intelligence has always been at its best in using new technologies, intelligence law will always be falling out of date, and the more specific its requirements the sooner it will be outmoded.

Second, we aren’t good at regulating government uses of technology. That’s especially a risk in the context of intelligence, where the government often pushes the technological envelope. The privacy advocates who tend to dominate the early debates about government and technology suffer from a sort of ideological technophobia, at least as far as government is concerned. Even groups that claim to embrace the future want government to cling to the past. And the laws they help pass reflect that failing.

To take an old example, in the 1970s, well before the personal computer and the Internet, privacy campaigners persuaded the country that the FBI's newspaper clipping files about U.S. citizens were a threat to privacy. Sure, the information was public, they acknowledged, but gathering it all in one file was viewed as sinister. And maybe it was; it certainly gave J. Edgar Hoover access to embarrassing information that had been long forgotten everywhere else. So in the wake of Watergate, the attorney general banned the practice in the absence of some investigative predicate.

The ban wasn't reconsidered for twenty-five years. And so, in 2001, when search engines had made it possible for anyone to assemble a clips file about anyone in seconds, the one institution in the country that could not print out the results of its Internet searches about Americans was the FBI. This was bad for our security, and it didn't protect anyone's privacy either.

Now we're hearing calls to regulate how the government uses big data in security and law enforcement investigations. This is about as likely to protect our privacy as reinstating the ban on clips files. We can pass laws turning the federal government into an Amish village, but big data is here to stay, and it will be used by everyone else. Every year, data gets cheaper to collect and cheaper to analyze. You can be sure that corporate America is taking advantage of this remorseless trend. The same is true of the cyberspies in China's Peoples' Liberation Army.

If we're going to protect privacy, we won't succeed by standing in front of big data shouting "Stop!" Instead, we need to find privacy tools – even big data privacy tools – that take advantage of technological advances. The best way to do that, in my view, was sketched a decade ago by the Markle Foundation Task Force on National Security, which called on the government to use new technologies to better monitor government employees who have access to sensitive information.¹¹ We need systems that audit for data misuse, that flag questionable searches, and that require employees to explain why they are seeking unusual data access. That's far more likely to provide effective protection against misuse of private data than trying to keep cheap data out of government hands. The federal government has in fact made progress in this area; that's one reason that the minimization and targeting rules could be as detailed as they are. But it clearly needs to do better. A proper system for auditing access to restricted data would

¹¹ The Task Force's first report called for the federal government to adopt

robust permissioning structures and audit trails that will help enforce appropriate guidelines. These critical elements could employ a wide variety of authentication, certification, verification, and encryption technologies. Role-based permissions can be implemented and verified through the use of certificates, for example, while encryption can be used to protect communications and data transfers. ... Auditing tools that track how, when, and by whom information is accessed or used ensure accountability for network users. These two safeguards—permissioning and auditing—will free participants to take initiatives within the parameters of our country's legal, cultural, and societal norms.

MARKLE FOUNDATION TASK FORCE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE 17 (October 2002), http://www.markle.org/sites/default/files/nstf_full.pdf.

not just improve privacy enforcement, it likely would have flagged both Bradley Manning and Edward Snowden for their unusual network browsing habits.

2. The Rest of the World Has a Ringside Seat – And It Wants a Vote, Too

There's a second reason why the American experiment in creating a detailed set of legal restraints on intelligence gathering is facing unexpected difficulties. The purpose of those restraints is to protect Americans from the intelligence collection techniques we use on foreign governments and nationals. At every turn, the laws and regulations reassure Americans that they will not be targeted by their own intelligence services. This makes plenty of sense from a policy and civil liberties point of view. Intelligence gathering isn't pretty, and it isn't patty cake. On occasion, the survival of the country may depend on good intelligence. Wars are won and lives are lost when intelligence succeeds or fails. Nations do whatever they can to collect information that might affect their future so dramatically. After a long era of national naïveté, when we thought that gentlemen didn't read other gentlemen's mail and when intercepting even diplomatic radio signals was illegal, the United States found itself thrust by World War II and the Cold War into the intelligence business, and now we play by the same rules as the rest of the world.

The purpose of much intelligence law and regulation is to make sure we do not apply those rules to our own citizens. On the whole, I'm confident that we have gone about as far in pursuit of that goal as we can without seriously compromising our ability to conduct foreign intelligence. And we've spelled those assurances out in unprecedented detail. All of that should – and largely has – left the majority of Americans satisfied that intelligence under law is working reasonably well.

The problem is that Americans aren't the only people who read our laws or follow our debates. So does the rest of the world. And it doesn't take much comfort from legal assurances that the privacy interests of *Americans* are well protected from our intelligence agencies' reach. So, while the debate over U.S. intelligence gathering is already beginning to recede in this country, the storm is still gathering abroad. Many other countries have complained about the idea that NSA may be spying on their citizens. Politicians in France, Brazil, Germany, the Netherlands, the United Kingdom, Belgium, and Romania, among others, have expressed shock and called for investigations into PRISM. On July 4, the European Parliament passed a resolution calling for a range of possible actions, such as delaying trade talks and suspending law enforcement and intelligence agreements with the United States over allegations that the United States gathered intelligence on European diplomats.¹²

¹² European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)) at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN> [hereinafter *European Parliament Resolution*].

Some of this is just hypocrisy. Shortly after President Hollande demanded that the U.S. “immediately stop” its intercepts¹³ and the French Interior Minister used his position as guest of honor at a July 4th celebration to chide the United States for its intercepts, *Le Monde* disclosed what both French officials well knew – that France has its own program for large-scale interception of international telecommunications traffic.¹⁴

But some of reaction is grounded in ignorance. Thanks to our open debates and detailed legislative limits on intelligence gathering, Europeans know far more about U.S. intelligence programs than about their own. The same is true around the world.

As a result, it’s easy for European politicians to persuade their publics that the United States is uniquely intrusive in the way it conducts law enforcement and intelligence gathering from electronic communications providers. In fact, the reverse is true.

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

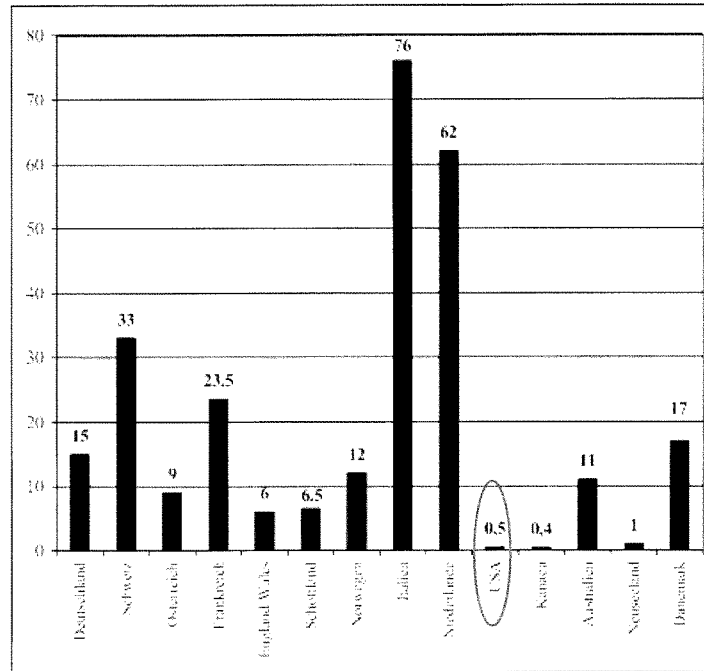
I’ve included below two figures that illustrate this phenomenon. One is from a study done by the Max Planck Institute, estimating the number of surveillance orders per 100,000 people in several countries. While the statistics in each are not exactly comparable, the chart published in that study shows an unmistakable overall trend. The number of U.S. orders is circled, because it’s practically invisible next to most European nations; indeed, an Italian or Dutch citizen is more than a hundred times more likely to be wiretapped by his government than an American.¹⁵

¹³ 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>.

¹⁴ Jacques Follorou and Franck Johannès, *In English: Revelations on the French Big Brother*, LE MONDE (July 4, 2013, 5:24 PM), http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html.

¹⁵ Hans-Jörg Albrecht, et al., *Legal Reality and Efficiency of the Surveillance of Telecommunications*, MAX PLANCK INSTITUTE 104 (2003), http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_%20abschlussbericht.pdf.

Which countries do the most surveillance per capita?



Similarly, the PRISM program is widely believed to show a uniquely American enthusiasm for collecting data from service providers. In fact, it owes that reputation in part to detailed statutory provisions that are meant to protect privacy but that also spell out how the program works.

European regimes, by and large, offer far less protection against arbitrary collection of personal data – and expose their programs to far less public scrutiny. One recent study showed that, out of a dozen advanced democracies, only two – the United States and Japan – impose serious limits on what electronic data private companies can give to the government without legal process. In most other countries, and particularly in Europe,

little or no process is required before a provider hands over information about subscribers.¹⁶

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

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

*Voluntary disclosure of personal data requires valid reason

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

¹⁶ Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*. HOGAN LOVELLS (July 18, 2012).

At most, European providers must have a good reason for sharing personal data, but assisting law enforcement investigations is highly likely to satisfy this requirement. In the United States, such sharing is prohibited in the absence of legal process.

Despite the evidence, however, it is an article of faith in Europe that the United States lags Europe in respect for citizens' rights when collecting data for security and law enforcement purposes. Again, this is the unfortunate result of our commitment to regulating our intelligence services in a more open fashion than other countries.

The U. S. government has learned to live with Europe's misplaced zeal for moral tutelage where data collection is concerned. Our government can ride out this storm as it has ridden out others. But the antagonism spawned by Snowden's disclosures could have more serious consequences for our information technology companies.

Many countries around the world have launched investigations designed to punish American companies for complying with American law. Some of the politicians and data protection agencies pressing for sanctions are simply ignorant of their own nation's aggressive use of surveillance, others are jumping at any opportunity to harm U.S. security interests. But the fact remains that the price of obeying U.S. law could be very high for our information technology sector.

Foreign officials are seizing on the disclosures to fuel a new kind of information protectionism. During a French parliament hearing, France's Minister for the Digital Economy declared that, if the report about PRISM "turns out to be true, it makes [it] relatively relevant to locate datacenters and servers in [French] national territory in order to better ensure data security."¹⁷ Germany's Interior Minister was even more explicit, saying, "Whoever fears their communication is being intercepted in any way should use services that don't go through American servers."¹⁸ And Neelie Kroes, Vice President of the European Commission, said, "If European cloud customers cannot trust the United States government or their assurances, then maybe they won't trust US cloud providers either. That is my guess. And if I am right then there are multi-billion euro consequences for American companies."¹⁹

Hurting U.S. information technology firms this way is a kind of three-fer for European officials. It boosts the local IT industry, it assures more data for Europe's own surveillance systems, and it hurts U.S. intelligence.

¹⁷ Valéry Marchive *France hopes to turn PRISM worries into cloud opportunities*, ZDNET (June 21, 2013, 9:02 GMT), <http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/>.

¹⁸ *German minister: Drop US sites if you fear spying*, ASSOCIATED PRESS (July 3, 2013), http://m.apnews.com/ap/db_307122/contentdetail.htm?contentguid=OmnMPwXK.

¹⁹ Neelie Kroes, Vice President, European Commission, Statement after the meeting of European Cloud Partnership Board, Tallinn, Estonia (July 4, 2013) (transcript available at http://europa.eu/rapid/press-release_MEMO-13-654_en.htm).

The European Parliament has been particularly aggressive in condemning the program as a violation of European human rights.²⁰ Its resolution pulls out all the stops, threatening sanctions if the United States does not modify its intelligence programs to provide privacy protections for European nationals. The resolution raises the prospect of suspending two anti-terror agreements with the United States on passenger and financial data, it “demands” U.S. security clearances for European officials so they can review all the documents about PRISM, and it threatens US-EU trade talks as well as the Safe Harbor that allows companies to move data freely across the Atlantic.

This may be the most egregious double standard to come out of Europe yet. Unlike our section 215 program, the EU doesn’t have a big metadata database. But that’s because Europe doesn’t need one. Instead, the European Parliament passed a measure forcing all of its information technology providers to create their own metadata databases so that law enforcement and security agencies could conveniently search up to two years’ worth of logs. These databases are full of data about American citizens, and under EU law any database held anywhere in Europe is open to search (and quite likely to “voluntary” disclosure) at the request of any government agency anywhere between Bulgaria and Portugal.

I have seen this movie before, too. During my tenure at Homeland Security, European officials tried to keep the United States from easily accessing travel reservation data to screen for terrorists hoping to blow up planes bound for the United States. In order to bring the United States to the table, European officials threatened to impose sanctions not on the government but on air carriers who cooperated with the data program.²¹ Similarly, to limit U.S. access to terror finance information, European data protection authorities threatened the interbank transfer company, SWIFT, with criminal prosecution and fines for giving the U.S. access to transfer data.²² In the end, the threat of sanctions forced SWIFT to keep a large volume of its data in Europe and to deny U.S. authorities access to it.

Now, whenever Europe has a beef with U.S. use of data in counterterrorism programs, it threatens not the U.S. government but U.S. companies. The European Parliament is simply returning to that same playbook. There is every reason to believe that European governments, and probably some imitators in Latin America and elsewhere, will hold U.S. information technology companies hostage in order to show their unhappiness at the PRISM disclosures.

3. What Congress Should Do About It

As a result, 2013 is going to be a bad year for companies that complied with U.S. law. We need to recognize that our government put them in this position. Not just the

²⁰ *European Parliament Resolution*, *supra* note 12.

²¹ BAKER, *supra* note 3, at 114-15.

²² *Id.* at 145-51.

executive branch that served those orders, but Congress too, which has debated and written intelligence laws as though the rest of the world wasn't listening.

The U.S. government, all of it, has left U.S. companies seriously at risk for doing nothing more than their duty under U.S. law. And the U.S. government, all of it, has a responsibility to protect U.S. companies from the resulting foreign government attacks.

The executive branch has a responsibility to interpose itself between the companies and foreign governments. The flap over Snowden's disclosures is a dispute between governments, and it must be kept in those channels. Diplomatic, intelligence, and law enforcement partners in every other country should hear the same message: "If you want to talk about U.S. intelligence programs, you can talk to us – but not to U.S. companies and individuals; they are prohibited by law from discussing those programs."

Congress too needs to speak up on this question. European politicians feel free to demand security clearances and a vote on U.S. data programs in part because they think Congress and the American public share their views. It's time to make clear to other countries that we do not welcome foreign regulation of U.S. security arrangements.

There are many ways to convey that message. Congress could – should – adopt its own resolution rejecting the European Parliament's.

Congress could prohibit U.S. agencies from providing intelligence and law enforcement assistance or information to nations that have harassed or threatened U.S. companies for assisting their government – unless the agency head decides that providing a particular piece of information will also protect U.S. security.

It could require similar review procedures to make sure that Mutual Legal Assistance Treaties do not provide assistance to nations that try to punish U.S. companies for obeying U.S. law.

And it could match the European Parliament's willingness to reopen the travel data and terror finance pacts with its own, prescribing in law that if the agreements are reopened they must be amended to include an anti-hypocrisy clause ("no privacy obligations may be imposed on U.S. agencies that have not already been imposed on European agencies") as well as an anti-hostage-taking clause ("concerns about government conduct will be raised between governments and not by threatening private actors with inconsistent legal obligations").

And, just to show that this particular road runs in both directions, perhaps Congress could mandate an investigation into how much data about individual Americans is being retained by European companies, how often it is accessed by European governments, and whether access meets our constitutional and legal standards.

Conclusion

Thirty-five years of trying to write detailed laws for intelligence gathering have revealed just how hard that exercise is – and why so few nations have tried to do it. In closing, let me offer some quick thoughts on two proposals that would “fix” FISA by doubling down on this approach.

One idea is to declassify FISA court opinions. Another is to appoint outside lawyers with security clearances who can argue against the government. The problem with these proposals is that they’re not likely to persuade the FISA doubters that the law protects their rights. But they are likely to put sources and methods at greater risk.

Declassification of the FISA court opinions already happens, but only when the opinion can be edited so that the public version does not compromise sources and methods. The problem is that most opinions make law only by applying legal principles to particular facts. In the FISA context, those facts are almost always highly classified, so it’s hard to explain the decision without getting very close to disclosing sources and methods. To see what I mean, I suggest this simple experiment. Let’s ask the proponents of declassification to write an unclassified opinion approving the current section 215 program – without giving away details about how the program works. I suspect that the result will be at best cryptic; it will do little to inspire public trust but much to spur speculation and risk to sources and methods.

What about appointing counsel in FISA matters? Well, we don’t appoint counsel to protect the rights of Mafia chieftains or drug dealers. Wiretap orders and search warrants aimed at them are reviewed by judges without any advocacy on behalf of the suspect. Why in the world would we offer more protection to al Qaeda?

I understand the argument that appointing counsel will provide a check on the government, whose orders may never see the light of day or be challenged in a criminal prosecution. But the process is already full of such checks. The judges of the FISA court have cleared law clerks who surely see themselves as counterweights to the government’s lawyers. The government’s lawyers themselves come not from the intelligence community but from a Justice Department office that sees itself as a check on the intelligence community and feels obligated to give the FISA court facts and arguments that it would not offer in an adversary hearing. There may be a dozen offices that think their job is to act as a check on the intelligence community’s use of FISA: inspectors general, technical compliance officers, general counsel, intelligence community staffers, and more. To that army of second-guessers, are we really going to add yet another lawyer, this time appointed from outside the government?

For starters, we won’t be appointing a lawyer. There certainly are outside lawyers with clearances. I’m one. But senior partners don’t work alone, and there are very few nongovernment citecheckers and associates and typists with clearances. Either we’ll have to let intercept orders sit for months while we try to clear a law firm’s worth of staff –

along with their computer systems, Blackberries, and filing systems – or we'll end up creating an office to support the advocates.

And who will fill that office? I've been appointed to argue cases, even one in the Supreme Court, and I can attest that deciding what arguments to make has real policy implications. Do you swing for the fences and risk a strikeout, or do you go for a bunt single that counts as a win but might change the law only a little? These are decisions on which most lawyers must consult their clients or, if they work for governments, their political superiors. But the lawyers we appoint in the FISA court will have no superiors and effectively no clients.

To update the old saw, a lawyer who represents himself has an ideologue for a client. In questioning the wisdom of special prosecutors, Justice Scalia noted the risk of turning over prosecutorial authority to high-powered private lawyers willing to take a large pay cut and set aside their other work for an indeterminate time just to be able to investigate a particular President or other official. Well, who would want to turn over the secrets of our most sensitive surveillance programs, and the ability to suggest policy for those programs, to high-powered lawyers willing to take a large pay cut and set aside their other work for an indeterminate period just to be able to argue that the programs are unreasonable, overreaching, and unconstitutional?

Neither of these ideas will, in my view, add a jot to public trust in the intelligence gathering process. But they will certainly add much to the risk that intelligence sources and methods will be compromised. For that reason, we should approach them with the greatest caution.

QUESTIONS SUBMITTED BY SENATOR LEAHY FOR JAMES M. COLE

QUESTIONS FOR THE RECORD – Chairman Leahy
7/31/13 - FISA Hearing**Questions for Deputy Attorney General Cole**

1. Please provide a summary of the legal arguments that the United States government has submitted to the Foreign Intelligence Surveillance Court in support of conducting bulk collection of telephone and Internet metadata under Section 215 of the USA PATRIOT Act and Section 402 of the Foreign Intelligence Surveillance Act.
2. Marc Zwillinger represented Yahoo! in its challenge to the Protect America Act, and he submitted written testimony for the record of the hearing. In his testimony, he expressed the view that the Yahoo! challenge was not a fully adversarial process because the government submitted *ex parte* filings even though only cleared counsel were involved in the proceeding.

Q: Please describe what government *ex parte* submissions were made in that case, why those filings were not disclosed to opposing counsel, and whether you believe opposing counsel would have been better able to litigate the challenge with access to those submissions.

3. I appreciate Judge Walton's letter explaining the FISA Court procedures when considering applications by the government for orders under FISA. While it is important for the public to understand the FISA Court process, it is even more important that we have an open debate about the legal rationale used to justify such broad authorities as the bulk collection of telephone metadata – particularly if these opinions stretch the understanding of existing law.

Q: Would declassifying and releasing the portions of FISA Court opinions that include significant interpretations of existing law, with appropriate redactions to protect intelligence sources or methods, be harmful to our national security?

Q: Now that certain information has been declassified about Section 215 bulk collection, is there any objection to releasing any FISA Court opinions that support and explain the legal basis for these programs?

4. Please provide a full description of the ways in which information obtained by the NSA is shared with law enforcement components of the Department of Justice, including but not limited to, the Drug Enforcement Administration, and how, if at all, that information is used in criminal investigations and proceedings.

QUESTIONS SUBMITTED BY SENATOR LEAHY FOR JOHN C. INGLIS

QUESTIONS FOR THE RECORD – Chairman Leahy
7/31/13 - FISA Hearing**Questions for NSA Deputy Director Inglis**

1. In your testimony, you stated that 13 terrorist plots with a domestic nexus were disrupted as a result of both Section 702 and Section 215 authorities. You further testified that, of those 13, Section 215 contributed to the “disruption” of 12 plots. Notably, however, you cited the case of Basaaly Moalin as the only domestic terrorist plot that could be considered close to an example of where information obtained through Section 215 could be considered to have contributed in a “but-for” causal relationship to the disruption of a plot. At various times, other administration officials have testified and spoken publicly about “disrupting”, “preventing”, or “thwarting” 54 terrorist “plots” or terrorist “events”.

Q: Would you call the Basaaly Moalin case a thwarted terrorist *plot* or a terrorist *event*? If the case was a “plot”, what was the nature of the “plot” that was thwarted or prevented? Please provide additional information about the Moalin case, and whether the government has any evidence to indicate that Moalin and his co-conspirators specifically intended to conduct an attack on U.S. soil directed at U.S. persons.

Q: What is the difference between a terrorist “plot” and a terrorist “event”?

Q: How do you define “disruption” in terms of terrorist plots and events?

Q: In how many instances was information obtained through Section 215 bulk phone records collection critical to thwarting, preventing, or disrupting a terrorist plot or event?

Q: If there have been cases where Section 215 collection was critical to preventing a terrorist plot, how many of those cases involved a plot to harm Americans?

2. In your testimony, you indicated that, in 2012, the NSA approved less than 300 telephone numbers or selectors to be queried for records in the database containing telephone metadata pursuant to Section 215. However, querying a single telephone number could potentially return thousands, if not millions of records on law-abiding Americans, depending on how many hops are conducted.

Q: For the period of 2006-2012, please provide the following for each year:

- a. **The total number of numbers/selectors that were approved and queried;**
- b. **The total number of telephone records that were identified or returned as a result of those approved queries (including numbers identified or returned as a result of “two-hop” or “three-hop” analysis);**

- c. The number of selectors that were queried multiple times for each year;
- d. The number of reports generated for dissemination to the FBI as a result of querying a selector; and
- e. The total number of telephone records that were included or identified in reports to the FBI.

QUESTIONS SUBMITTED BY SENATOR LEAHY FOR JAMEEL JAFFER

QUESTIONS FOR THE RECORD – Chairman Leahy
7/31/13 - FISA Hearing

Questions for Jameel Jaffer:

1. Your written testimony discusses the constitutional implications of the Section 215 phone records program. We have heard government witnesses state repeatedly that under the 1979 case of *Smith v. Maryland*, phone records and other digital data are not protected by the Fourth Amendment because we have already revealed them to a third party, and that only the contents of our communications are protected.
 - Q: Do you agree that the *Smith v. Maryland* case provides definitive guidance on the constitutional standard to be applied to the bulk collection of telephone metadata under the Section 215 program? Is there case law suggesting that courts are reconsidering this doctrine in the face of new technology?**
 - Q: In today's world of technological convergence, social media, web browsing, and location-enabled devices, is it possible to draw a clear line between content that is protected by the Fourth Amendment, and non-content information that is not? What implications does this have for the constitutional analysis that is based on this distinction?**
2. As an alternative to the government bulk collection of telephone metadata under Section 215, some have proposed requiring the telecommunications providers to retain these records for five years so the records can be searched when it is deemed necessary.
 - Q: Do you believe that such an arrangement would alleviate any privacy concerns that may exist with regard to the Section 215 bulk collection program?**

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR JAMES M. COLE

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

James Cole, Deputy Attorney General

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?

Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected;
- (c) How many U.S. persons’ information was collected; and
- (d) How many U.S. persons’ electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Would the government’s annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such

disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals' (foreign and U.S. persons) information was collected; and
- (c) How many U.S. persons' information was collected.

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information they produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information they produced.

When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

In the Department's experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges? If so, what is that difference?

To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR JOHN C. INGLIS

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

John C. Inglis, NSA Deputy Director

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?

Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected;
- (c) How many U.S. persons’ information was collected; and
- (d) How many U.S. persons’ electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Would the government’s annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected; and
- (c) How many U.S. persons’ information was collected.

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information they produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information they produced.

What safeguards are in place to ensure that once the telephone metadata collected under Section 215 is in the possession of the NSA, it is used only in an authorized fashion? Specifically, what safeguards help prevent (a) the searching of the metadata without the required reasonable and articulable suspicion; (b) the improper dissemination of information related to U.S. persons obtained as a result of a query of the metadata; (c) any unauthorized use whatsoever of the metadata? Under the law and current practice, to what institutions are any instances of non-compliance reported, and do these reports include the details of the non-compliance, or merely the fact that an instance of non-compliance occurred? Has anyone ever been disciplined for an instance of non-compliance?

What safeguards are in place to ensure that once information is collected under Section 702, the targeting and minimization procedures approved by the FISC are followed? Under the law and current practice, to what institutions are any instances of non-compliance with the targeting and minimization procedures reported, and do these reports include the details of the non-compliance, or merely the fact that an instance of non-compliance occurred? Has anyone ever been disciplined for an instance of non-compliance?

You testified that the FISC permits NSA analysts to query up to three "hops" from the initial telephone number used as a selector, which can result in a substantial number of telephone numbers being identified through the query. What happens to these query results after the query is completed? Are these query results then subsequently searchable by the NSA at any time without a showing of reasonable and articulable suspicion?

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR ROBERT S. LITT

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Robert Litt, ODNI General Counsel

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?

Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected;
- (c) How many U.S. persons’ information was collected; and
- (d) How many U.S. persons’ electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Would the government’s annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such

disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals' (foreign and U.S. persons) information was collected; and
- (c) How many U.S. persons' information was collected.

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information the company produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information the company produced.

When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

In the ODNI's experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges? If so, what is that difference?

To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR SEAN M. JOYCE

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Sean M. Joyce, FBI Deputy Director

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?

Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected;
- (c) How many U.S. persons’ information was collected; and
- (d) How many U.S. persons’ electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Would the government’s annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such

disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals' (foreign and U.S. persons) information was collected; and
- (c) How many U.S. persons' information was collected.

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information they produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information they produced.

Please provide to the Committee all unclassified information available that, in your view, demonstrates the usefulness of the Section 215 and 702 authorities in protecting the national security.

Boston Marathon Bombing

On May 10, 2013, the FBI provided to staff members of the Senate, a comprehensive TS/SCI briefing on the Boston Marathon bombing. During the course of the briefing, several unclassified questions were asked. One series of unclassified questions was asked by a member of my staff and you provided no substantive answer, saying you would need to gather more information and provide a complete answer at a later date. My staff received no further information. I would like to follow up now:

At what time and date were the images of Dzhokhar Tsarnaev and/or Tamerlan Tsarnaev discovered on video or photograph for the *first time* as being at least one or both of the individuals reasonably believed to be involved in the bombing?

Who made that determination and for what agency did that individual work?

Following this initial determination, what investigative steps did the FBI take *or* attempt to take *prior* to releasing the photos to the public?

Did the FBI have the suspects under physical surveillance at any time *prior* to releasing the photos to the public?

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR JAMES G. CARR

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Judge James G. Carr

You testified that in very rare instances – perhaps five or fewer during your years on the FISC -- you would have benefitted from the analysis of an independent attorney regarding a novel question of statutory or constitutional interpretation. In your view, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government’s applications before the FISC help strike the correct balance between privacy and national security? Why or why not?

Under your proposal, would the independent attorney be required to argue against the government’s position in every instance, or would the attorney be permitted to agree with the government if he or she felt that that position was the required outcome under the law?

Do you believe that the FISC is a rubber stamp for the government? If not, what explains the government’s high success rate before it? Is that success rate in part the product of a “give and take” process by which the Court reviews the government’s applications and provides feedback?

In your experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges?

On how many occasions during your tenure on the FISC were you informed about an instance of non-compliance with the court’s orders by the government? How many, if any, of these occasions involved intentional non-compliance? In each case, did the government remedy the situation satisfactorily?

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR JAMEEL JAFFER

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Jameel Jaffer, ACLU Deputy Legal Director

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. In your view, would such an arrangement resolve your concerns about the legality of the telephone metadata program under Section 215? Why or why not?

Has the one-year ban on challenging non-disclosure orders under Section 215 posed practical problems or difficulties for private companies, especially since those companies may challenge the underlying order requiring the production of business records immediately? If so, what are they? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected;
- (c) How many U.S. persons’ information was collected; and
- (d) How many U.S. persons’ electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Would the government’s annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such

disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals' (foreign and U.S. persons) information was collected; and
- (c) How many U.S. persons' information was collected.

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information they produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information they produced.

When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

Do you believe that the FISC is a rubber stamp for the government? If not, what explains the government's high success rate before it? Is that success rate in part the product of a "give and take" process by which the Court reviews the government's applications and provides feedback?

Does the Fourth Amendment or any other protections under the Bill of Rights apply to non-U.S. persons in foreign countries? Why or why not? What does this mean for orders issued under Section 702?

To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

QUESTIONS SUBMITTED BY SENATOR GRASSLEY FOR STEWART BAKER

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Stewart Baker, Steptoe & Johnson

Would ending the collection of telephone metadata in bulk under Section 215 -- and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?

Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals’ (foreign and U.S. persons) information was collected;
- (c) How many U.S. persons’ information was collected; and
- (d) How many U.S. persons’ electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Would the government’s annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such

disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals' (foreign and U.S. persons) information was collected; and
- (c) How many U.S. persons' information was collected.

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information they produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information they produced.

When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

In your experience, are there institutional checks and safeguards in place that ensure that the FISC hears both sides of an issue, and not just the government's? If so, what are they and how do they work?

In your experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges? If so, what is that difference?

Are there any specific reforms to the current law and practice that you would suggest to help ensure that any data the government collects from the 215 and 702 programs is accessed and used only as the law or a court permits?

To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

RESPONSES OF JAMES M. COLE TO QUESTIONS SUBMITTED BY SENATORS LEAHY AND GRASSLEY

[NOTE: SOME RESPONSES OF JAMES M. COLE ARE CLASSIFIED AND THEREFORE NOT PRINTED AS A PART OF THIS HEARING.]

**Hearing Before the
Committee on the Judiciary
United States Senate**

**Entitled
“Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs”
July 31, 2013**

**Questions for the Record Addressed to
James M. Cole
Deputy Attorney General
Department of Justice**

Questions Posed by Chairman Leahy

1. Please provide a summary of the legal arguments that the United States government has submitted to the Foreign Intelligence Surveillance Court in support of conducting bulk collection of telephone and Internet metadata under Section 215 of the USA PATRIOT Act and Section 402 of the Foreign Intelligence Surveillance Act.

Answer:

The Government has published a white paper summarizing its views on the legal basis for the collection of bulk telephony metadata under Section 215. *See Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act*, available at <http://publicintelligence.net/doj-bulk-telephony-collection/>. The Government’s classified brief on this subject, which was submitted to the Foreign Intelligence Surveillance Court (FISC) in 2006, was provided to this committee in 2010, and was declassified and made publicly available by the Director of National Intelligence on November 18, 2013.

Section 402 of FISA, which governs installation and use of pen registers and trap and trace devices for foreign intelligence and international terrorism investigations, has different requirements and standards than Section 215 of the USA PATRIOT Act. The Government’s classified brief on collection of bulk Internet metadata under Section 402 has also been provided to this committee.

2. Marc Zwillinger represented Yahoo! in its challenge to the Protect America Act, and he submitted written testimony for the record of the hearing. In his testimony, he expressed the view that the Yahoo! challenge was not a fully adversarial process because the government submitted *ex parte* filings even though only cleared counsel were involved in the proceeding.

Q: Please describe what government *ex parte* submissions were made in that case, why those filings were not disclosed to opposing counsel, and whether you believe opposing counsel would have been better able to litigate the challenge with access to those submissions.

Answer:

On August 5, 2007, Congress enacted the Protect America Act (PAA), the predecessor to Section 702 of FISA. In general, the PAA authorized the Attorney General and the Director of National Intelligence to authorize, for periods of up to one year, the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States and to compel, through the issuance of directives, the assistance of communications services providers in accomplishing such acquisitions. A directive was issued to Yahoo! requiring Yahoo! to provide such assistance. Yahoo! refused to comply with the directive. The Government then moved the FISC to compel Yahoo!'s compliance with the properly issued directive. Classified adversarial litigation ensued in both the FISC and the Foreign Intelligence Surveillance Court of Review (FISC-R) over several months, culminating in a classified oral argument before the FISC-R. Both the FISC and the FISC-R ruled that Yahoo! was required to comply with the directive, and Yahoo! ultimately complied in the wake of these rulings.

The Yahoo! challenge to the PAA was, in the Government's view, a full and fair adversarial proceeding that resulted in thoughtful and comprehensive presentations of the legal issues involved to the FISC and, on appeal, to the FISC-R. Although counsel for Yahoo! had been granted security clearances by the Government and was provided access to some classified information in government submissions based on his need to know that information, those clearances did not entitle counsel access to certain sensitive compartmented information related to sources and methods. Although in certain limited circumstances the Government, compelled by requirements pertaining to the protection of classified national security information, submitted certain pleadings/information *ex parte* and in camera to the FISC and the FISC-R, the more typical practice was for the Government to serve counsel for Yahoo! with appropriately redacted versions of briefs and other filings. The Government redacted information in a manner consistent with governing law and Executive Orders on the protection of classified information in order to protect sensitive sources and methods and other classified matters that counsel for Yahoo! had no need to know. Moreover, the information withheld was not material to their ability to mount a vigorous legal challenge to the PAA. For example, Yahoo!'s counsel did not need to know certain details about internal government processes and procedures that were used by the Government in implementing PAA authorities, and their litigation of these matters was in no way prejudiced by the redaction of that information. Briefing on the core legal issues was presented unredacted to Yahoo!'s counsel. Both the FISC and FISC-R had full visibility into the redactions. The lengthy and well-reasoned opinions of the FISC and the FISC-R on Yahoo!'s challenge to the PAA (including the FISC-R's published opinion) are evidence of the sufficiency of the legal process afforded to Yahoo! in that matter.

3. I appreciate Judge Walton's letter explaining the FISA Court procedures when considering applications by the Government for orders under FISA. While it is important for the public to understand the FISA Court process, it is even more important that we have an open debate

about the legal rationale used to justify such broad authorities as the bulk collection of telephone metadata – particularly if these opinions stretch the understanding of existing law.

Q: Would declassifying and releasing the portions of FISA Court opinions that include significant interpretations of existing law, with appropriate redactions to protect intelligence sources or methods, be harmful to our national security?

Answer:

The Administration has committed to reviewing significant FISC opinions for declassification, recognizing that, as Judge Walton has explained, the facts presented in applications to the FISC almost always involve classified intelligence activities, the disclosure of which could be harmful to national security and, in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC’s analysis would result in a remnant void of much or any useful meaning. In connection with the recent unauthorized disclosures of information concerning intelligence activities carried out under sections 501 and 702 of FISA, the President has directed that as much information as possible be made public about these activities, consistent with the need to protect sources and methods and national security, including relevant FISC opinions related to these activities. In recent months, the Government has declassified several FISC opinions concerning these activities, with appropriate redactions for national security purposes.

Q: Now that certain information has been declassified about Section 215 bulk collection, is there any objection to releasing any FISA Court opinions that support and explain the legal basis for these programs?

Answer:

See response above.

4. Please provide a full description of the ways in which information obtained by the NSA is shared with law enforcement components of the Department of Justice, including but not limited to, the Drug Enforcement Administration, and how, if at all, that information is used in criminal investigations and proceedings.

Answer:

For information collected under FISA, NSA shares information in accordance with the applicable provisions of that statute. The USA PATRIOT Act amended FISA to facilitate information sharing, and to ensure an end to the FISA “wall” inhibiting information sharing between intelligence and law enforcement components of the Government. Thus FISA provides that federal officials conducting electronic surveillance under FISA “may consult” with law enforcement officials “to coordinate efforts to investigate or protect against” international terrorism, espionage, and other threats. 50 U.S.C. § 1806(k). FISA also requires that dissemination of information about U.S. persons comply with minimization procedures, and

FISA contemplates that these procedures will permit the dissemination of foreign intelligence information and evidence of a crime, including to law enforcement authorities. *See, e.g.*, 50 U.S.C. § 1801(h)(3) (defining minimization procedures for electronic surveillance in part as “procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes”). The Attorney General and the FISA Court (or, in certain circumstances, like emergency authorization, the Attorney General alone) must approve the minimization procedures. FISA also has provisions governing the use of most kinds of information obtained under FISA authorities in criminal and other proceedings. *See, e.g.*, 50 U.S.C. §§ 1806(c)-(h) (governing the use of information obtained from electronic surveillance in proceedings).

For information collected under Executive Order 12333, NSA shares information about U.S. persons in accordance with procedures established by the Secretary of Defense and approved by the Attorney General. Those procedures generally permit the dissemination of information to “[a]n agency of the federal government authorized to receive such information in the performance of a lawful governmental function” and to a federal, state, or local law enforcement agency if “the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce.” *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons (DOD Reg. 5240.1-R), Procedure 4—Dissemination of Information About United States Persons § C4.2.2* (Dec. 1982). *See also Classified Annex to Department of Defense Procedures Under Executive Order 12333 § 4.A.4* (May 27, 1988).

Information received from NSA is used in a variety of ways, depending on the nature of the information. It may be used to generate leads to further an investigation, in discovery as part of a criminal proceeding, or as evidence at trial.

RESPONSES OF JOHN C. INGLIS TO QUESTIONS SUBMITTED BY SENATORS LEAHY AND
GRASSLEY

[NOTE: THE RESPONSES OF JOHN C. INGLIS ARE CLASSIFIED AND THEREFORE NOT
PRINTED AS A PART OF THIS HEARING.]

RESPONSES OF ROBERT S. LITT TO QUESTIONS SUBMITTED BY SENATOR GRASSLEY

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
OFFICE OF GENERAL COUNSEL
WASHINGTON, DC 20511

December 6, 2013

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy and Ranking Member Grassley:

On November 20, 2013, the U.S. Department of Justice provided their responses to your written questions from Committee members for the July 31, 2013 hearing entitled "Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs." The identical questions were also sent to me and I concur with the responses provided.

If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,



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

RESPONSES OF SEAN M. JOYCE TO QUESTIONS SUBMITTED BY SENATOR GRASSLEY

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the July 31, 2013, Hearing Before the
Senate Committee on the Judiciary
Regarding “Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs”**

Questions Posed by Senator Grassley

1. Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected – affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?
2. Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?
3. Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?
4. Would the government’s annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government’s ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?
 - a. How many FISA court orders were issued.
 - b. How many individuals’ (foreign and U.S. persons) information was collected.
 - c. How many U.S. persons’ information was collected.

These responses are current as of 9/27/13

d. How many U.S. persons' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

5. Would the government's annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

a. How many FISA court orders were issued.

b. How many individuals' (foreign and U.S. persons) information was collected.

c. How many U.S. persons' information was collected.

6. Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

a. How many FISA court orders the company received.

b. The percentage of those orders the company complied with.

c. How many of their users' information they produced.

d. How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

7. Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

a. How many FISA court orders the company received.

b. The percentage of those orders the company complied with.

c. How many of their users' information they produced.

These responses are current as of 9/27/13

Response to Questions 1 through 7:

These questions were additionally posed to the Deputy Attorney General. The FBI refers the Committee to those responses.

8. Please provide to the Committee all unclassified information available that, in your view, demonstrates the usefulness of the Section 215 and 702 authorities in protecting the national security.

Response:

The Office of the Director of National Intelligence (ODNI) has obtained from multiple agencies information regarding the cases in which Section 215 and 702 authorities have contributed to the protection of national security. Consequently, the ODNI is better able to respond to this inquiry.

Boston Marathon Bombing

9. On May 10, 2013, the FBI provided to staff members of the Senate, a comprehensive TS/SCI briefing on the Boston Marathon bombing. During the course of the briefing, several unclassified questions were asked. One series of unclassified questions was asked by a member of my staff and you provided no substantive answer, saying you would need to gather more information and provide a complete answer at a later date. My staff received no further information. I would like to follow up now.

a. At what time and date were the images of Dzhokhar Tsarnaev and/or Tamerlan Tsarnaev discovered on video or photograph for the first time as being at least one or both of the individuals reasonably believed to be involved in the bombing?

b. Who made that determination and for what agency did that individual work?

c. Following this initial determination, what investigative steps did the FBI take or attempt to take prior to releasing the photos to the public?

d. Did the FBI have the suspects under physical surveillance at any time prior to releasing the photos to the public?

Response to subparts a through d:

The FBI did not identify Tamerlan or Dzhokhar Tsarnaev by name as suspects in the Boston Marathon bombing until Tamerlan was killed in the aftermath of the shootout

These responses are current as of 9/27/13

with law enforcement on April 19, 2013. The FBI did not have the Tsarnaevs under surveillance at any time after the assessment of Tamerlan was closed in 2011.

These responses are current as of 9/27/13

RESPONSES OF JAMES G. CARR TO QUESTIONS SUBMITTED BY SENATOR GRASSLEY

Senate Committee on the Judiciary

"Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs"

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

to

Sr. U.S. District Judge James G. Carr

ANSWERS

QUESTION ONE:

You testified that in very rare instances – perhaps five or fewer during your years on the FISC -- you would have benefitted from the analysis of an independent attorney regarding a novel question of statutory or constitutional interpretation. In your view, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC help strike the correct balance between privacy and national security? Why or why not?

ANSWER TO QUESTION ONE:

I do not believe that having independent counsel review all government's applications before the FISC would be necessary or desirable. This is so for at least two reasons.

First: the FISC has a cadre of highly experienced and thoroughly knowledgeable Legal Advisors who review all applications before the government presents them formally to the FISC duty Judge.¹ Those attorneys often raise questions with the Justice Department attorney who prepared the application. It was my practice, in consultation with a Legal Advisor, to do likewise. Thus, "vetting" of the sort which the question suggests already occurs.

¹ The FISC Rules of Procedure require the Department to submit a copy of a proposed application and order at least seven days before formal filing with the Court. FISC R. Proc. 9(a). The proposed application is called the "read copy." Rule 9(a) ensures that the Legal Advisors and duty Judge have sufficient time to review the application and order and raise questions before formal submission for judicial review.

FISC Presiding Judge Reggie Walton attached a copy of the FISC Rules to his letter of July 29, 2013, to the Committee ("Walton Letter").

Second: the FISA probable cause standard is considerably lower than that which the Fourth Amendment requires with regard to a conventional search warrant application. With a Fourth Amendment warrant (or a Title III law enforcement electronic surveillance order), the government must show probable cause with regard to criminal activity. That can sometimes be difficult.

With a FISA application, in contrast, the government need only show probable cause to believe that the target is connected with a foreign government or a foreign-based terrorist organization.² In the vast majority of cases, the government readily meets this standard.

Moreover, almost all applications are fact based; *i.e.*, involve only whether the government has shown such connection. Novel issues of law – the situation to which I addressed my New York Times op-ed and my prepared remarks and testimony before the Committee on July 31, 2013 – arise very infrequently. It is only in some (and not necessarily all) of those instances that, despite the review by and comments of the FISC Legal Advisors that a FISC Judge might desire to have independent counsel speak to some or all of the issues in such an application. In other words, the instances when independent counsel might serve a meaningful and useful role before the FISC are likely to be quite infrequent.

Thus, creating an independent office to review *all* applications (where most simply do not raise new issues of constitutional or statutory law) would be redundant and, in my view, unnecessary.

I note, as the Committee no doubt is aware, that Sen. Richard Blumenthal has submitted proposed legislation to create an Office of Special Advocate. His proposal, like that contained in a July 26, 2013, *Boston Globe* op-ed by former Chief Judge Mark L. Wolf of the District of Massachusetts,³ is considerably more substantial and substantive than my modest suggestion that Congress amend the FISA to give express authority to FISC Judges to appoint outside counsel where the government has submitted an application which raises new or novel issues of constitutional or statutory law.

While both Sen. Blumenthal's and Judge Wolf's proposals provide for more extensive independent review and involvement on the part of outside counsel, my proposal, should, I

² As is the case with a Title III application in an ordinary criminal investigation, FISC applications are very lengthy and detailed. The requirement of submission of the read copy provides both the Legal Advisor and duty Judge the necessary opportunity to take the necessary time to review the applications in close detail.

³ Judge Wolf proposes creation of a Cabinet level "Secretary of Civil Liberties." See <http://www.bostonglobe.com/opinion/2013/07/26/acting-judicially/T3ryyd01MqdOVc223aMPeJ/story.html>

believe, be in any event adopted (as, in effect, it would be if Congress enacted Sen. Blumenthal's proposed legislation or the Executive created, as Judge Wolf suggests, a Cabinet level Secretary of Civil Liberties).

QUESTION TWO:

Under your proposal, would the independent attorney be required to argue against the government's position in every instance, or would the attorney be permitted to agree with the government if he or she felt that that position was the required outcome under the law?

ANSWER TO QUESTION TWO:

The independent attorney could, and should reach an independent judgment with regard to the issues – and inform the FISC of his or her views without raising artificial or baseless arguments.

Sometimes this would lead the independent attorney to disagree with the government; other times independent counsel might inform the FISC that the government's assessment of the lawfulness of its request was, in his or her view, entirely correct. Thus, the independent attorney would function as does counsel in a conventional civil or criminal case, where the lawyer does not raise challenges that have no basis simply because the opponent is asking the court to do something in its favor.

Even in that circumstance the independent counsel would be of use to the FISC Judge.

QUESTION THREE:

Do you believe that the FISC is a rubber stamp for the government? If not, what explains the government's high success rate before it? Is that success rate in part the product of a "give and take" process by which the Court reviews the government's applications and provides feedback?

ANSWER TO QUESTION THREE:

I disagree that the Judges of the FISC "rubber stamp" orders. I know that I was not, and, during my years on the FISC (2002-08), the other Judges (whom I came to know well), never struck me as having any inclination to act in that manner.

Like almost all FISC Judges, my rate of approval of *formal applications* was 100%. This was so because, as indicated in Answer to Question One, almost all the applications were simply fact based, and the government readily met the lower FISA standard of probable cause.

The FISA, moreover, properly does not give the FISC Judges discretion to second-guess the usefulness of a particular surveillance. This is as it should be, in view of the unique role the

FISC plays in the President's exercise of his Article II powers and responsibility to conduct our nation's foreign affairs and protect our country from foreign-based dangers. Thus, once the government meets the FISA probable cause standard, as it invariably does in the formal applications, the Judge is duty-bound to issue the order.

In addition, the small number of formally reported denials understates the work and role of the FISC Judges and Legal Advisors. According to my understanding, a "denial" "for the record" occurs only where the government has formally filed and presented an application to a FISC Judge, and the Judge has declined to issue the requested order. For the reasons just stated, denial of a *formal application* is a rare event.

But – and this is very important – there are many other instances where the read copy of an application encounters question from either a Legal Advisor or the FISC duty Judge to whom the government will be submitting the formal application. This can, and does from time to time lead to a decision by the government not to file a formal application before the FISC Judge.⁴

In those instances where no formal denial, and thus no reportable denial occurs, the FISC has acted institutionally to cause the government not to proceed with presentation of a formal application to the FISC duty Judge.

I would recommend, accordingly, that instances where the government, following submission of a read copy, thereafter has not presented a formal application, be reported publicly.

If such reporting occurred (perhaps as "Applications Submitted for Initial Review, But Not Formally Presented"), Congress and the public would have a more accurate view of the effectiveness of the FISC review and deliberation process.

QUESTION FOUR:

In your experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges?

ANSWER TO QUESTION FOUR:

I do not know the answer to that question.

⁴ I cannot say, for many reasons, not the least of which is faded memory, how common these instances are. But I note the Walton Letter (pg. 2, ¶ 1) alludes to this practice (*i.e.*, submission of the read copy of the application, questions to the government from a Legal Advisor or the FISC duty Judge, and withdrawal or non-submission of the final application).

This is so for two reasons.

First, as noted in the Walton Letter (pg. 1, ¶ 2), duty Judges sit singly. Even if I was aware of who my predecessor had been, rarely, if ever would I know what the applications he or she considered contained or the issues those applications raised. Nor would I know what questions the Legal Advisor or prior duty Judge may have had or how the Judge handled the read copy or final application.

Second, during my tenure, the entire Court would meet semi-annually to discuss various issues.⁵ While I may have known who appointed some of my FISC colleagues, that was not something that appeared to me to affect the positions various Judges expressed during those sessions on any particular topic.

QUESTION FIVE:

On how many occasions during your tenure on the FISC were you informed about an instance of non-compliance with the court's orders by the government? How many, if any, of these occasions involved intentional non-compliance? In each case, did the government remedy the situation satisfactorily?

ANSWER TO QUESTION FIVE:

While I can recall learning of instances of non-compliance with an order, I cannot say exactly how many times that occurred. It was, in any event, quite rare – somewhere between a couple and a few times.

As best I can recall, none of those instances involved deliberate non-compliance with an order. When noncompliance with one of my orders occurred, the government's explanation always struck me as being forthright and candid. To the best of my recollection, the government also explained its corrective actions.

[As I was preparing my responses to Sen. Grassley's Questions, the press reported numerous instances of NSA noncompliance with FISC orders since my term on the FISC ended. I do not know either the extent to which agencies have reported noncompliance or how the FISC has handled such reports since I left the Court in May of 2008.

I would note, however, that, were my proposal that Congress give FISC Judges discretion to appoint outside counsel, such appointment could occur not just prior to initial review (and possible appeal) of applications and orders raising new or novel legal issues, but where the government, as required by FISC R. Proc. has notified the FISC of noncompliance with an

⁵ When I was a member of the FISC, the Court did not have, as it now does, *en banc* authority.

order. Adoption of either Judge Wolf's "Civil Liberties" Cabinet position or Sen. Blumenthal's Special Advocate proposal would potentially bring about more extensive monitoring of compliance and more effective responses to notices of noncompliance with FISC orders or rules.]

Respectfully submitted,

James G. Carr
Sr. U.S. District Judge

Toledo, Ohio
August 19, 2013



Answers to Questions for the Record of
The Senate Judiciary Committee

Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy
Director, Washington Legislative Office
American Civil Liberties Union

*Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs*

August 22, 2013

QUESTIONS FROM THE CHAIRMAN

1. **Your written testimony discusses the constitutional implications of the Section 215 phone records program. We have heard government witnesses state repeatedly that under the 1979 case of *Smith v. Maryland*, phone records and other digital data are not protected by the Fourth Amendment because we have already revealed them to a third party, and that only the contents of our communications are protected.**

Q: Do you agree that the *Smith v. Maryland* case provides definitive guidance on the constitutional standard to be applied to the bulk collection of telephone metadata under the Section 215 program? Is there case law suggesting that courts are reconsidering this doctrine in the face of new technology?

Q: In today's world of technological convergence, social media, web browsing, and location-enabled devices, is it possible to draw a clear line between content that is protected by the Fourth Amendment, and non-content information that is not? What implications does this have for the constitutional analysis that is based on this distinction?

The government's reliance on *Smith v. Maryland*, 442 U.S. 735 (1979), is misplaced. The Supreme Court held in *Smith* that the government's use of a so-called "pen register" did not constitute a search under the Fourth Amendment, but the technology at issue in that case was very primitive—it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls. *Id.* at 741. The pen register was in place for less than two days, and it was directed at a single criminal suspect. *Id.* at 737 (noting that pen register was installed after woman who had been robbed began receiving threatening and obscene phone calls from man purporting to be robber). Moreover, the information the pen register yielded was not aggregated with information from other pen registers, let alone with information relating to hundreds of millions of innocent people. *Id.* Nothing in *Smith*—a case involving narrow surveillance directed at a specific criminal suspect over a very limited time period—remotely suggests that the Constitution would be indifferent to the government's mass collection of sensitive information about every single phone call made or received in the United States over a period of seven years. It is also important to remember that *Smith* was decided in 1979, when the government lacked the technological capability to conduct generalized surveillance of telephony metadata, to store the huge volumes of information that would be generated by it, or to analyze that information quickly.

The more relevant case is *United States v. Jones*, 132 S. Ct. 945 (2012), in which five Justices of the Supreme Court concluded that the government's long-term collection and aggregation of location information constituted a search. In *Jones*, the Supreme Court considered whether police had conducted a Fourth Amendment search when they attached a GPS tracking device to a vehicle and monitored its movements over a period of twenty-eight days. The Court held that the installation of the GPS device and the use

of it to monitor the vehicle's movements constituted a search because it involved a trespass "conjoined with . . . an attempt to find something or to obtain information." *Id.* at 951 n.5. In two concurring opinions, five Justices concluded that the surveillance constituted a search because it "impinge[d] on expectations of privacy." *Id.* at 964 (Alito, J., concurring); *accord id.* at 955 (Sotomayor, J., concurring). Justice Sotomayor explained:

GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.

Id. at 955–56 (citations and quotation marks omitted); *see also id.* at 964 (Alito, J., concurring).

What the five concurring Justices observed of long-term location tracking is equally true of the NSA's telephony metadata program. Call records can reveal personal relationships, medical issues, and political and religious affiliations. The government has sought to reassure the public that this program collects "only" metadata, not content, but metadata can be very rich, and the aggregation of metadata permits the government to assemble comprehensive maps of citizens' relationships to one another.

To the extent the government's argument is that individuals lack a constitutionally protected privacy interest in telephony metadata because that information has been shared with telecommunications companies, this argument, too, is mistaken. *Jones* makes clear that mere fact that a person has shared information with the public or a third party does not mean that the person lacks a constitutionally protected privacy interest in it. *Jones*, moreover, is only the most recent in a line of Supreme Court cases confirming that the so-called "third-party records doctrine" is more nuanced than the government contends it is. *See, e.g., Florida v. Jardines*, 133 S. Ct. 1409 (2013) (odors detectable by police dog that emanate outside of a home); *Kyllo v. United States*, 533 U.S. 27 (2001) (thermal imaging available outside a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results in hospital); *Bond v. United States*, 529 U.S. 334, 338–39 (2000) (personal luggage in overhead bin on bus).

2. **As an alternative to the government bulk collection of telephone metadata under Section 215, some have proposed requiring the telecommunications providers to retain these records for five years so the records can be searched when it is deemed necessary.**

Q: Do you believe that such an arrangement would alleviate any privacy concerns that may exist with regard to the Section 215 bulk collection program?

The ACLU opposes legislative proposals that would compel telecommunications providers to create the same kinds of vast databases of Americans' most sensitive information that have until now been maintained by the government in secret. Housing this massive amount of Americans' information in private rather than government hands would not eliminate the potential for abuse and misuse; indeed, in some respects it would increase it. Moreover, the existence of massive databases of information relating to Americans' communications and interactions may have a chilling effect on the freedoms of speech and association even if the databases are in private rather than government hands. The problem with the call-records program is less about who is amassing and retaining those records than about the fact they are being amassed and retained for long periods in the first place.

Moreover, the government has simply not demonstrated that the long-term retention of this kind of sensitive information is actually necessary. As discussed further below, the government has been unable to supply evidence that the metadata program played a crucial role in any specific terrorism investigation or prosecution. The proper course of action for Congress is to end the program, not to repackage it.

QUESTIONS FROM THE RANKING MEMBER

1. Would ending the collection of telephone metadata in bulk under Section 215—and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected—affect the government's ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

There is no evidence that the metadata program has provided uniquely valuable intelligence information. Members of the Senate Select Committee on Intelligence, which oversees the call-tracking program, have made clear that they have seen no evidence either in a public or classified setting that substantiates the intelligence community's general claims about the program's effectiveness.¹ In addition, the Chairman of this Committee reviewed a classified list of terrorist events supposedly prevented by the call-tracking program and reported that the program had not played a role in the breakup of even “several” plots.² The intelligence community has many tools at its disposal to capture and consult call data when it has reason to suspect an individual of terrorism.

¹ Press Release, *Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs*, June 19, 2013, <http://www.wyden.senate.gov/news/press-releases/wyden-udall-issue-statement-on-effectiveness-of-declassified-nsa-programs>.

² Hearing on Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, S. Comm. on the Judiciary (July 31, 2013) (statement of Sen. Patrick Leahy, Chairman), <https://www.leahy.senate.gov/press/senate-judiciary-committee-holds-oversight-hearing-on-government-surveillance-programs>.

Those tools include court orders under FISA and Title III, pen-register orders, national-security letters, and subpoenas—in addition to non-bulk business-records orders under Section 215. All of these tools allow the government to seek information about suspected terrorists without needlessly invading the privacy rights of millions of Americans at the same time.

Some defenders of the call-tracking program have suggested that eliminating ongoing bulk collection under Section 215 would slow down investigations in which speed is paramount, but, again, the public record is devoid of any examples of cases in which the government's possession of years of Americans' phone-call data proved to be important, let alone critical, in timely identifying a phone number of counterterrorism value. Moreover, law enforcement already has the ability to seek emergency orders or administrative subpoenas when time is of the essence. Intelligence officials have repeatedly pointed to one criminal case, *United States v. Moalin*, to defend the utility of the call-records database. But Senator Wyden recently noted to *The Washington Post* that in that case (which involved efforts to send \$8500 to the Somali terrorist group al-Shabaab) the government did not arrest the principal defendant until long after analysis of the call database helped identify him.³

2. **Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. In your view, would such an arrangement resolve your concerns about the legality of the telephone metadata program under Section 215? Why or why not?**

See above.

3. **Has the one-year ban on challenging non-disclosure orders under Section 215 posed practical problems or difficulties for private companies, especially since those companies may challenge the underlying order requiring the production of business records immediately? If so, what are they? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?**

It is of course impossible to know the extent to which the one-year bar has dissuaded private companies from challenging gag orders and has deprived the public of important information about the government's surveillance activities. In an analogous context, however, the recipient of a national-security letter explained the way an FBI-imposed gag order had affected his ability to disclose crucial information to Congress:

The inspector general's report makes clear that NSL gag orders have had even more pernicious effects. Without the gag orders issued on recipients of the letters, it is doubtful that the FBI would have been able to abuse the NSL power the way that it did. Some recipients would have

³ Ellen Nakashima, *NSA Cites Case as Success of Phone Data-Collection Program*, Wash. Post, Aug. 8, 2013, http://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_print.html.

spoken out about perceived abuses, and the FBI's actions would have been subject to some degree of public scrutiny. To be sure, not all recipients would have spoken out; the inspector general's report suggests that large telecom companies have been all too willing to share sensitive data with the agency—in at least one case, a telecom company gave the FBI even more information than it asked for. But some recipients would have called attention to abuses, and some abuse would have been deterred.

I found it particularly difficult to be silent about my concerns while Congress was debating the reauthorization of the Patriot Act in 2005 and early 2006. If I hadn't been under a gag order, I would have contacted members of Congress to discuss my experiences and to advocate changes in the law. The inspector general's report confirms that Congress lacked a complete picture of the problem during a critical time: Even though the NSL statute requires the director of the FBI to fully inform members of the House and Senate about all requests issued under the statute, the FBI significantly underrepresented the number of NSL requests in 2003, 2004 and 2005, according to the report.

I recognize that there may sometimes be a need for secrecy in certain national security investigations. But I've now been under a broad gag order for three years, and other NSL recipients have been silenced for even longer. At some point—a point we passed long ago—the secrecy itself becomes a threat to our democracy. In the wake of the recent revelations, I believe more strongly than ever that the secrecy surrounding the government's use of the national security letters power is unwarranted and dangerous. I hope that Congress will at last recognize the same thing.⁴

The danger of the one-year prohibition is that it may prevent an individual or business from disclosing important information to the public or to Congress until after the value of the information has diminished or disappeared. It is important to remember that most information in the public domain about the government's surveillance programs is provided by the government itself. Gag orders related to the government's use of these programs prevent the public from confronting concrete examples of how these programs affect Americans who are forced to comply with them. Indeed, one reason that the public and Congress have reacted so energetically to the revelations made just a few months ago is that they disclosed the existence of expansive and intrusive government powers that had remained almost entirely secret for many years. Nondisclosure provisions thwart meaningful and necessary discussion about the government's surveillance policies. As a result, they undermine the legitimacy of even properly drawn national-security policies. Wide-ranging and intrusive surveillance programs like the Section 215 call-tracking program require robust and fully informed debate. Gag orders stifle that debate.

⁴ Anonymous, *My National Security Gag Order*, Wash. Post, March 23, 2007, <http://wapo.st/XBX7g>.

At the same time, removing the one-year bar would not jeopardize national security in any way. Removing the bar, after all, would not prevent the government from imposing a gag order; its only effect would be to require the government to defend certain gag orders to a court.

As explained in earlier submitted testimony, the one-year bar is not the only problem with Section 215's gag-order provisions.⁵ Removing the one-year bar, however, should be part of a larger reform package.

4. **Would the government's annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?**
 - a. How many FISA court orders were issued;
 - b. How many individuals' (foreign and U.S. persons) information was collected;
 - c. How many U.S. persons' information was collected; and
 - d. How many U.S. persons' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

5. **Would the government's annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?**
 - a. How many FISA court orders were issued;
 - b. How many individuals' (foreign and U.S. persons) information was collected;
 - c. How many U.S. persons' information was collected; and

6. **Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?**

⁵ See Hearing on Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, S. Comm. on the Judiciary (July 30, 2013) (written testimony of Jameel Jaffer and Laura Murphy), <http://1.usa.gov/18CuNpF> (discussing, among other things, the requirement that reviewing courts defer to the government's determination of whether secrecy is necessary).

- a. **How many FISA court orders the company received;**
 - b. **The percentage of those orders the company complied with;**
 - c. **How many of their users' information they produced; and**
 - d. **How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.**
7. **Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?**
- a. **How many FISA court orders the company received;**
 - b. **The percentage of those orders the company complied with; and**
 - c. **How many of their users' information they produced.**

As we wrote in our earlier-submitted written testimony, the public should have access to basic statistics concerning the government's use of new surveillance authorities. Amendments to FISA made since 2001 have substantially expanded the government's surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of Congress and the public have learned more about domestic surveillance in last three months than in the last several decades combined.

We know of no practical reason why the government could not disclose the statistics listed above. If the government cannot say precisely how many U.S. persons' information was collected, Congress should require it to disclose an estimate. Neither Congress nor the public can evaluate the implications of the government's surveillance activities without knowing how broad those activities are.

Nor do we know of any reason why private corporations could not disclose the statistics listed above. Some private corporations have said they would like to disclose these statistics in order to help the public understand what steps they are taking to protect their customers' privacy.⁶ Some of these corporations have said that the restrictions on their disclosure of these statistics puts them at a disadvantage vis a vis their competitors in other countries.⁷ On June 18, 2013, Google and Microsoft separately petitioned the

⁶ See, e.g., Ted Ulyot, *Facebook Releases Data, Including All National Security Requests*, Facebook Newsroom, June 14, 2013, <https://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests> ("We will continue to be vigilant in protecting our users' data from unwarranted government requests, and we will continue to push all governments to be as transparent as possible.").

⁷ See, e.g., Ryan W. Neal, *NSA Surveillance Costing U.S. Businesses Billions: PRISM, XKeyScore Hurt American Cloud Companies*, Int'l Bus. Times, Aug. 9, 2013, <http://www.ibtimes.com/nsa-surveillance-costing-us-businesses-billions-prism-xkeyscore-hurt-american-cloud-companies>.

FISC arguing that the First Amendment permitted them to release aggregate statistics about two categories of national-security requests: those issued under Section 215 and Section 702.⁸ (These companies already disclose broad approximations of the number of national-security letters they receive, but they have not been permitted to disclose the exact number, or the number of individuals whose privacy was implicated by these letters.⁹) More recently, a coalition of Internet companies including Google and Microsoft—as well as other technology giants like AOL, Apple, Facebook, Mozilla, Twitter, and Yahoo!—signed a public letter addressed to the President, this Committee, and others urging the government to allow regular reporting of statistics reflecting: (1) the number of government requests that they receive under surveillance authorities like Section 215, Section 702, and the national-security-letter statutes; (2) the number of individuals, accounts, or devices about which the government requested under each authority; and (3) the number of requests under each authority that sought communications content, subscriber information, or other information.¹⁰ The companies also requested that the government itself publish a regular “transparency report” that aggregates the total number of requests the government makes under its surveillance authorities as well as the total number of individuals affected by those requests.

It is important to note that aggregate statistics alone would not allow the public to understand the reach of the government’s surveillance powers. As we have seen with Section 215, one application may implicate the privacy of millions of people. It is crucial that Congress require the disclosure of richer statistical information as well as relevant decisions of the FISC.

The release of this information would not compromise national security. There may be a very narrow category of exceptions—for example, the release of certain information by a small Internet Service Provider could, in certain time-limited circumstances, tip off one of its clients about surveillance directed at it. But these exceptions will quite clearly be rare, and any rules surrounding statistical releases can be crafted in ways that avoid these kinds of problems. (One possibility would be to permit private corporations to disclose precise numbers only if they received more than ten demands under a given national-security provision, and otherwise to disclose only that they received between one and ten demands under that provision.)

⁸ See Motion for Declaratory Judgment of Google Inc.’s First Amendment Right to Publish Aggregate Information About FISA Orders, *In re Motion for Declaratory Judgment*, Misc. 13-03 (FISC June 16, 2013), <http://www.uscourts.gov/uscourts/courts/fisc/misc-13-03-motion.pdf>; Microsoft Corporation’s Motion for Declaratory Judgment or Other Appropriate Relief Authorizing Disclosure of Aggregate Data Regarding Any FISA Orders It Has Received, *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, Misc. 13-04 (FISC June 16, 2013), <http://www.uscourts.gov/uscourts/courts/fisc/misc-13-04-motion.pdf>.

⁹ See, e.g., Google, Transparency Report: User Data Requests, <https://www.google.com/transparencyreport/userdatarequests/US/>.

¹⁰ Letter from Coalition to President Barack Obama *et al.* (July 18, 2013), <https://www.aclu.org/files/assets/weneedtoknow-transparency-letter.pdf>.

Again, the release of these statistics would permit a more informed debate about the government's surveillance activities. It would also increase the democratic legitimacy of practices that the country collectively chooses to endorse. In the long run, it could also restore the confidence of Americans and others in the American companies that hold so much sensitive information relating to their users.

- 8. When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?**

The ACLU generally supports proposals to make proceedings before the FISC adversarial. In particular, we support the FISA Court Reform Act of 2013 sponsored by Senators Blumenthal, Wyden, and Udall. That bill would create an Office of the Special Advocate (OSA) to advocate before the FISC for legal interpretations that minimize the scope of intrusion into individual privacy. The OSA would have the authority to appeal FISC decisions. The bill would also allow third parties to participate as amici in cases involving significant or novel issues of law. Finally, it would require the disclosure of significant legal opinions issued by the FISC and the FISCR.

As we stated in our earlier-submitted testimony, we believe that any reform to the FISC should be paired with reforms to the substantive surveillance laws. These laws, including Sections 215 and 702, are far too broad, and no structural reform will be meaningful if the substantive surveillance laws are not significantly narrowed.

- 9. Do you believe that the FISC is a rubber stamp for the government? If not, what explains the government's high success rate before it? Is that success rate in part the product of a "give and take" process by which the Court reviews the government's applications and provides feedback?**

The true problems with the FISC are structural ones—meaning they are capable of being addressed by Congress. In a letter to the Chairman of this Committee dated July 29, 2013, Presiding Judge of the FISC, the Hon. Reggie B. Walton, explained the process by which FISC orders are approved and addressed several questions from the Chairman about the operation of the court.¹¹ Judge Walton described the work of the FISC as an essentially collaborative process between FISC judges, clerks, and staff and government attorneys.¹² He also generally outlined the procedures the court uses to approve regular

¹¹ See Letter from Hon. Reggie B. Walton, Presiding Judge, FISC, to Sen. Patrick Leahy, Chairman, Senate Judiciary Committee (July 29, 2013), <http://www.scribd.com/doc/156993381/FISC-letter-to-Leahy>.

¹² See *id.* at 5–7.

FISA orders, bulk-collection orders under Section 215, as well as Section 702 applications.¹³ In doing so, Judge Walton noted the oft-cited statistic that final FISA applications are approved more than 99% of the time. And he provided a rare window into the operation of an extremely and unusually secretive judicial institution.

As Judge Walton's letter notes, the FISC was created to hear individualized surveillance applications, but its docket has changed quite dramatically in recent years. Thirty years ago, the FISC's principal task was to determine whether the government had, in any given case, demonstrated probable cause to believe that a specific surveillance target was an agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2). Today, the FISC addresses novel and complex statutory and constitutional questions in order to evaluate the lawfulness of broad surveillance programs that rely on complicated and quickly changing technology.

10. Does the Fourth Amendment or any other protections under the Bill of Rights apply to non-U.S. persons in foreign countries? Why or why not? What does this mean for orders issued under Section 702?

Orders issued under Section 702 must conform to the Fourth Amendment not because non-U.S. persons in foreign countries have Fourth Amendment rights but because Americans and others living in the United States have Fourth Amendment rights. Because Americans have a reasonable expectation of privacy in their international communications, surveillance that implicates those communications must conform to the Fourth Amendment's requirements.

This is not to say that Congress should be indifferent to the privacy rights of foreigners living outside the United States. The United States has obligations to respect and protect the rights to privacy and free expression under international instruments like the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It also has a political interest in respecting the privacy rights of foreigners outside the United States. As the Chairman of this Committee has said "repeatedly, . . . just because we have the ability to collect huge amounts of data does not mean that we should be doing so."¹⁶ The damage to the credibility and moral authority of the United States that these surveillance programs has inflicted is plain, and the government's ability to apply pressure to other countries who engage in violations of human rights has been significantly diminished.

11. To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

Public access to the FISA Court's substantive legal reasoning is essential. Without it, some of the government's most far-reaching policies will lack democratic legitimacy.

¹³ *See id.* at 1–5.

¹⁶ *See* Statement of Sen. Patrick Leahy, *supra* note 2.

Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.¹⁷ Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA's sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such opinions, some close to one hundred pages long.¹⁸ We are hopeful that the release of several FISC opinions earlier this week signifies a new commitment on the part of the government to ensure that the public has access to crucial information about the government's surveillance policies.

¹⁷ See, e.g., Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, Wash. Post, June 12, 2013, <http://wapo.st/170VVSu>.

¹⁸ See Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 6, 2013, <http://nyti.ms/12beiA3>.

RESPONSES OF STEWART BAKER TO QUESTIONS SUBMITTED BY SENATOR GRASSLEY

Senate Committee on the Judiciary

“Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs”

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Stewart Baker, Steptoe & Johnson

Question:

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government’s ability to protect national security by “connecting the dots” of terrorist plots? Why or why not?

Response:

This is really a question that the government is in the best position to answer. According to declassified documents, the government, as recently as in 2011, believed that bulk collection of metadata under Section 215 is necessary to locate terrorists in the United States. Apparently, this information would have helped the government find one of the 9/11 hijackers, who was making calls to Yemen from San Diego. There is no reason to believe that the conditions that caused the government to take this position in 2011 have changed. So unless we plan to repeat the errors of 9/11 – by imposing artificial barriers on the government’s ability to use information to keep us safe – my view is that we should continue to allow bulk collection.

Question:

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government’s ability to protect national security and the privacy interests of the public be affected by this potential change?

Response:

This proposal simply isn’t practical for a number of reasons. The first problem with it is that if phone carriers retain the data, the government will be required to tell companies the telephone numbers it is worried about in order to conduct searches. This in itself increases the risk that these programs will be compromised as more actors get in involved with them. Moreover, some telecom providers are foreign-owned. Sharing the searches that the government wishes to conduct with those companies will certainly be less secure.

A second problem with leaving the data in the hands of private companies is that it complicates the process of searching it. The government would no longer be able to conduct searches of data that spans carriers. It would likely need to conduct more searches across more databases in order to obtain the same results. And it would need to find a way to fold all of the data together. This would be a complex and expensive IT problem.

Concerns about cost also apply to the actual storage of the data. If the government is going to require telecom companies to retain their metadata and periodically search it, the government will have to pay for it. Paying for the data to be held and searched by multiple companies in separate storage databases will impose a far greater cost on the government than simply holding it in one place.

Of course, overcoming all of these problems may be worthwhile if having private companies retain the data offered some real benefits for privacy and civil liberties. But it's hard to say what the benefits of this proposal would be. True, under this proposal the government wouldn't actually possess the metadata in question, but it would still be able to search it.

Further, there is no reason to believe that leaving metadata in the hands of private companies will prevent abuse. One thing we can say for certain is that when the government holds the data there are numerous oversight mechanisms, including Congress, the FISA Court, and numerous executive offices

Question:

Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government's ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Response:

I do not have sufficient information to address this question.

Question:

Would the government's annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
- (b) How many individuals' (foreign and U.S. persons) information was collected;

- (c) How many U.S. persons' information was collected; and
 (d) How many U.S. persons' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Response:

This question is quite similar to the question of whether to declassify the annual intelligence budget. People who are already suspicious of the Intelligence Community want this information published. One suggested response is to just publish the topline numbers. But the Intelligence Community rightly points out that just issuing the topline numbers will only lead to more questions and more speculation.

At first blush, the argument that more transparency will make us more comfortable seems compelling. But for national security reasons, we're never ever going to be able to be fully transparent about our FISA activities. Moreover, simply providing numbers in isolation may not communicate meaningful information. It's hard for most of us to really know what constitutes a large or troubling number of FISA court orders. Is a hundred a lot? What about a thousand? Ten thousand? In the absence of complete information, additional data is more likely to be used by people that have already made up their mind to attack the Intelligence Community than it is to make people comfortable with the IC's actions.

Question:

Would the government's annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders were issued;
 (b) How many individuals' (foreign and U.S. persons) information was collected; and
 (c) How many U.S. persons' information was collected.

Response:

See my response above.

Question:

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with;
- (c) How many of their users' information they produced; and
- (d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Response:

Allowing companies to disclose this information poses a risk to our national security. The more detail you release regarding individual companies, the more information you provide to terrorists about which companies to avoid. There's no question that foreign intelligence organizations and terrorist groups are right now analyzing the data that has already been leaked to strengthen their own counterintelligence tactics. Providing company-specific data will only increase the problem.

Question:

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

- (a) How many FISA court orders the company received;
- (b) The percentage of those orders the company complied with; and
- (c) How many of their users' information they produced.

Response:

See my response above.

Question:

When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

Response:

Setting up an independent office to advocate against the government before the FISC is a bad idea, both for the FISC as an institution and for the cause of privacy. Putting in place a

permanent advocate for privacy would turn the FISC proceedings adversarial and force the government to take sides against privacy protection.

This is not how the process works now. Contrary to many of the criticisms that have been circulating, the government largely pulls its punches today. The Department of Justice already sees itself as responsible for balancing privacy and security. The Office of Intelligence at the DOJ plays a role closer to umpire than advocate.

Staff attorneys at the FISC also play a significant role in protecting privacy rights. They're responsible for reviewing FISA warrant applications before they reach the desk of FISC judges. This involves both working with the government to ensure that the requested warrant complies with FISA as well as the US Constitution and providing recommendations to the Court.

If we decide to make the FISC process adversarial, by setting up an independent office to advocate for privacy, then it will necessarily change the FISC process in other ways. The government should no longer be required to pull its punches. It would necessarily have to advocate for its right to catch terrorists, and this would likely weaken internal oversight by agencies like the Office of Intelligence.

I believe that it is a fundamentally bad idea to rely on the FISA court in the way we now do. And loading the court up with more judicial trappings will only heighten the contradiction between the quasi-managerial oversight role it has assumed and the job that judges ordinarily do. I see signs that the court is already allowing its legal judgment to be warped in ways unfavorable to intelligence gathering by the role it has been given. I covered this point in more detail in a recent article on *Skating on Stilts* concerning the claim by Judge Walton of the FISA court that NSA had engaged in misrepresentations to him. Stewart A. Baker, *FISA: The Uncanny Valley of Article III?*, *Skating on Stilts* (Sept. 11, 2013, 12:19 AM), <http://www.skatingonstilts.com/>. It is excerpted below:

There's an old saying that megalomania is an occupational hazard for district court judges. While Chief Judge Walton's opinion doesn't quite succumb to megalomania, there is a distinct lack of perspective in his approach that makes me wonder whether the FISA job slowly distorts a judge's perspective in unhealthy ways.

That was certainly true of Judge Lamberth, who spent most of 2001 persecuting a well-regarded FBI agent for not observing the "wall" between law enforcement and intelligence. That's the wall that the court of appeals found to be utterly without a basis in law but that Chief Judge Lamberth nonetheless enforced with an iron hand. Judge Lamberth forced FISA applicants to swear an oath that they were observing the wall, a tactic that allowed him to sanction the applicants for misrepresentation if they didn't live up to his expectations. He was so aggressive in this pursuit that he had sidelined the most effective FBI counterterrorism teams

in August of 2001. The bureau knew by then that al Qaeda had terrorists in the United States but it couldn't use its best assets to find them because Judge Lamberth had made it clear that he was willing to wreck their careers if they breached the wall.

I fear that Chief Judge Walton is going down the same road -- that the FISA court is the only agency of government not humbled by its failures on the road to 9/11 and is therefore the only agency that will repeat those failures. My concerns are best illustrated by the court's opinion of March 2, 2009, about which I offer three thoughts:

1. In much covered language, the judge claims that the government engaged in "misrepresentations" to the court. This is one of the three alleged misrepresentations mentioned by Chief Judge Bates in an opinion released last month. Since that opinion was released, commentators have widely assumed that NSA has been lying to the court. Because, frankly, that's what "misrepresentation" usually means. But the other filings declassified today show pretty persuasively that there was no intentional misrepresentation. Here's what seems to have happened, in brief. Back in 2006, scrambling to write procedures for the metadata program, a lawyer in NSA's Office of General Counsel wrote in a draft filing that a certain dataset of phone numbers always met the "reasonable articulable suspicion" standard. Turns out that that wasn't true; only some of the numbers did. The lawyer circulated his draft for comment, suggesting that he wasn't absolutely sure of his facts, but no one flagged the error, which turned out to be surprisingly difficult to verify. From then on, NSA and Justice simply copied the original error, over and over, all of their submissions. A mistake for sure. But a "material misrepresentation"? Only to a judge with a very warped view of the world, and the NSA.

2. How about the other headline-grabbing statement in the opinion, that the government's position "strained credulity"? Here, I think the court is on even shakier ground. The debate is about the court's minimization order, which declared that "any search or analysis of the [phone metadata] archive" must adhere to certain procedures. NSA dutifully imposed those procedures on analysts' ability to search or analyze the archive. The problem arose not from giving analysts access to the archive but from some pre-processing NSA performed as the data was flowing into the archive.

If I'm reading the filings properly (and I confess to some uncertainty on this point), NSA keeps an "alert" list of terror-related phone numbers of interest to individual analysts. Since new data shows up at NSA every day, the agency has automated the job of scanning to find those numbers as they show up in the

agency's daily take. The numbers on the alert list are compared to the day's incoming intercept data, and each analyst gets a report telling him how many times "his" numbers appear in which databases.

This alert list was run against data bound for the telephone metadata along with all the other incoming data. The difference was that an analyst who got a "hit" on that database couldn't access it without jumping through the hoops already set up by the FISA court -- reasonable articulable suspicion, special procedures, etc. This must have seemed quite reasonable to the techies at NSA. They knew what it meant for an analyst to "access" the database, and an automated scanning system that yielded only pointers was not the same as giving an analyst access. In the end NSA's office of general counsel came to the same conclusion: the court's orders regulated actual archive access, not scanning against a list for statistics and pointers.

But that's not how Chief Judge Walton saw it. He held that it "strained credulity" to say that alert list scanning was different from "accessing" the archive. Maybe he just didn't understand the technology (the opinion offers some reason to think that). Or maybe he just thought about the question like a judge, always alert to slippery slopes and unintended consequences: "If you can lawfully search this data without limit before the data gets into the archive, you will make meaningless all the limits I've set. Why would you think I'd let you undermine my order in so transparent a way?"

Unfortunately, Judge Walton wasn't thinking like a techie. The techies who implemented the court's order thought they'd been told to restrict access to the database, and they did. They weren't told to restrict the use of statistical tools that scanned incoming data automatically, so they didn't. They certainly didn't believe they were undermining the court's order. Quite the contrary, they had designed the system to make sure that the alert list was just a starting point. Analysts who learned they had a hit in the database couldn't get any further information without meeting the FISA court's "reasonable articulable suspicion" requirement.

It's hard not to see this as a misunderstanding, perhaps exacerbated by the difference between legal and technical cultures. But that's not how Judge Walton sees it. His opinion dismisses the possibility that this could possibly be a good-faith misunderstanding. It's an outrage, he fumes, and efforts to explain it "strain credulity." Frankly, if anything strains credulity in this case, it's that line in the opinion.

3. The chief judge is so sure there's evil afoot that he calls for briefing on "whether the Court should take action regarding persons responsible for any

misrepresentations to the Court or violations of its Orders, either through its contempt powers or by referral to appropriate investigative agencies." For anyone steeped in the disaster caused by Chief Judge Lamberth's witch-hunt for violators of the wall, this is tragically familiar ground. It's almost exactly how the FISA court drove the wall deep into the FBI.

I'm sure we'll be told by the press that this opinion brings to light another scandal and an agency out of control. But that's not how I see it. It looks to me as though NSA was doing its best to implement a set of legal concepts in a remarkably complex network. All complex systems have bugs, and sometimes you only find them when they fail. NSA found a bug and reported it, thinking that it was one more thing to fix. Then the roof fell in.

The interesting question is why it fell in. I think a fair-minded judge encountering the issue for the first time in the courtroom would not likely say that NSA's interpretations were disingenuous or the result of bad faith or misrepresentation. Yet Judge Walton went there from the start.

I suspect that it's because we've unfairly given FISA judges a role akin to a school desegregation master -- more administrator than judge. Instead of resolving a setpiece dispute and moving on, FISA judges are dragged into a long series of linked encounters with the agency. In ordinary litigation, the judges misunderstand things all the time and reach decisions anyway, and they rarely discover all that they've misunderstood. The repetitive nature of the FISA court's contacts with the agency mean that they're always discovering that they only half understood things the last time around. It's only human to put the blame for that on somebody else. And so the judges' tempers get shorter and shorter, the presumption of agency good faith gets more and more frayed. Meanwhile, judges who are used to adulation, or at least respect, from the outside world, keep reading in the press that they are mere "rubber stamps" who should show some spine already. Sooner or later, it all comes together in a classic district judge meltdown, with sanctions, harsh words, and bad law all around.

If I'm right about the all too human frailties that beset the FISA court, building yet more quasijudicial, quasimanagerial oversight structures is precisely the wrong prescription. We'll be forcing judges to expand into a role they are utterly unsuited for and we'll put at risk our ability to actually collect intelligence. In fact, the more adversarial and court-like we make the system, the more weird and disorienting it will become for the judges, who will surely understand that at bottom they are being asked to be managers, not judges.

The further we go down the road, the more likely we are to turn FISA into the Uncanny Valley of Article III.

Question:

In your experience, are there institutional checks and safeguards in place that ensure that the FISC hears both sides of an issue, and not just the government's? If so, what are they and how do they work?

Response:

Yes. As explained above, the FISA warrant process contains a number of safeguards that I believe appropriately protect privacy interests.

Question:

In your experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges? If so, what is that difference?

Response:

In my experience, Democratic appointees to the FISC are indistinguishable from Republican appointees. The presiding judge of the FISC when I was dealing with it as the General Counsel of NSA was appointed by President Carter. The Court during that time was completely fair, and I did not find her or the rest of the court particularly hostile to the Intelligence Community.

The presiding judge that followed was a Republican appointee. During his tenure, the FISC imposed the wall between law enforcement and intelligence activities that I believe was largely responsible for the intelligence failures that led to 9/11 and that I discuss in more detail above. Thus, the most aggressive – and in my view improper -- use of FISA to limit the powers of the Intelligence Community occurred under a Republican appointee.

Question:

Are there any specific reforms to the current law and practice that you would suggest to help ensure that any data the government collects from the 215 and 702 programs is accessed and used only as the law or a court permits?

Response:

One possible area for reform is the obligation to report crimes identified as a result of intelligence programs. This is not an obligation that bears on national security. It is an additional requirement imposed by the DOJ based on the wishes of prosecutors. To the extent that intelligence efforts are being compromised by doubts that information obtained will be used

for prosecutions, additional safeguards are appropriate and unlikely to damage our national security.

Question:

To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

Response:

It is hard to know with certainty, but there is little question that the FISA opinions that have been disclosed have promoted speculation and provided information about the functioning of programs that likely has compromised our national security. The recent decision by the Director of National Intelligence to declassify certain FISC opinions should not be read as indicating that there is no risk to declassification. It simply indicates that the damage being done by the current controversy was deemed to be greater than harm created by disclosure. I would therefore advise caution about further disclosures.

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

A Better Secret Court**New York Times****Op Ed****By JAMES G. CARR****July 22, 2013**

TOLEDO, Ohio — CONGRESS created the Foreign Intelligence Surveillance Court in 1978 as a check on executive authority. Recent disclosures about vast data-gathering by the government have raised concerns about the legitimacy of the court's actions. Congress can take a simple step to restore confidence in the court's impartiality and integrity: authorizing its judges to appoint lawyers to serve the public interest when novel legal issues come before it.

The court is designed to protect individual liberties as the government protects us from foreign dangers. In 1972, the Supreme Court ruled that the Nixon administration had violated the Fourth Amendment by conducting warrantless surveillance on a radical domestic group, the White Panthers, who were suspected of bombing a C.I.A. recruiting office in Ann Arbor, Mich. In 1975 and 1976, the Church Committee, a Senate panel, produced a series of reports about foreign and domestic intelligence operations, including surveillance by the F.B.I. of suspected communists, radicals and other activists — including, notoriously, the Rev. Dr. Martin Luther King Jr.

The Foreign Intelligence Service Act set up the FISA Court in response. To obtain authority to intercept the phone and electronic communications of American citizens and permanent residents, the government must only show probable cause that the target has a connection to a foreign government or entity or a foreign terrorist group. It does not have to show, as with an ordinary search warrant, probable cause that the target is suspected of a crime.

For decades, the court worked under the radar. That changed after 2005, when The New York Times disclosed a National Security Agency program of surveillance of e-mail to and from foreign countries. Though the surveillance was conducted outside of FISA (Congress later specified that FISA court approval was required), the disclosures brought the court to the public's attention. Criticism of the court (on which I served for six years after 9/11, while the caseload grew enormously) revived recently after revelations that the N.S.A., without court orders specifying individual targets, gathered troves of data from companies like Google and Facebook.

Critics note that the court has approved almost all of the government's surveillance requests. Some say the court is virtually creating a secret new body of law governing privacy, secrecy and surveillance. Others have called for declassified summaries of all of the court's secret rulings.

James Robertson, a retired federal judge who served with me on the FISA court, recently called for greater transparency of the court's proceedings. He has proposed the naming of an advocate, with high-level security clearance, to argue against the government's filings. He suggested that the Privacy and Civil Liberties Oversight Board, which oversees surveillance activities, could also provide a check. I would go even further.

In an ordinary criminal case, the adversarial process assures legal representation of the defendant. Clearly, in top-secret cases involving potential surveillance targets, a lawyer cannot, in the conventional sense, represent the target.

Congress could, however, authorize the FISA judges to appoint, from time to time, independent lawyers with security clearances to serve "pro bono publico" — for the public's good — to challenge the government when an application for a FISA order raises new legal issues.

During my six years on the court, there were several occasions when I and other judges faced issues none of us had encountered before. A staff of experienced lawyers assists the court, but their help was not always enough given the complexity of the issues.

The low FISA standard of probable cause — not spinelessness or excessive deference to the government — explains why the court has so often granted the Justice Department's requests. But rapid advances in technology have outpaced the amendments to FISA, even the most recent ones, in 2008.

Having lawyers challenge novel legal assertions in these secret proceedings would result in better judicial outcomes. Even if the government got its way all or most of the time, the court would have more fully developed its reasons for letting it do so. Of equal importance, the appointed lawyer could appeal a decision in the government's favor to the Foreign Intelligence Surveillance Court of Review — and then to the Supreme Court. No opportunity for such review exists today, because only the government can appeal a FISA court ruling.

One obvious objection: judges considering whether to issue an ordinary search warrant hear only from the government. Why should this not be the same when the government goes to the Foreign Intelligence Surveillance Court?

My answer: the court is unique among judicial institutions in balancing the right to privacy against the president's duty to protect the public, and it encounters issues of statutory and constitutional interpretation that no other court does or can.

For an ordinary search warrant, the judge has a large and well-developed body of precedent. When a warrant has been issued and executed, the subject knows immediately. If indicted, he can challenge the warrant. He can also move to have property returned or sue for damages. These protections are not afforded to FISA surveillance targets. Even where a target is indicted, laws like the Classified Information Procedures Act almost always preclude the target from learning

about the order or challenging the evidence. This situation puts basic constitutional protections at risk and creates doubts about the legitimacy of the court's work and the independence and integrity of its judges. To avert these dangers, Congress should amend FISA to give the court's judges the discretion to appoint lawyers to serve not just the interests of the target and the public — but those of the court as well.

James G. Carr, a senior federal judge for the Northern District of Ohio, served on the Foreign Intelligence Surveillance Court from 2002 to 2008.

UNITED STATES FOREIGN
INTELLIGENCE SURVEILLANCE COURT
Washington, D.C.



Honorable Reggie B. Walton
Presiding Judge

July 29, 2013

Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to your letter of July 18, 2013, in which you posed several questions about the operations of the Foreign Intelligence Surveillance Court (the Court). As you requested, we are providing unclassified responses. We would note that, as a general matter, the Court's practices have evolved over time. Various developments in the last several years – including statutory changes, changes in the size of the Court and its staff, the adoption of new Rules of Procedure in 2010, and the relocation of the Court's facilities from the Department of Justice headquarters to a secure space in the federal courthouse in 2009 – have affected some of these practices. The responses below reflect the current practices of the Court.

1. *Describe the typical process that the Court follows when it considers the following: (1) an application for an order for electronic surveillance under Title I of FISA; (2) an application for an order for access to business records under Title V of FISA; and (3) submissions from the government under Section 702 of FISA. As to applications for orders for access to business records under Title V of FISA, please describe whether the process for the Court's consideration of such applications is different when considering requests for bulk collection of phone call metadata records, as recently declassified by the Director of National Intelligence.*

Each week, one of the eleven district court judges who comprise the Court is on duty in Washington. As discussed below, most of the Court's work is handled by the duty judge with the assistance of attorneys and clerk's office personnel who staff the Court. Some of the Court's more complex or time-consuming matters are handled by judges outside of the duty-week system, at the discretion of the Presiding Judge. In either case, matters before the Court are thoroughly reviewed and analyzed by the Court.

Rule 9(a) of the United States Foreign Intelligence Surveillance Court Rules of Procedure

Honorable Patrick J. Leahy
July 29, 2013
Page 2

(FISC Rules of Procedure)¹ requires that except in certain circumstances (i.e., a submission pursuant to an emergency authorization under the statute or as otherwise permitted by the Court), a proposed application must be submitted by the government no later than seven days before the government seeks to have the matter entertained.² Upon the Court's receipt of a proposed application for an order under FISA, a member of the Court's legal staff reviews the application and evaluates whether it meets the legal requirements under the statute. As part of this evaluation, a Court attorney will often have one or more telephone conversations with the government³ to seek additional information and/or raise concerns about the application. A Court attorney then prepares a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws, or other concerns. For example, the attorney may recommend that the judge consider requiring the addition of information to the application; imposing special reporting requirements;⁴ or shortening the requested duration of an authorization.

The judge then reviews the proposed application, as well as the attorney's written analysis.⁵ The judge typically makes a preliminary determination at that time about what course

¹ A copy of the FISC Rules of Procedure is appended hereto as Attachment A. The rules are also available at <http://www.uscourts.gov/uscourts/rules/FISC2010.pdf>.

² A proposed application is also sometimes referred to as a "read copy" and has been referred to in this manner in at least one recent congressional hearing. A proposed application or "read copy" is a near-final version of the government's application, which does not include the signatures of executive branch officials required by statutory provisions such as 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6). As described below, in most circumstances, the government will subsequently file a final copy of an application pursuant to Rule 9(b) of the FISC Rules of Procedure. Both the proposed and final applications include proposed orders.

The process of using proposed applications and final applications is altogether similar to the process employed by other federal courts in considering applications for wiretap orders under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended ("Title III"), which is codified at 18 U.S.C. §§ 2510-2522.

³ In discussing Court interactions with "the government" throughout this document, I am referring to interactions with attorneys in the Office of Intelligence of the National Security Division of the United States Department of Justice.

⁴ Pursuant to 50 U.S.C. §§ 1805(d)(3) and 1824(d)(3), the Court is authorized to assess compliance with the statutorily-required minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

⁵ For each application, the Court retains the attorney's written analysis and the notes made by the judge, so that if the government later seeks to renew the authorization, the judge who considers the next

Honorable Patrick J. Leahy
July 29, 2013
Page 3

of action to take. These courses of action might include indicating to Court staff that he or she is prepared to approve the application without a hearing; indicating an inclination to impose conditions on the approval of the application; determining that additional information is needed about the application; or determining that a hearing would be appropriate before deciding whether to grant the application. A staff attorney will then relay the judge's inclination to the government, and the government will typically proceed by providing additional information, or by submitting a final application (sometimes with amendments, at the government's election) for the Court's ruling pursuant to Rule 9(b) of the FISC Rules of Procedure. In conjunction with its submission of a final application, the government has an opportunity to request a hearing, even if the judge did not otherwise intend to require one. The government might request a hearing, for example, to challenge conditions that the judge has indicated he or she would impose on the approval of an application. If the judge schedules a hearing, the judge decides whether to approve the application thereafter. Otherwise, the judge makes a determination based on the final written application submitted by the government. In approving an application, a judge will sometimes issue a Supplemental Order in addition to signing the government's proposed orders. Often, a Supplemental Order imposes some form of reporting requirement on the government.

If after receiving a final application, the judge is inclined to deny it, the Court will prepare a statement of reason(s) pursuant to 50 U.S.C. § 1803(a)(1). In some cases, the government may decide not to submit a final application, or to withdraw one that has been submitted, after learning that the judge does not intend to approve it. The annual statistics provided to Congress by the Attorney General pursuant to 50 U.S.C. §§ 1807 and 1862(b) – frequently cited to in press reports as a suggestion that the Court's approval rate of applications is over 99% – reflect only the number of *final* applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.⁶

Most applications under Title V of FISA are handled pursuant to the process described above. However, applications under Title V of FISA for bulk collection of phone call metadata records are normally handled by the weekly duty judge using a process that is similar to the one described above, albeit more exacting. The government typically submits a proposed application of this type more than one week in advance. The attorney who reviews the application spends a

application has the benefit of the prior thoughts of the judge(s) and staff, and a written record of any problems with the case.

⁶ Notably, the approval rate for Title III wiretap applications (see note 2 above) is higher than the approval rate for FISA applications, even using the Attorney General's FISA statistics as the baseline for comparison, as recent statistics show that from 2008 through 2012, only five of 13,593 Title III wiretap applications were requested but not authorized. See Administrative Office of the United States Courts, *Wiretap Report 2012*, Table 7 (available at <http://www.uscourts.gov/uscourts/statistics/wiretapreports/2012/Table7.pdf>).

Honorable Patrick J. Leahy
July 29, 2013
Page 4

greater amount of time reviewing and preparing a written analysis of such an application, in part because the Court has always required detailed information about the government's implementation of this authority. The judge likewise typically spends a greater amount of time than he or she normally spends on an individual application, carefully considering the extensive information provided by the government and determining whether to seek more information or hold a hearing before ruling on the application.

As described above, the majority of applications submitted to the Court are handled on a seven-day cycle, by a judge sitting on a weekly duty schedule. Applications that are novel or more complex are sometimes handled on a longer time-line, usually require additional briefing, and are assigned by the Presiding Judge based on judges' availability. Section 702 (i.e., 50 U.S.C. § 1881a) applications⁷ would typically fall into this category.

Where the Court's process for handling Section 702 applications differs from the process described above, it is largely based on the statutory requirements of that section, which was enacted as part of the FISA Amendments Act of 2008 (FAA). Pursuant to 50 U.S.C. §§ 1881a(g)(1)(A) & (g)(2)(D)(i), prior to the implementation of an authorization under Section 702, the Attorney General and the Director of National Intelligence must provide the Court with a written certification containing certain statutorily required elements, and that certification must include an effective date for the authorization that is at least 30 days after the submission of the written certification to the Court.⁸ Under 50 U.S.C. § 1881a(i)(B), the Court must review the certification, as well as the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e), not later than 30 days after the date on which the certification and procedures are submitted. The statutorily-imposed deadline for the Court's review typically coincides with the effective date identified in the final certification filed with the Court.

The government's submission of a Section 702 application typically includes a cover filing that highlights any special issues and identifies any changes that have been made relative to the prior application. The government has typically filed proposed (read copy) Section 702 applications approximately one month before filing a final application. Proposed Section 702 applications are reviewed by multiple members of the Court's legal staff. At the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the

⁷ "Section 702 application" is used here to refer collectively to a Section 702 certification and supporting affidavit, as well as to the statutorily-required targeting and minimization procedures.

⁸ If the acquisition has already begun (e.g., pursuant to a determination of exigent circumstances under 50 U.S.C. § 1881a(c)(2)) or the effective date is less than 30 days after the submission of the written certification to the Court (e.g., because of an amendment to a certification while judicial review is pending, pursuant to 50 U.S.C. § 1881a(i)(1)(C)), 50 U.S.C. § 1881a(g)(2)(D)(ii) requires the certification to include the date the acquisition began or the effective date of the authorization.

Honorable Patrick J. Leahy
July 29, 2013
Page 5

Court's legal staff may request a meeting with the government to discuss a proposed application. Also at the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the Court legal staff may request additional information from the government or convey a judge's concerns about the legal sufficiency of a proposed Section 702 application. Following these interactions, the government files a final Section 702 application, which the government may have elected to amend based on any concerns raised by the judge.

The judge reviews the final Section 702 application and may set a hearing if he or she has additional questions about it. If the judge finds (based on the written submission alone or the written submission in combination with a hearing) that the certification contains all of the required elements, and that the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States, the judge enters an order approving the certification in accordance with 50 U.S.C. § 1881a(i)(3)(A). As required by 50 U.S.C. § 1881a(i)(3)(C), the judge also issues an opinion in support of the order. If the judge finds that the certification does not contain the required elements or the targeting and minimization procedures are inconsistent with the requirements of 50 U.S.C. §§ 1881a(d) & (e), or the Fourth Amendment, the judge will, pursuant to 50 U.S.C. § 1881a(i)(3)(B), issue an order directing the government to, at the government's election and to the extent required by the Court's order, either correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order, or cease, or not begin, the implementation of the authorization for which the certification was submitted. Subsequent review of any remedial measures taken by the government may then be required and may result in another order and opinion pursuant to 50 U.S.C. § 1881a(i).

2. *When considering such applications and submissions, please describe the interaction between the government and the Court (including both judges and court staff), including any hearings, meetings, or other means through which the Court has the opportunity to ask questions or seek additional information from the government. Please describe how frequently such exchanges occur, and generally what types of additional information that the Court might request of the government, if any. Please also describe how frequently the Court asks the government to make changes to its applications and submissions before ruling.*

The process through which the Court interacts with the government in reviewing proposed applications, seeking additional information, conveying Court concerns, and adjudicating final applications, is very similar to the process employed by other federal courts in considering applications for wiretap orders under Title III (discussed in notes 2 and 6 above).

Under FISA practice, the first set of interactions often take place at the staff level. The Court's legal staff frequently interacts with the government in various ways in the context of

Honorable Patrick J. Leahy
July 29, 2013
Page 6

examining the legal sufficiency of applications before they are presented in final form to a judge. Indeed, in the process of reviewing the government's applications and submissions in order to provide advice to the judge, the legal staff interact with the government on a daily basis. These daily interactions typically consist of secure telephone conversations in which legal staff ask the government questions about the legal and factual elements of applications or submissions. These questions may originate with legal staff after an initial review of an application or submission, or they may come from a judge.

At the direction of the Presiding Judge or the judge assigned to a matter, Court legal staff sometimes meet with the government in connection with applications and submissions. The Court typically requests such meetings when a proposed application or submission presents a special legal or factual concern about which the Court would like additional information (e.g., a novel use of technology or a request to use a new surveillance or search technique). The frequency of such meetings varies depending on the Court's assessment of its need for additional information in matters before it and the most conducive means to obtain that information. Court legal staff may meet with the government as often as 2-3 times a week, or as few as 1-2 times a month, in connection with the various matters pending before the Court.

Pursuant to 50 U.S.C. § 1803(a)(2)(A) and Rule 17(a) of the FISC Rules of Procedure, the Court also holds hearings in cases in which a judge assesses that he or she needs additional information in order to rule on a matter. The frequency of hearings varies depending on the nature and complexity of matters pending before the Court at a given time, and also, to some extent, based on the individual preferences of different judges. Hearings are attended, at a minimum, by the Department of Justice attorney who prepared the application and a fact witness from the agency seeking the Court's authorization.

The types of additional information sought from the government – through telephone conversations, meetings, or hearings – include, but are not limited to, the following: additional facts to justify the government's belief that its application meets the legal requirements for the type of authority it is seeking (e.g., in the case of electronic surveillance, that might include additional information to justify the government's belief that a target of surveillance is a foreign power or an agent of a foreign power, as required by 50 U.S.C. § 1804(a)(3)(A), or that the target is using or about to use a particular facility, as required by 50 U.S.C. § 1804(a)(3)(B)); additional facts about how the government intends to implement statutorily required minimization procedures (see, e.g., 50 U.S.C. §§ 1801(h); 1805(a)(3); 1824(a)(3); 1861(c)(1); 1881a(i)(3)(A); and 1881c(c)(1)(c)); additional information about the government's prior implementation of a Court order, particularly if the government has previously failed to comply fully with a Court order; or additional information about novel issues of technology or law (see Rule 11 of FISC Rules of Procedure).

In a typical week, the Court seeks additional information or modifies the terms proposed

Honorable Patrick J. Leahy
 July 29, 2013
 Page 7

by the government in a significant percentage of cases.⁹ (The Court has recently initiated the process of tracking more precisely how frequently this occurs.) The judge may determine, for example, that he or she cannot make the necessary findings under the statute without the addition of information to the application, or that he or she can approve only some of the authorities sought through the application. The government then has the choice to alter its final application or proposed orders in response to the judge's concerns; request a hearing to address those concerns; submit a final application without changes; or elect not to proceed at all with a final application. If the government files a final application, the Court may, on its own, make changes to the government's proposed orders (or issue totally redrafted orders) to address the judge's concern about a given application. The judge may choose, for example, to make an authorization of a shorter duration than what was requested by the government, or the judge may issue a Supplemental Order imposing special reporting or minimization requirements on the government's implementation of an authorization.

3. *Public FISA Court opinions and orders make clear that the Court has considered the views of non-governmental parties in certain cases, including a provider challenge to the Protect America Act of 2007. Describe instances where non-governmental parties have appeared before the Court. Has the Court invited or heard views from a nongovernmental party regarding applications or submissions under Title I, Title V, or Title VII of FISA? If so, how did this come about, and what was the process or mechanism that the Court used to enable such views to be considered?*

FISA does not provide a mechanism for the Court to invite the views of nongovernmental parties. In fact, the Court's proceedings are *ex parte* as required by the statute (see, e.g., 50 U.S.C. §§ 1805(a), 1824(a), 1842(d)(1) & 1861(c)(1)), and in keeping with the procedures followed by other courts in applications for search warrants and wiretap orders. Nevertheless, the statute and the FISC Rules of Procedure provide multiple opportunities for recipients of Court orders or government directives to challenge those orders or directives, either directly or through refusal to comply with orders or directives. Additionally, as detailed below, there have been several instances – particularly in the past several months – in which nongovernmental parties have appeared before the Court outside of the context of a challenge to an individual Court order or government directive.

There has been one instance in which the Court heard arguments from a nongovernmental party that sought to substantively contest a directive from the government. Specifically, in 2007, the government issued directives to Yahoo!, Inc. (Yahoo) pursuant to Section 105B of the Protect America Act of 2007 (PAA). Yahoo refused to comply with the directives, and the government

⁹ This assessment does not include minor technical or typographical changes, which occur more frequently.

Honorable Patrick J. Leahy
July 29, 2013
Page 8

filed a motion with this Court to compel compliance. The Court ordered and received briefing from both parties, and rendered a decision in April 2008.¹⁰

As noted above, the FISC Rules of Procedure and the FISA statute provide opportunities for the appearance of nongovernmental parties before the Court in matters pending pursuant to Titles I, V and VII of the statute. For example, Rule 19(a) of the FISC Rules of Procedure provides that if a person or entity served with a Court order fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. Thus, a nongovernmental party served with an order may invite an opportunity to be heard by the Court through refusal to comply with an order.

With respect to applications filed under Title V of FISA, 50 U.S.C. § 1861(f)(2)(A)(i) provides that a person receiving a production order may challenge the legality of that order by filing a petition with the Court. The same section of the statute provides that the recipient of a production order may challenge the non-disclosure order imposed in connection with a production order by filing a petition to modify or set aside the nondisclosure order. Rules 33-36 of the FISC Rules of Procedure delineate the procedures and requirements for filing such petitions, including the time limits on such challenges. To date, no recipient of a production order has opted to invoke this section of the statute.

With respect to applications filed under Title VII of FISA, 50 U.S.C. § 1881a(h)(4)(A) provides that an electronic communication service provider who receives a directive pursuant to Section 702 may file a petition to modify or set aside the directive with the Court. Sections 1881a(h)(4)(A)-(G) of the statute, as well as Rule 28 of the FISC Rules of Procedure, delineate

¹⁰ Yahoo thereafter appealed the Court's decision to the Foreign Intelligence Surveillance Court of Review (FISCR). *See In re Directives [redacted] Pursuant to Section 105b of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008). This is not the only instance in which a nongovernmental entity has appeared before the FISCR. In 2002, the FISCR accepted briefs filed by the ACLU and the National Association of Criminal Defense Lawyers as *amici curiae* in *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

While Yahoo's identity as the provider that challenged these directives was previously under seal pursuant to the FISCR's decision in *In re Directives*, 551 F.3d 1004, 1016-18, the FISCR issued an Order on June 26, 2013, indicating that it does not object to the release of Yahoo's identity, and ordering, among other things, a new declassification review of the FISCR's opinion in *In re Directives*. The FISCR issued this order in response to a motion by Yahoo's counsel, and after receiving briefing by Yahoo and the government. Yahoo also recently filed a motion for publication of the Court's decision that was appealed to the FISCR, resulting in the published opinion in *In re Directives*. The Court granted the motion. Documents related to Yahoo's recent motion to this Court are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Docket No. 105B(g) 07-01.

Honorable Patrick J. Leahy
July 29, 2013
Page 9

the procedures and requirements for such challenges. Relatedly, 50 U.S.C. § 1881a(h)(5)(A) provides that if an electronic communication service provider fails to comply with a directive issued under Section 702, the Attorney General may file a petition with the Court for an order to compel compliance, which would likely result in the service provider's appearance before the Court through its legal representatives. (Section 1881a(h)(5), as well as Rule 29 of the FISC Rules of Procedure, provide further detail on the procedures and requirements for the enforcement of Section 702 directives.) Finally, 50 U.S.C. § 1881a(h)(6) and Rule 31 of the FISC Rules of Procedure allow for the government or an electronic communication service provider to appeal an order of this Court under §§ 1881a(h)(4) or (5) to the FISCR. To date, no electronic communication service provider has opted to challenge a directive issued pursuant to Section 702, although, as noted above, Yahoo refused to comply with government directives issued under the PAA, which resulted in the government invoking a provision under that statute to compel compliance.

As noted above, there have been a number of other instances in which nongovernmental parties have appeared before the Court outside of the context of a direct challenge to a court order or a government directive, particularly recently. Those instances are as follows:

In August 2007, the American Civil Liberties Union (ACLU) filed a motion with the Court for the release of certain records. The Court ordered and received briefing on the matter from the ACLU and the government, and rendered a decision in December 2007. *See In re Motion for Release of Court Records*, 526 F. Supp. 2d 484 (FISA Ct. 2007).

On May 23, 2013, the Electronic Frontier Foundation (EFF) filed a motion with this Court for consent to disclosure of court records, or in the alternative, a determination of the effect of the Court's rules on access rights under the Freedom of Information Act. Following briefing by EFF and the government, the Court issued an Opinion and Order on June 12, 2013. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-01.

On June 12, 2013, the ACLU, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic (Movants) filed a motion with this Court for the release of Court records. The Court ordered and has received briefing on the matter from the Movants and the government. On July 18, 2013, the Court granted the motions of (1) sixteen members of the House of Representatives and (2) a coalition of news media organizations for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-02.

On June 18, 2013, Google, Inc. filed a motion with this Court for declaratory judgment of the company's first amendment right to publish aggregate information about FISA orders. The

Honorable Patrick J. Leahy
July 29, 2013
Page 10

court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and Techfreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-03.

On June 19, 2013, Microsoft Corporation filed a motion in this Court for declaratory judgment or other appropriate relief authorizing disclosure of aggregate data regarding any FISA orders it has received. The court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and Techfreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at <http://www.uscourts.gov/uscourts/courts/fisc/index.html> under Case No. Misc. 13-04.

4. *Please describe the process used by the Court to consider and resolve any instances where the government notifies the Court of compliance concerns with any of the FISA authorities.*

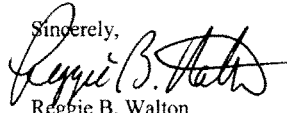
Pursuant to 50 U.S.C. § 1803(h), the Court is empowered to ensure compliance with its orders. Additionally, Rule 13(a) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented (either by government officials or others operating pursuant to Court order) in a manner that did not comply with the Court's authorization or approval or with applicable law. Rule 13(a) also requires the government to notify the Court in writing of the facts and circumstances relevant to the non-compliance; any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

When the government discovers instances of non-compliance, it files notices with the Court as required by Rule 13(a). Because the rule requires the government to "immediately inform the Judge" of a compliance incident, the government typically files a preliminary notice that provides whatever facts are available at the time an incident is discovered. The legal staff review these notices as they are received and call significant matters to the attention of the appropriate judge. In instances in which the non-compliance has not been fully addressed by the time the preliminary Rule 13(a) notice is filed, the Court may seek additional information through telephone calls, meetings, or hearings. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. However, judges sometimes issue orders directing the government to take specific

Honorable Patrick J. Leahy
July 29, 2013
Page 11

actions to address instances of non-compliance either before or after a final notice is filed, and, less frequently, to cease a course of action that the Court considers non-compliant. This process is followed for compliance issues in all matters, including matters handled under Title V and Section 702.

I hope these responses are helpful to the Senate Judiciary Committee in its deliberations.

Sincerely,

Reggie B. Walton
Presiding Judge

Identical letter sent to: Honorable Charles E. Grassley

The attached *Rules of Procedure* for the Foreign Intelligence Surveillance Court supersede both the February 17, 2006 *Rules of Procedure* and the May 5, 2006 *Procedures for Review of Petitions Filed Pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended*. These revised *Rules of Procedure* are effective immediately.

John D. Bates
Presiding Judge
Foreign Intelligence Surveillance Court

November 1, 2010

**UNITED STATES FOREIGN
INTELLIGENCE SURVEILLANCE COURT
Washington, D.C.**

**RULES OF PROCEDURE
*Effective November 1, 2010***

Rule	Page
Title I. Scope of Rules; Amendment	
1. Scope of Rules	1
2. Amendment	1
Title II. National Security Information	
3. National Security Information	1
Title III. Structure and Powers of the Court	
4. Structure	1
5. Authority of the Judges	1
Title IV. Matters Presented to the Court	
6. Means of Requesting Relief from the Court	2
7. Filing Applications, Certifications, Petitions, Motions, or Other Papers ("Submissions")	2
8. Service	3
9. Time and Manner of Submission of Applications	3
10. Computation of Time	4
11. Notice and Briefing of Novel Issues	4
12. Submission of Targeting and Minimization Procedures	5
13. Correction of Misstatement or Omission; Disclosure of Non-Compliance	5
14. Motions to Amend Court Orders	5
15. Sequestration	5
16. Returns	6
Title V. Hearings, Orders, and Enforcement	
17. Hearings	6
18. Court Orders	6
19. Enforcement of Orders	7

Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)

20. Scope	7
21. Petition to Modify or Set Aside a Directive	7
22. Petition to Compel Compliance With a Directive	7
23. Contents of Petition	8
24. Response	8
25. Length of Petition and Response; Other Papers	8
26. Notification of Presiding Judge	8
27. Assignment	8
28. Review of Petition to Modify or Set Aside a Directive	9
29. Review of Petition to Compel Compliance Pursuant to 50 U.S.C. § 1881a(h)(5)(C)	9
30. <i>In Camera</i> Review	9
31. Appeal	9

Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)

32. Scope	10
33. Petition Challenging Production or Nondisclosure Order	10
34. Contents of Petition	10
35. Length of Petition	10
36. Request to Stay Production	10
37. Notification of Presiding Judge	10
38. Assignment	11
39. Initial Review	11
40. Response to Petition; Other Papers	11
41. Rulings on Non-frivolous Petitions	11
42. Failure to Comply	12
43. <i>In Camera</i> Review	12
44. Appeal	12

Title VIII. En Banc Proceedings

45. Standard for Hearing or Rehearing En Banc	12
46. Initial Hearing En Banc on Request of a Party	12
47. Rehearing En Banc on Petition by a Party	12
48. Circulation of En Banc Petitions and Responses	13
49. Court-Initiated En Banc Proceedings	13
50. Polling	13
51. Stay Pending En Banc Review	13
52. Supplemental Briefing	13
53. Order Granting or Denying En Banc Review	13

Title IX. Appeals

54. How Taken 14
55. When Taken 14
56. Stay Pending Appeal 14
57. Motion to Transmit the Record 14
58. Transmitting the Record 14
59. Oral Notification to the Court of Review 14

Title X. Administrative Provisions

60. Duties of the Clerk 14
61. Office Hours 15
62. Release of Court Records 15
63. Practice Before Court 15

Title I. Scope of Rules; Amendment

Rule 1. Scope of Rules. These rules, which are promulgated pursuant to 50 U.S.C. § 1803(g), govern all proceedings in the Foreign Intelligence Surveillance Court (“the Court”). Issues not addressed in these rules or the Foreign Intelligence Surveillance Act, as amended (“the Act”), may be resolved under the Federal Rules of Criminal Procedure or the Federal Rules of Civil Procedure.

Rule 2. Amendment. Any amendment to these rules must be promulgated in accordance with 28 U.S.C. § 2071.

Title II. National Security Information

Rule 3. National Security Information. In all matters, the Court and its staff shall comply with the security measures established pursuant to 50 U.S.C. §§ 1803(c), 1822(e), 1861(f)(4), and 1881a(k)(1), as well as Executive Order 13526, “Classified National Security Information” (or its successor). Each member of the Court’s staff must possess security clearances at a level commensurate to the individual’s responsibilities.

Title III. Structure and Powers of the Court**Rule 4. Structure.**

(a) **Composition.** In accordance with 50 U.S.C. § 1803(a), the Court consists of United States District Court Judges appointed by the Chief Justice of the United States.

(b) **Presiding Judge.** The Chief Justice designates the “Presiding Judge.”

Rule 5. Authority of the Judges.

(a) **Scope of Authority.** Each Judge may exercise the authority vested by the Act and such other authority as is consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.

(b) **Referring Matters to Other Judges.** Except for matters involving a denial of an application for an order, a Judge may refer any matter to another Judge of the Court with that Judge’s consent. If a Judge directs the government to supplement an application, the Judge may direct the government to present the renewal of that application to the same Judge. If a matter is presented to a Judge who is unavailable or whose tenure on the Court expires while the matter is pending, the Presiding Judge may re-assign the matter.

(c) **Supplementation.** The Judge before whom a matter is pending may order a party to furnish any information that the Judge deems necessary.

Title IV. Matters Presented to the Court**Rule 6. Means of Requesting Relief from the Court.**

- (a) **Application.** The government may, in accordance with 50 U.S.C. §§ 1804, 1823, 1842, 1861, 1881b(b), 1881c(b), or 1881d(a), file an application for a Court order (“application”).
- (b) **Certification.** The government may, in accordance with 50 U.S.C. § 1881a(g), file a certification concerning the targeting of non-United States persons reasonably believed to be located outside the United States (“certification”).
- (c) **Petition.** A party may, in accordance with 50 U.S.C. §§ 1861(f) and 1881a(h) and the Supplemental Procedures in Titles VI and VII of these Rules, file a petition for review of a production or nondisclosure order issued under 50 U.S.C. § 1861 or for review or enforcement of a directive issued under 50 U.S.C. § 1881a (“petition”).
- (d) **Motion.** A party seeking relief, other than pursuant to an application, certification, or petition permitted under the Act and these Rules, must do so by motion (“motion”).

Rule 7. Filing Applications, Certifications, Petitions, Motions, or Other Papers (“Submissions”).

- (a) **Filing.** A submission is filed by delivering it to the Clerk or as otherwise directed by the Clerk in accordance with Rule 7(k).
- (b) **Original and One Copy.** Except as otherwise provided, a signed original and one copy must be filed with the Clerk.
- (c) **Form.** Unless otherwise ordered, all submissions must be:
- (1) on 8½-by-11-inch opaque white paper; and
 - (2) typed (double-spaced) or reproduced in a manner that produces a clear black image.
- (d) **Electronic Filing.** The Clerk, when authorized by the Court, may accept and file submissions by any reliable, and appropriately secure, electronic means.
- (e) **Facsimile or Scanned Signature.** The Clerk may accept for filing a submission bearing a facsimile or scanned signature in lieu of the original signature. Upon acceptance, a submission bearing a facsimile or scanned signature is the original Court record.
- (f) **Citations.** Each submission must contain citations to pertinent provisions of the Act.
- (g) **Contents.** Each application and certification filed by the government must be approved and certified in accordance with the Act, and must contain the statements and other information required by the Act.
- (h) **Contact Information in Adversarial Proceedings.**
- (1) **Filing by a Party Other Than the Government.** A party other than the government must include in the initial submission the party’s full name, address, and telephone number, or, if the party is represented by counsel, the full name of the party and the party’s counsel, as well as counsel’s address, telephone number, facsimile number, and bar membership information.
 - (2) **Filing by the Government.** In an adversarial proceeding, the initial

submission filed by the government must include the full names of the attorneys representing the United States and their mailing addresses, telephone numbers, and facsimile numbers.

(i) Information Concerning Security Clearances in Adversarial Proceedings. A party other than the government must:

- (1) state in the initial submission whether the party (or the party's responsible officers or employees) and counsel for the party hold security clearances;
- (2) describe the circumstances in which such clearances were granted; and
- (3) identify the federal agencies granting the clearances and the classification levels and compartments involved.

(j) Ex Parte Review. At the request of the government in an adversarial proceeding, the Judge must review *ex parte* and *in camera* any submissions by the government, or portions thereof, which may include classified information. Except as otherwise ordered, if the government files *ex parte* a submission that contains classified information, the government must file and serve on the non-governmental party an unclassified or redacted version. The unclassified or redacted version, at a minimum, must clearly articulate the government's legal arguments.

(k) Instructions for Delivery to the Court. A party may obtain instructions for making submissions permitted under the Act and these Rules by contacting the Clerk at (202) 357-6250.

Rule 8. Service.

(a) By a Party Other than the Government. A party other than the government must, at or before the time of filing a submission permitted under the Act and these Rules, serve a copy on the government. Instructions for effecting service must be obtained by contacting the Security and Emergency Planning Staff, United States Department of Justice, by telephone at (202) 514-2094.

(b) By the Government. At or before the time of filing a submission in an adversarial proceeding, the government must, subject to Rule 7(j), serve a copy by hand delivery or by overnight delivery on counsel for the other party, or, if the party is not represented by counsel, on the party directly.

(c) Certificate of Service. A party must include a certificate of service specifying the time and manner of service.

Rule 9. Time and Manner of Submission of Applications.

(a) Proposed Applications. Except when an application is being submitted following an emergency authorization pursuant to 50 U.S.C. §§ 1805(e), 1824(e), 1843, 1881b(d), or 1881c(d) ("emergency authorization"), or as otherwise permitted by the Court, proposed applications must be submitted by the government no later than seven days before the government seeks to have the matter entertained by the Court. Proposed applications submitted following an emergency authorization must be submitted as soon after such authorization as is reasonably practicable.

(b) Final Applications. Unless the Court permits otherwise, the final application,

including all signatures, approvals, and certifications required by the Act, must be filed no later than 10:00 a.m. Eastern Time on the day the government seeks to have the matter entertained by the Court.

(c) **Proposed Orders.** Each proposed application and final application submitted to the Court must include any pertinent proposed orders.

(d) **Number of Copies.** Notwithstanding Rule 7(b), unless the Court directs otherwise, only one copy of a proposed application must be submitted and only the original final application must be filed.

(e) **Notice of Changes.** No later than the time the final application is filed, the government must identify any differences between the final application and the proposed application.

Rule 10. Computation of Time. The following rules apply in computing a time period specified by these Rules or by Court order:

(a) **Day of the Event Excluded.** Exclude the day of the event that triggers the period.

(b) **Compute Time Using Calendar Days.** Compute time using calendar days, not business days.

(c) **Include the Last Day.** Include the last day of the period; but if the last day is a Saturday, Sunday, or legal holiday, the period continues to run until the next day that is not a Saturday, Sunday, or legal holiday.

Rule 11. Notice and Briefing of Novel Issues.

(a) **Notice to the Court.** If a submission by the government for Court action involves an issue not previously presented to the Court — including, but not limited to, a novel issue of technology or law — the government must inform the Court in writing of the nature and significance of that issue.

(b) **Submission Relating to New Techniques.** Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court that:

(1) explains the technique;

(2) describes the circumstances of the likely implementation of the technique;

(3) discusses any legal issues apparently raised; and

(4) describes the proposed minimization procedures to be applied.

At the latest, the memorandum must be submitted as part of the first proposed application or other submission that seeks to employ the new technique.

(c) **Novel Implementation.** When requesting authorization to use an existing surveillance or search technique in a novel context, the government must identify and address any new minimization or other issues in a written submission made, at the latest, as part of the application or other filing seeking such authorization.

(d) **Legal Memorandum.** If an application or other request for action raises an issue of law not previously considered by the Court, the government must file a memorandum of law in support of its position on each new issue. At the latest, the memorandum must be

submitted as part of the first proposed application or other submission that raises the issue.

Rule 12. Submission of Targeting and Minimization Procedures. In a matter involving Court review of targeting or minimization procedures, such procedures may be set out in full in the government's submission or may be incorporated by reference to procedures approved in a prior docket. Procedures that are incorporated by reference to a prior docket may be supplemented, but not otherwise modified, in the government's submission. Otherwise, proposed procedures must be set forth in a clear and self-contained manner, without resort to cross-referencing.

Rule 13. Correction of Misstatement or Omission; Disclosure of Non-Compliance.

(a) Correction of Material Facts. If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of:

- (1) the misstatement or omission;
- (2) any necessary correction;
- (3) the facts and circumstances relevant to the misstatement or omission;
- (4) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (5) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission.

(b) Disclosure of Non-Compliance. If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made of:

- (1) the non-compliance;
- (2) the facts and circumstances relevant to the non-compliance;
- (3) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (4) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

Rule 14. Motions to Amend Court Orders. Unless the Judge who issued the order granting an application directs otherwise, a motion to amend the order may be presented to any other Judge.

Rule 15. Sequestration. Except as required by Court-approved minimization procedures, the government must not submit material for sequestration with the Court without the prior approval of the Presiding Judge. To obtain such approval, the government must, prior to tendering the material to the Court for sequestration, file a motion stating the circumstances of the material's acquisition and explaining why it is necessary for such material to be retained in the custody of the Court.

Rule 16. Returns.**(a) Time for Filing.**

(1) **Search Orders.** Unless the Court directs otherwise, a return must be made and filed either at the time of submission of a proposed renewal application or within 90 days of the execution of a search order, whichever is sooner.

(2) **Other Orders.** The Court may direct the filing of other returns at a time and in a manner that it deems appropriate.

(b) Contents. The return must:

(1) notify the Court of the execution of the order;

(2) describe the circumstances and results of the search or other activity including, where appropriate, an inventory;

(3) certify that the execution was in conformity with the order or describe and explain any deviation from the order; and

(4) include any other information as the Court may direct.

Title V. Hearings, Orders, and Enforcement**Rule 17. Hearings.**

(a) **Scheduling.** The Judge to whom a matter is presented or assigned must determine whether a hearing is necessary and, if so, set the time and place of the hearing.

(b) **Ex Parte.** Except as the Court otherwise directs or the Rules otherwise provide, a hearing in a non-adversarial matter must be *ex parte* and conducted within the Court's secure facility.

(c) **Appearances.** Unless excused, the government official providing the factual information in an application or certification and an attorney for the applicant must attend the hearing, along with other representatives of the government, and any other party, as the Court may direct or permit.

(d) **Testimony; Oath; Recording of Proceedings.** A Judge may take testimony under oath and receive other evidence. The testimony may be recorded electronically or as the Judge may otherwise direct, consistent with the security measures referenced in Rule 3.

Rule 18. Court Orders.

(a) **Citations.** All orders must contain citations to pertinent provisions of the Act.

(b) Denying Applications.

(1) **Written Statement of Reasons.** If a Judge denies the government's application, the Judge must immediately provide a written statement of each reason for the decision and cause a copy of the statement to be served on the government.

(2) **Previously Denied Application.** If a Judge denies an application or other request for relief by the government, any subsequent submission on the matter must be referred to that Judge.

(c) **Expiration Dates.** An expiration date in an order must be stated using Eastern Time and must be computed from the date and time of the Court's issuance of the order, or, if applicable, of an emergency authorization.

(d) **Electronic Signatures.** The Judge may sign an order by any reliable, appropriately secure electronic means, including facsimile.

Rule 19. Enforcement of Orders.

(a) **Show Cause Motions.** If a person or entity served with a Court order (the "recipient") fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. The motion must be presented to the Judge who entered the underlying order.

(b) **Proceedings.**

(1) An order to show cause must:

- (i) confirm that the underlying order was issued;
- (ii) schedule further proceedings; and
- (iii) afford the recipient an opportunity to show cause why the recipient should not be held in contempt.

(2) A Judge must conduct any proceeding on a motion to show cause *in camera*. The Clerk must maintain all records of the proceedings in conformance with 50 U.S.C. § 1803(c).

(3) If the recipient fails to show cause for noncompliance with the underlying order, the Court may find the recipient in contempt and enter any order it deems necessary and appropriate to compel compliance and to sanction the recipient for noncompliance with the underlying order.

(4) If the recipient shows cause for noncompliance or if the Court concludes that the order should not be enforced as issued, the Court may enter any order it deems appropriate.

Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)

Rule 20. Scope. Together with the generally-applicable provisions of these Rules concerning filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1881a(h).

Rule 21. Petition to Modify or Set Aside a Directive. An electronic communication service provider ("provider"), who receives a directive issued under 50 U.S.C. § 1881a(h)(1), may file a petition to modify or set aside such directive under 50 U.S.C. § 1881a(h)(4). A petition may be filed by the provider's counsel.

Rule 22. Petition to Compel Compliance With a Directive. In the event a provider fails to comply with a directive issued under 50 U.S.C. § 1881a(h)(1), the government may, pursuant to 50 U.S.C. § 1881a(h)(5), file a petition to compel compliance with the directive.

Rule 23. Contents of Petition. The petition must:

- (a) state clearly the relief being sought;
- (b) state concisely the factual and legal grounds for modifying, setting aside, or compelling compliance with the directive at issue;
- (c) include a copy of the directive and state the date on which the directive was served on the provider; and
- (d) state whether a hearing is requested.

Rule 24. Response.

- (a) **By Government.** The government may, within seven days following notification under Rule 28(b) that plenary review is necessary, file a response to a provider's petition.
- (b) **By Provider.** The provider may, within seven days after service of a petition by the government to compel compliance, file a response to the petition.

Rule 25. Length of Petition and Response; Other Papers.

- (a) **Length.** Unless the Court directs otherwise, a petition and response each must not exceed 20 pages in length, including any attachments (other than a copy of the directive at issue).
- (b) **Other papers.** No supplements, replies, or sur-replies may be filed without leave of the Court.

Rule 26. Notification of Presiding Judge. Upon receipt, the Clerk must notify the Presiding Judge that a petition to modify, set aside, or compel compliance with a directive issued under 50 U.S.C. § 1881a(h)(1) has been filed. If the Presiding Judge is not reasonably available when the Clerk receives a petition, the Clerk must notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge ("Presiding Judge") for the case.

Rule 27. Assignment.

- (a) **Presiding Judge.** As soon as possible after receiving notification from the Clerk that a petition has been filed, and no later than 24 hours after the filing of the petition, the Presiding Judge must assign the matter to a Judge in the petition review pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.
- (b) **Transmitting Petition.** The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

Rule 28. Review of Petition to Modify or Set Aside a Directive.**(a) Initial Review Pursuant to 50 U.S.C. § 1881a(h)(4)(D).**

(1) A Judge must conduct an initial review of a petition to modify or set aside a directive within five days after being assigned such petition.

(2) If the Judge determines that the provider's claims, defenses, or other legal contentions are not warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the Judge must promptly deny such petition, affirm the directive, and order the provider to comply with the directive. Upon making such determination or promptly thereafter, the Judge must provide a written statement of reasons. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

(b) Plenary Review Pursuant to 50 U.S.C. § 1881a(h)(4)(E).

(1) If the Judge determines that the petition requires plenary review, the Court must promptly notify the parties. The Judge must provide a written statement of reasons for the determination.

(2) The Judge must affirm, modify, or set aside the directive that is the subject of the petition within the time permitted under 50 U.S.C. §§ 1881a(h)(4)(E) and 1881a(j)(2).

(3) The Judge may hold a hearing or conduct proceedings solely on the papers filed by the provider and the government.

(c) Burden. Pursuant to 50 U.S.C. § 1881a(h)(4)(C), a Judge may grant the petition only if the Judge finds that the challenged directive does not meet the requirements of 50 U.S.C. § 1881a or is otherwise unlawful.

(d) Continued Effect. Pursuant to 50 U.S.C. § 1881a(h)(4)(F), any directive not explicitly modified or set aside by the Judge remains in full effect.

Rule 29. Review of Petition to Compel Compliance Pursuant to 50 U.S.C. § 1881a(h)(5)(C).

(a) The Judge reviewing the government's petition to compel compliance with a directive must, within the time permitted under 50 U.S.C. §§ 1881a(h)(5)(C) and 1881a(j)(2), issue an order requiring the provider to comply with the directive or any part of it, as issued or as modified, if the Judge finds that the directive meets the requirements of 50 U.S.C. § 1881a and is otherwise lawful.

(b) The Judge must provide a written statement of reasons for the determination. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

Rule 30. *In Camera* Review. Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1881a(h) and conduct related proceedings *in camera*.

Rule 31. Appeal. Pursuant to 50 U.S.C. § 1881a(h)(6) and subject to Rules 54 through 59 of these Rules, the government or the provider may petition the Foreign Intelligence Surveillance Court of Review ("Court of Review") to review the Judge's ruling.

Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)

Rule 32. Scope. Together with the generally-applicable provisions of these Rules regarding filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1861(f).

Rule 33. Petition Challenging Production or Nondisclosure Order.

(a) **Who May File.** The recipient of a production order or nondisclosure order under 50 U.S.C. § 1861 (“petitioner”) may file a petition challenging the order pursuant to 50 U.S.C. § 1861(f). A petition may be filed by the petitioner’s counsel.

(b) **Time to File Petition.**

(1) **Challenging a Production Order.** The petitioner must file a petition challenging a production order within 20 days after the order has been served.

(2) **Challenging a Nondisclosure Order.** A petitioner may not file a petition challenging a nondisclosure order issued under 50 U.S.C. § 1861(d) earlier than one year after the order was entered.

(3) **Subsequent Petition Challenging a Nondisclosure Order.** If a Judge denies a petition to modify or set aside a nondisclosure order, the petitioner may not file a subsequent petition challenging the same nondisclosure order earlier than one year after the date of the denial.

Rule 34. Contents of Petition. A petition must:

(a) state clearly the relief being sought;

(b) state concisely the factual and legal grounds for modifying or setting aside the challenged order;

(c) include a copy of the challenged order and state the date on which it was served on the petitioner; and

(d) state whether a hearing is requested.

Rule 35. Length of Petition. Unless the Court directs otherwise, a petition may not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

Rule 36. Request to Stay Production.

(a) **Petition Does Not Automatically Effect a Stay.** A petition does not automatically stay the underlying order. A production order will be stayed only if the petitioner requests a stay and the Judge grants such relief.

(b) **Stay May Be Requested Prior to Filing of a Petition.** A petitioner may request the Court to stay the production order before filing a petition challenging the order.

Rule 37. Notification of Presiding Judge. Upon receipt, the Clerk must notify the Presiding Judge that a petition challenging a production or nondisclosure order has been filed. If the Presiding Judge is not reasonably available when the Clerk receives the petition, the Clerk must

notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge (“Presiding Judge”) for the case.

Rule 38. Assignment.

(a) **Presiding Judge.** Immediately after receiving notification from the Clerk that a petition has been filed, the Presiding Judge must assign the matter to a Judge in the petition pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.

(b) **Transmitting Petition.** The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

Rule 39. Initial Review.

(a) **When.** The Judge must review the petition within 72 hours after being assigned the petition.

(b) **Frivolous Petition.** If the Judge determines that the petition is frivolous, the Judge must:

- (1) immediately deny the petition and affirm the challenged order;
- (2) promptly provide a written statement of the reasons for the denial; and
- (3) provide a written ruling, together with the statement of reasons, to the Clerk, who must transmit the ruling and statement of reasons to the petitioner and the government.

(c) **Non-Frivolous Petition.**

(1) **Scheduling.** If the Judge determines that the petition is not frivolous, the Judge must promptly issue an order that sets a schedule for its consideration. The Clerk must transmit the order to the petitioner and the government.

(2) **Manner of Proceeding.** The judge may hold a hearing or conduct the proceedings solely on the papers filed by the petitioner and the government.

Rule 40. Response to Petition; Other Papers.

(a) **Government’s Response.** Unless the Judge orders otherwise, the government must file a response within 20 days after the issuance of the initial scheduling order pursuant to Rule 39(c). The response must not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

(b) **Other Papers.** No supplements, replies, or sur-replies may be filed without leave of the Court.

Rule 41. Rulings on Non-frivolous Petitions.

(a) **Written Statement of Reasons.** If the Judge determines that the petition is not frivolous, the Judge must promptly provide a written statement of the reasons for modifying, setting aside, or affirming the production or nondisclosure order.

(b) Affirming the Order. If the Judge does not modify or set aside the production or nondisclosure order, the Judge must affirm it and order the recipient promptly to comply with it.

(c) Transmitting the Judge's Ruling. The Clerk must transmit the Judge's ruling and written statement of reasons to the petitioner and the government.

Rule 42. Failure to Comply. If a recipient fails to comply with an order affirmed under 50 U.S.C. § 1861(f), the government may file a motion seeking immediate enforcement of the affirmed order. The Court may consider the government's motion without receiving additional submissions or convening further proceedings on the matter.

Rule 43. In Camera Review. Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1861(f) and conduct related proceedings *in camera*.

Rule 44. Appeal. Pursuant to 50 U.S.C. § 1861(f)(3) and subject to Rules 54 through 59 of these Rules, the government or the petitioner may petition the Court of Review to review the Judge's ruling.

Title VIII. En Banc Proceedings

Rule 45. Standard for Hearing or Rehearing En Banc. Pursuant to 50 U.S.C. § 1803(a)(2)(A), the Court may order a hearing or rehearing en banc only if it is necessary to secure or maintain uniformity of the Court's decisions, or the proceeding involves a question of exceptional importance.

Rule 46. Initial Hearing En Banc on Request of a Party. The government in any proceeding, or a party in a proceeding under 50 U.S.C. § 1861(f) or 50 U.S.C. § 1881a(h)(4)-(5), may request that the matter be entertained from the outset by the full Court. However, initial hearings en banc are extraordinary and will be ordered only when a majority of the Judges determines that a matter is of such immediate and extraordinary importance that initial consideration by the en banc Court is necessary, and en banc review is feasible in light of applicable time constraints on Court action.

Rule 47. Rehearing En Banc on Petition by a Party.

(a) Timing of Petition and Response. A party may file a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) no later than 30 days after the challenged order or decision is entered. In an adversarial proceeding in which a petition for rehearing en banc is permitted under § 1803(a)(2), a party must file a response to the petition within 14 days after filing and service of the petition.

(b) Length of Petition and Response. Unless the Court directs otherwise, a petition for rehearing en banc and a response to a petition for rehearing en banc each must not exceed 15 pages, including any attachments (other than the challenged order or decision).

Rule 48. Circulation of En Banc Petitions and Responses. The Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide a copy of any timely-filed en banc petition permitted under 50 U.S.C. § 1803(a)(2), and any timely-filed response thereto, to each Judge.

Rule 49. Court-Initiated En Banc Proceedings. A Judge to whom a matter has been presented may request that all Judges be polled with respect to whether the matter should be considered or reconsidered en banc. On a Judge's request, the Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide notice of the request, along with a copy of pertinent materials, to every Judge.

Rule 50. Polling.

(a) **Deadline for Vote.** The Presiding Judge must set a deadline for the Judges to submit their vote to the Clerk on whether to grant a hearing or rehearing en banc. The deadline must be communicated to all Judges at the time the petition or polling request is circulated.

(b) **Vote on Stay.** In the case of rehearing en banc, the Presiding Judge may request that all Judges also vote on whether and to what extent the challenged order or ruling should be stayed or remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

Rule 51. Stay Pending En Banc Review.

(a) **Stay or Modifying Order.** In accordance with 50 U.S.C. §§ 1803(a)(2)(B) and 1803(f), the Court en banc may enter a stay or modifying order while en banc proceedings are pending.

(b) **Statement of Position Regarding Continued Effect of Challenged Order.** A petition for rehearing en banc and any response to the petition each must include a statement of the party's position as to whether and to what extent the challenged order should remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

Rule 52. Supplemental Briefing. Upon ordering hearing or rehearing en banc, the Court may require the submission of supplemental briefs.

Rule 53. Order Granting or Denying En Banc Review.

(a) **Entry of Order.** If a majority of the Judges votes within the time allotted for polling that a matter be considered en banc, the Presiding Judge must direct the Clerk to enter an order granting en banc review. If a majority of the Judges does not vote to grant hearing or rehearing en banc within the time allotted for polling, the Presiding Judge must direct the Clerk to enter an order denying en banc review.

(b) **Other Issues.** The Presiding Judge may set the time of an en banc hearing and the time and scope of any supplemental hearing in the order granting en banc review. The

order may also address whether and to what extent the challenged order or ruling will be stayed or remain in effect pending a decision by the en banc Court on the merits.

Title IX. Appeals

Rule 54. How Taken. An appeal to the Court of Review, as permitted by law, may be taken by filing a petition for review with the Clerk.

Rule 55. When Taken.

(a) **Generally.** Except as the Act provides otherwise, a party must file a petition for review no later than 30 days after entry of the decision or order as to which review is sought.

(b) **Effect of En Banc Proceedings.** Following the timely submission of a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) or the grant of rehearing en banc on the Court's own initiative, the time otherwise allowed for taking an appeal runs from the date on which such petition is denied or dismissed or, if en banc review is granted, from the date of the decision of the en banc Court on the merits.

Rule 56. Stay Pending Appeal. In accordance with 50 U.S.C. § 1803(f), the Court may enter a stay of an order or an order modifying an order while an appeal is pending.

Rule 57. Motion to Transmit the Record. Together with the petition for review, the party filing the appeal must also file a motion to transmit the record to the Court of Review.

Rule 58. Transmitting the Record. The Clerk must arrange to transmit the record under seal to the Court of Review as expeditiously as possible, no later than 30 days after an appeal has been filed. The Clerk must include a copy of the Court's statement of reasons for the decision or order appealed from as part of the record on appeal.

Rule 59. Oral Notification to the Court of Review. The Clerk must orally notify the Presiding Judge of the Court of Review promptly upon the filing of a petition for review.

Title X. Administrative Provisions

Rule 60. Duties of the Clerk.

(a) **General Duties.** The Clerk supports the work of the Court consistent with the directives of the Presiding Judge. The Presiding Judge may authorize the Clerk to delegate duties to staff in the Clerk's office or other designated individuals.

(b) **Maintenance of Court Records.** The Clerk:

(1) maintains the Court's docket and records — including records and recordings of proceedings before the Court — and the seal of the Court;

- (2) accepts papers for filing;
- (3) keeps all records, pleadings, and files in a secure location, making those materials available only to persons authorized to have access to them; and
- (4) performs any other duties, consistent with the usual powers of a Clerk of Court, as the Presiding Judge may authorize.

Rule 61. Office Hours. Although the Court is always open, the regular business hours of the Clerk's Office are 9:00 a.m. to 5:00 p.m. daily except Saturdays, Sundays, and legal holidays. Except when the government submits an application following an emergency authorization, or when the Court otherwise directs, any filing outside these hours will be recorded as received at the start of the next business day.

Rule 62. Release of Court Records.

(a) **Publication of Opinions.** The Judge who authored an order, opinion, or other decision may *sua sponte* or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published. Before publication, the Court may, as appropriate, direct the Executive Branch to review the order, opinion, or other decision and redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).

(b) **Other Records.** Except when an order, opinion, or other decision is published or provided to a party upon issuance, the Clerk may not release it, or other related record, without a Court order. Such records must be released in conformance with the security measures referenced in Rule 3.

(c) **Provision of Court Records to Congress.**

(1) **By the Government.** The government may provide copies of Court orders, opinions, decisions, or other Court records, to Congress, pursuant to 50 U.S.C. §§ 1871(a)(5), 1871(c), or 1881f(b)(1)(D), or any other statutory requirement, without prior motion to and order by the Court. The government, however, must contemporaneously notify the Court in writing whenever it provides copies of Court records to Congress and must include in the notice a list of the documents provided.

(2) **By the Court.** The Presiding Judge may provide copies of Court orders, opinions, decisions, or other Court records to Congress. Such disclosures must be made in conformance with the security measures referenced in Rule 3.

Rule 63. Practice Before Court. An attorney may appear on a matter with the permission of the Judge before whom the matter is pending. An attorney who appears before the Court must be a licensed attorney and a member, in good standing, of the bar of a United States district or circuit court, except that an attorney who is employed by and represents the United States or any of its agencies in a matter before the Court may appear before the Court regardless of federal bar membership. All attorneys appearing before the Court must have the appropriate security clearance.

July 30, 2013

Dear Members of the Senate Judiciary Committee,

We welcome the Senate Judiciary Committee's review of NSA surveillance programs and the impact of these programs on privacy and civil liberties. The undersigned organizations are submitting this coalition letter to emphasize our organizations' agreement on some overall concerns and recommendations.

While additional information is necessary to fully understand the secret legal authorities being used by the government, recent disclosures regarding NSA programs under Section 215 of the Patriot Act and under Section 702 of the FISA Amendments Act raise serious legal and constitutional concerns about the scope of government surveillance. For example, it is difficult to understand how collection of the phone records of millions of Americans who are not suspected of any connection to terrorism could be authorized under the plain terms of Section 215. More significantly, the vast scope of the reported surveillance under Section 215 and Section 702 threatens Americans' First Amendment rights of free association and Fourth Amendment rights. The lack of full information about the scope of such secret national security surveillance increases our concern.

We understand that the NSA's collection of phone records under Section 215 includes metadata and not the content of phone conversations. Although traditionally, courts have not treated such information as being protected by the Fourth Amendment, rapid changes in technology have made metadata more revealing of an individual's private life and courts are taking note. Last year, in *United States v. Jones*, the Supreme Court began to recognize that continuous electronic surveillance for an extended period of time implicates the Fourth Amendment. Although the case involved GPS tracking of a car on public roads and the majority decided the case on relatively narrow grounds, five Justices acknowledged the intrusiveness of powerful electronic surveillance technologies and that continuous use of such technologies over extensive periods of time can impinge on reasonable expectations of privacy. The data collected in the Section 215 program show what numbers are calling each other, when the calls are made, the duration of the calls, and the frequency with which particular numbers call each other. This information, like the pattern of the car's movements in the *Jones* case, can be highly revealing, including demonstrating the patterns of individuals' daily activities and their associations with others. And all of this information is being collected on millions of Americans who are not even suspected of any connection to terrorism. Extensive collection of such non-content meta-data about individuals threatens both First Amendment rights of free association and Fourth Amendment rights to be free from unreasonable searches and seizures.

Similarly, the reportedly broad surveillance of communications content under Section 702 of the FISA Amendments Act threatens First and Fourth Amendment rights. Even though Section 702 surveillance must “target” non-U.S. persons reasonably believed to be abroad, recent disclosures indicate that this surveillance is collecting vast amounts of communications in which U.S. persons (citizens and permanent legal residents) and people located within the United States are on one end of the communication. As the Section 702 surveillance is conducted inside the United States and is deliberately collecting the content of communications of people with recognized Fourth Amendment rights, the limited review conducted by the FISA court under existing law is not adequate to protect these constitutional rights.

We urge Congress to evaluate these surveillance authorities and the risks to civil liberties. In doing so, we urge you to review how other authorities, for example national security letter authorities, overlap, expand or complement the specific authorities under sections 215 and 702. Based upon this review, Congress should enact critical reforms to ensure that government surveillance programs include robust safeguards for constitutional rights. We believe that such reforms should include tightening the standards for collection and use of information, including communications metadata; increasing meaningful judicial authorization and review of such programs, and limiting the secrecy of such programs.

At a minimum, they should include:

1. Enacting legislation to prohibit bulk collection of Americans’ communications metadata under Section 215 or any other authority, and to bar use of Section 215 for prospective surveillance. Passing S. 1215, the bipartisan FISA Accountability and Privacy Protection Act of 2013 co- sponsored by Chairman Leahy and Senators Blumenthal and Lee, would be an important step in this direction.
2. Determining the scope of existing repositories of bulk metadata on U.S. persons and the authorities under which these data were collected and seeking public disclosure of this information, to determine whether or how the government should be permitted to use the bulk metadata already collected.
3. Enacting legislation to provide more rigorous safeguards in Section 702 to restrict the warrantless collection of the content of communications by and metadata concerning U.S. persons or people inside the United States.
4. Pressing for public disclosure of opinions by the Foreign Intelligence Surveillance Court (FISC) containing legal interpretations of the government’s surveillance authorities, redacted as necessary, as well as additional information necessary for public understanding of the scope of surveillance authorities, safeguards for privacy rights and civil liberties, and the historical development of the law since

2001. Passing S. 1130, the bipartisan End Secret Law Act co-sponsored by Senators Merkley and Lee, would be an important step in this direction.

Thank you for your attention to these important issues.

Sincerely,

Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Association of Law Libraries
American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Amicus
Arab American Institute
Association of Research Libraries
Bill of Rights Defense Committee
Hon. Bob Barr
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Center for Media and Democracy
Center for National Security Studies
Citizens for Responsibility and Ethics in Washington
Competitive Enterprise Institute
The Constitution Project
Council on American-Islamic Relations
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org, Inc.
Drum Majors for Truth
Entertainment Consumers Association
Equal Justice Alliance
Firedoglake
Floor64
Foundation for Innovation and Internet Freedom
Free Press Action Fund
Freedom of the Press Foundation
Government Accountability Project
iSolon.org
Liberty Coalition
Media Alliance
Montgomery County Civil Rights Coalition
Mozilla
National Association of Criminal Defense Lawyers

National Coalition Against Censorship
National Forum On Judicial Accountability
National Judicial Conduct and Disability Law Project, Inc.
National Whistleblower Center
OpenMedia International
OpenTheGovernment.org
Organizations Associating for the Kind of Change America Really Needs
PEN American Center
The Plea For Justice Program
PolitiHacks
Power Over Poverty Under Laws of America Restored
Privacy Camp
Project on Government Oversight
Public Knowledge
Reddit
Reporters Without Borders
Rights Working Group
RootsAction.org
Rutherford Institute
Society of Professional Journalists
Students for Sensible Drug Policy
TechFreedom

CC: Members of the Senate

President Barack Obama
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Attorney General Eric Holder
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Director of National Intelligence James R. Clapper
Office of the Director of National Intelligence
Washington, D.C. 20511

General Keith Alexander
Director
National Security Agency
Fort Meade, MD 20755

The Honorable Harry Reid
Senate Majority Leader
S-221, The Capitol
Washington, DC 20510

The Honorable Mitch McConnell
Senate Minority Leader
S-230, The Capitol
Washington, DC 20510

The Honorable John Boehner
Speaker of the House
United States House of Representatives
H-232 The Capitol
Washington, DC 20515

The Honorable Nancy Pelosi
House Minority Leader
H-204, US Capitol
Washington, DC 20515

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

The Honorable Charles E. Grassley
Ranking Member
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

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

The Honorable Dianne Feinstein
Chairman
Senate Permanent Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20515

The Honorable Saxby Chambliss
Vice Chairman
Senate Permanent Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20515

The Honorable Mike Rogers
Chairman
House Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Dutch Ruppersberger
Ranking Member
House Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

We the undersigned are writing to urge greater transparency around national security-related requests by the US government to Internet, telephone and web-based service providers for information about their users and subscribers.

First, the US government should ensure that those companies who are entrusted with the privacy and security of their users' data are allowed to regularly report statistics reflecting:

- The number of government requests for information about their users made under specific legal authorities such as Section 215 of the USA PATRIOT Act, Section 702 of the FISA Amendments Act, the various National Security Letter (NSL) statutes, and others;

- The number of individuals, accounts or devices for which information was requested under each authority; and
- The number of requests under each authority that sought communications content, basic subscriber information, and/or other information.

Second, the government should also augment the annual reporting that is already required by statute by issuing its own regular “transparency report” providing the same information: the total number of requests under specific authorities for specific types of data, and the number of individuals affected by each.

As an initial step, we request that the Department of Justice, on behalf of the relevant executive branch agencies, agree that Internet, telephone and web-based service providers may publish specific numbers regarding government requests authorized under specific national security authorities, including the Foreign Intelligence Surveillance Act (FISA) and the NSL statutes. We further urge Congress to pass legislation requiring comprehensive transparency reporting by the federal government and clearly allowing for transparency reporting by companies without requiring companies to first seek permission from the government or the FISA Court.

Basic information about how the government uses its various law enforcement-related investigative authorities has been published for years without any apparent disruption to criminal investigations. We seek permission for the same information to be made available regarding the government’s national security-related authorities.

This information about how and how often the government is using these legal authorities is important to the American people who are entitled to have an informed public debate about the appropriateness of those authorities and their use, and to international users of US-based service providers who are concerned about the privacy and security of their communications.

Just as the United States has long been an innovator when it comes to the Internet and products and services that rely upon the Internet, so too should it be an innovator when it comes to creating mechanisms to ensure that government is transparent, accountable, and respectful of civil liberties and human rights. We look forward to working with you to set a standard for transparency reporting that can serve as a positive example for governments across the globe.

Thank you.

Companies

AOL
 Apple
 CloudFlare
 CREDO Mobile
 Digg
 Dropbox
 Evoca
 Facebook
 Google
 Heyzap
 LinkedIn
 Meetup
 Microsoft
 Mozilla
 Reddit
 salesforce.net
 Sonic.net
 Tumblr
 Twitter

Civil Society Organizations

Access
 American Booksellers Foundation for Free Expression
 American Society of News Editors
 American Civil Liberties Union
 Americans for Tax Reform
 Brennan Center for Justice at NYU Law School
 Center for Democracy & Technology
 Center for Effective Government
 Committee to Protect Journalists
 Competitive Enterprise Institute
 The Constitution Project
 Demand Progress
 Electronic Frontier Foundation
 First Amendment Coalition
 Foundation for Innovation and Internet Freedom
 Global Network Initiative
 GP-Digital
 Human Rights Watch

Wikimedia Foundation
Yahoo!
YouNow

Trade Associations & Investors

Boston Common Asset Management
Computer & Communications Industry
Association
Domini Social Investments
Internet Association
New Atlantic Ventures
Union Square Ventures
Y Combinator

National Association of Criminal Defense
Lawyers
National Coalition Against Censorship
New America Foundation's Open Technology
Institute
OpenTheGovernment.org
Project on Government Oversight
Public Knowledge
Reporters Committee for Freedom of The Press
Reporters Without Borders
TechFreedom
World Press Freedom Committee

Written Testimony of Marc J. Zwillinger

Founder

ZwillGen PLLC

United States Senate Committee on the Judiciary

Hearing on

***Strengthening Privacy Rights and National Security: Oversight of FISA
Surveillance Programs***

Washington, D.C.

July 31, 2013



Chairman Leahy, Ranking Member Grassley and Members of the Committee,

Thank you for asking me to submit written testimony about FISA oversight and specifically regarding my experience when confronted with government demands for user data under FISA and the FISA Amendments Act

By way of background, I worked as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last thirteen years I have had a private practice specializing in representing companies, including internet service providers, email providers, cloud services, social networking companies, and wireless carriers on issues related to government demands for user data under the Electronic Communications Privacy Act ("ECPA"), the Foreign Intelligence Surveillance Act ("FISA") and the FISA Amendments Act ("FAA").

I may also be the only private sector attorney to have ever appeared on behalf of a provider before the Foreign Intelligence Court of Review.¹ To be clear, I am submitting my written testimony today solely in my individual capacity, based on many experiences representing multiple clients from Apple to Yahoo!, and not on behalf of any one of them.

Although foreign intelligence surveillance is surely critical for national security, the FISA process has certain flaws which render it inconsistent with the core principles that are the foundation of this country's legal system. The most significant areas of concern are: (1) the lack of a true adversarial process with regard to specific legal issues that arise before the FISA court; and (2) the cloak of secrecy which covers not only the identity of targets, but also most everything else surrounding the actual operation of the surveillance processes authorized by FISA and the FAA, including the existence of an individual piece of legal process, the numbers of affected accounts, the legal arguments that support the government's demands, and the FISA court's decisions. In this secret process, in certain instances, the statute leaves the provider in the position of being the only bulwark against potential government overreaching, especially with regard to the Section 702 Directive process in which the FISA court has only limited authority to review the process where it is not challenged by a provider.² But for the reasons

¹ I was counsel to Yahoo! when it challenged the lawfulness of the directives served on it pursuant to the Protect America Act ("PAA"), the predecessor to the FAA, during 2007-2008. That challenge resulted in the partially released decision *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (Foreign Intl. Ct. of Rev. 2008), upholding the constitutionality of the PAA Directive process. It is possible that subsequent challenges by other providers may exist and remain under seal.

² In the criminal process, the legality of surveillance is usually tested when the evidence is sought to be introduced against the defendant. Because intelligence gathered for foreign intelligence purposes is rarely, if ever, used in criminal prosecutions, there will be no defendant to eventually challenge the surveillance.

described below, providers face significant pressure to comply with the government demands in some form rather than challenging them.

Accordingly, I believe the Senate should focus on adding stronger built-in safeguards to protect the rights of U.S. citizens and bringing greater transparency to the types of process used, the number of accounts affected, the legal arguments made, and the decisions that support surveillance orders. Though some aspects of any legal proceeding related to intelligence gathering -- like the target's identity -- must always remain secret, the current way the system operates -- which leaves only providers with the ability to challenge the government -- but forces them to do so in complete secrecy, can lead to legal interpretations that might not survive the light of public scrutiny. This system is insufficient for the reasons described below.

First, any FISA process a provider receives is under seal and classified. The company receiving an order (or directive) is restricted in their handling of the demand, which in turn, can adversely impact the amount of review it may receive. For example, a provider with limited resources or one who is new to receiving classified orders, may have no cleared employees, or the cleared employees may not be members of the legal department or executive management authorized to employ the substantial legal resources required to raise such a challenge. This makes internal escalation of individual demands extremely difficult. In addition, issues related to the storage of classified information often restrict the provider's ability to keep and refer back to the legal process. Instead, the government holds the demand itself and shares it with the company only upon initial service and then on request. Thus, in practice, a provider in these circumstances can be influenced by the government's view of what is within the scope of the request. And where the provider does seek the advice of outside counsel to evaluate the demand -- while under intense time pressure to start the surveillance -- the number of lawyers qualified and cleared to provide advice on FISA issues is small.

Second, without published cases to examine, providers are left with an uncertain basis upon which to base a challenge to an order or a directive, especially since the provider knows that the court has already approved the issuance of process after some limited review, the scope of which is not readily apparent. Also, there is often no way for a provider to determine whether such process is routine, or has been complied with by other similarly situated providers. This problem is especially acute with directives issued under 702, which, are not required by statute to contain information on the specific targets at the time the directives are issued. Nothing in the FAA prevents the government from identifying new specific targets after the directives have been issued. Yet it is the directives themselves, and not any subsequent orders identifying individual targets under the directives that the FAA specifically allows providers to challenge. Faced with limited information, no visibility into the basis for the certification, no ability to

disclose even the fact of the order or directive to anyone else (even other industry participants), providers are fairly isolated in determining the proper response. Indeed, one of the most valuable roles I can play as outside counsel is to help clients recognize the difference between a routine order and one based on a novel legal theory, which I am able to do on occasion because I represent multiple companies who receive national security demands. A lawyer representing only one client on such matters might not have any basis, other than representations from the government or the FISA court itself, to identify novel orders and arguments.

Third, there are some institutional pressures and procedural disincentives against levying a challenge. As various transparency reports issued by certain providers make clear, large providers have to deal with representatives of the Department of Justice regarding thousands of annual criminal and intelligence demands for user data. As a result, providers who challenge governmental authority could face pressure from the government in other areas, including delays in responding to criminal legal process. Moreover, the government can show little to no flexibility in applying a fairly rigid process of handling classified information where access is needed even to review process, let alone bring a challenge. This makes levying a challenge logistically difficult. Only cleared personnel and counsel can participate in such a challenge or discuss details of the Section 702 process and directives. With no public transparency, no ability to enlist amicus or industry participation,³ and a classification system that may limit the ability to brief internal and external corporate, legal, and business advisors, and limited counsel choices because many lawyers lack section 702 experience and clearances, only certain providers can contemplate challenging government orders or directives and only in fairly significant matters.

If a provider brings a challenge, the statutory process does not necessarily provide for complete transparency or a level playing field for the provider. As the published decision in *In re Directives* makes clear, a phalanx of 11 government lawyers, including the Acting Solicitor General of the United States, was involved in defending the statute.⁴ And the decision also makes clear that the company had to overcome the hurdle of demonstrating that it had

³ By contrast, when Yahoo! challenged what it believed to be an unconstitutional criminal order in the District of Colorado, many interest groups joined Yahoo! as amicus and the government ultimately withdrew its demand for additional documents.

⁴ According to the opinion, the government was represented in the case by Gregory G. Garre, Acting Solicitor General, Mark Filip, Deputy Attorney General, J. Patrick Rowan, Acting Assistant Attorney General, John A. Eisenberg, Office of the Deputy Attorney General, John R. Phillips, Office of Legal Counsel, Sharon Swingle, Civil Division, and Matthew G. Olsen, John C. Demers, Jamil N. Jaffer, Andrew H. Tannenbaum, and Matthew A. Anzaldi, National Security Division, United States Department of Justice. This does not count the Attorney General, Michael B. Mukasey, who was listed on the brief but may not have contributed to the briefing. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (Foreign Intl. Ct. of Rev. 2008).

standing to appear to litigate these issues -- notwithstanding fairly clear legislative language that authorized a provider to challenge the directives issued under the PAA.⁵ The decision also shows that some of the documents relied upon in the decision of the Court of Review were classified procedures submitted as part of an *ex parte* appendix that remains sealed.⁶

My point is not that the Court of Review should have reached a different conclusion in 2008. When additional portions of the decision and the legal briefs are unsealed, lawyers, Fourth Amendment scholars and the public can reach their own conclusion on that score. My point is that the existing statute -- which allows the court to do a fulsome review of a directive only when a provider levies a challenge -- does not provide the type of institutional safeguards that are typically built into our adversarial court system. In the history of the directive program under the PAA and the FAA, it may turn out that only one company has ever tried to challenge the lawfulness of the process. And that challenge included *ex parte* filings by the government, filings which were not disclosed even to cleared lawyers within the context of the sealed proceeding. Compare this to criminal legal process, which is much easier for providers to challenge when received, and is subject to a second set of challenges by criminal defendants, if the data is ever used in a criminal proceeding. The FAA simply does not provide for a similar type of adversary process on which the American judicial system is largely based.

The current system of checks and balances under the FAA is simply not sufficient. It's not due to a lack of desire on the part of the providers to defend their users. Quite the opposite, the types of providers I represent do have strong business reasons to challenge any overstepping of surveillance authority by the government or new legislation that may not provide adequate constitutional protections to their user's privacy. In some cases, if these companies do not rigorously enforce the limits imposed by law on the government, it can place increasing pressure on providers to turn over user data. Such pressure is not only a burden for the companies, but raises serious concerns about losing the trust of their users. If users do not trust these companies, they can and will take their business elsewhere.⁷ But Internet companies run the gamut from large entities such as Yahoo!, which had the will and the wherewithal to fight the directive process, to startups and smaller providers who may not have the money, knowledge, counsel or capability to fight government requests.

⁵ See *Id.* at 1008-09.

⁶ "The [redacted text] procedures [redacted text] are delineated in an *ex parte* appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. [redacted text] Although the PAA itself does not mandate a showing of particularity, see 50 U.S.C. § 1805b (b) , this pre-surveillance procedure strikes us as analogous to and in conformity with the particularity showing contemplated by Sealed Case. See 551 F.3d at 1013-14,

⁷ For these precise reasons, several of my clients are members of the Due Process Coalition which is seeking amendments to the Electronic Communications Privacy Act to better protect user privacy in a manner more consistent with the Fourth Amendment in the context of government demands issued in criminal investigations and prosecutions.

A built-in adversary in the FISA court, in the form of a Guardian *Ad Litem* for the American people would be a significant improvement addition to the existing statutory framework. Such an advocate could participate in all cases involving a new statute or authority or a new interpretation or application of an existing authority. The Guardian could either choose the cases in which to be involved, or the Guardian's participation can be requested by the court or a provider where an opposition would be useful to test and evaluate the legal arguments presented by the government. The Guardian's office could be established with proper security safeguards to draft, store, and access classified records more efficiently. It could also be required to report to the public and Congress the number of cases it has argued and how often it has limited or pared back the government's requests. The Guardian could also brief this committee, and provide a vital counterpoint for members to consider when exercising their oversight duties. Appointing a Guardian *Ad Litem* for the public ensures that novel legal arguments in the FISA court would face a consistent, steady challenge no matter who the provider is. This would make the FISA process stronger by ensuring that results are consistently subject to checks and balances. And, as we have seen, the result of not having such a process allows the court and DOJ work through difficult legal issues with no balancing input. The Guardian would be especially useful in cases where the government demands access to communications in a way that may have a profound impact on people other than the target, such as where decryption made be involved or where a provider is asked to provide assistance in ways that are unlike traditional wiretaps.

The lack of an adversary process and the need for additional transparency into the directives process, the types of legal challenges, and the number of uses affected by it are not the only reforms I would suggest to the Section 702 Directive process, although they would be a strong place to start. In that regard, I commend Senator Leahy and Senator Franken for proposing legislation that would improve the current situation and require more disclosure and mandatory public reporting to bring light to the government's practices. But I would also ask the Senate to consider further how to enhance the ability of providers to bring fair and meaningful challenges when they think it is necessary, and to build in a more systematic adversary, such as a Guardian *Ad Litem*, in appropriate cases.

While most of my written testimony has focused on the procedural deficiencies involved in the FISA and FAA challenge process, the basic premise of the FAA -- that a court order is not needed where one side of a communication is foreign -- should also be reconsidered. The types of communications that can be demanded under 702 directives are not just phone calls, but can also include all electronic content, including emails, instant messages, photos, videos, and stored cloud documents. Yet the framework of 702 is that whenever one party to the communication is reasonably believed to be outside the United States, any content sent to or from that party can be obtained. This paradigm may make sense if surveillance is analogized only to a traditional phone call, where a single foreign side means that conversation is at least

50% foreign. But this is not the case with in an internet communication – like a collaborative cloud document – which can have many “sides.”

For example, if a document stored on a collaborative sharing platform was accessed by 10 people, 9 of whom are in the United States but one of whom is outside the United States and deemed to be a proper surveillance target, the document may be eligible for disclosure under the FAA. Yet that document may have been created by a U.S. person, is usually accessed by U.S. persons, and may be stored in the United States. When such significant U.S. person involvement is present, any government request for surveillance should involve more traditional court involvement – not the minimal review of the 702 process. And, if such collection were to occur, the collection of U.S. communications traffic in such circumstances should not be deemed “incidental,” when it is the predominant activity being captured. Equally problematic is the theoretical issue of documents created in the U.S. and stored in the U.S. that a user then accesses from abroad. Under current law, the Government could argue that simple access from a hotel room in London would open the door to the collection of documents previously protected by the FISA warrant process without a court order simply because a foreign user boarded a plane. Allowing warrantless surveillance of U.S.–centric communications and documents is not consistent with the Fourth Amendment which doesn’t cease to apply just because one participant in the communication, no matter how minor their role, may be foreign. Accordingly, the framework of Section 702 may turn out to be inadequate to protect the interests of U.S. persons in certain circumstances, even if the Executive Branch does take measures to institute its own checks and balances.

Thank you for the opportunity to submit this written testimony. I would be pleased to work with the Committee on an ongoing basis as the process to reform FISA moves forward.



July 30, 2013

The Hon. Patrick Leahy
Chairman
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Hon. Chuck Grassley
Ranking Member
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

Dear Senators Leahy and Grassley and Members of the Senate Judiciary Committee:

The Constitution Project urges the Senate to support the FISA Accountability and Privacy Protection Act of 2013, S. 1215. As debate continues over the recently disclosed NSA programs, Congress should take this opportunity to ensure that we are protecting not only our security but also our constitutional rights and liberties.

The Constitution Project is a bipartisan organization that promotes and defends constitutional safeguards. The Project brings together legal and policy experts from across the political spectrum to promote consensus solutions to pressing constitutional issues. In 2009, well before the recent revelations regarding the scope of the current NSA programs, the Project's Liberty and Security Committee released a report entitled *Statement on Reforming the Patriot Act*. The statement is signed by twenty six policy experts, former government officials, and legal scholars of all political affiliations, and urges Congress to reform the Patriot Act and incorporate more robust protections for constitutional rights and civil liberties. Our Committee's recommendations include urging Congress to tighten the standards for Section 215 orders and national security letters (NSLs) and to provide increased judicial review for "gag orders" under these provisions.

The recent disclosures regarding NSA surveillance programs have underlined the wisdom and increased the urgency of our Committee's proposals. Hastily drafted in the wake of the September 11th attacks, the Patriot Act contains several provisions that give the executive branch extraordinarily broad law enforcement powers which raise serious constitutional concerns, and recent disclosures demonstrate that the government has interpreted these surveillance authorities aggressively. The Constitution Project is pleased to see the introduction of legislation which targets some of the most troubling provisions of the Patriot Act, and would help rein in the NSA's surveillance program under Section 215. The FISA Accountability and Privacy Protection Act (S. 1215) co-sponsored by Chairman Leahy and Senators Blumenthal and Lee is consistent with the recommendations in The Constitution Project's Liberty and Security Committee's report, and passage of this legislation would be an important step toward implementing proper safeguards for constitutional rights.

In particular, the bill would reform Section 215 of the Patriot Act, most notably by tightening the standards for obtaining an order compelling a business to turn over records. Importantly, the bill would also tighten the standards for issuing an NSL, would allow NSL recipients to challenge the nondisclosure or "gag orders" that can accompany NSLs, and would require public reporting on the use of such letters. In addition, TCP commends the bill provisions that would increase public reporting and oversight on the use of these authorities.

In short, The Constitution Project backs the FISA Accountability and Privacy Protection Act because it would protect civil liberties while also ensuring law enforcement's ability to protect our national security. We urge Members of the Senate Judiciary Committee to support this bill.

Sincerely,

A handwritten signature in black ink, appearing to read "Virginia E. Sloan". The signature is fluid and cursive, with the first name "Virginia" being the most prominent part.

Virginia E. Sloan
President
The Constitution Project

~~TOP SECRET//COMINT//NOFORN~~

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Dianne Feinstein
 Chairman
 The Honorable Saxby Chambliss
 Vice Chairman
 Select Committee on Intelligence
 United States Senate
 Washington, DC 20510

Dear Madam Chairman and Mr. Vice Chairman:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the SSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared SSCI, Judiciary Committee, and leadership staff), in a secure location in the SSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the SSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD
 Reason: 1.4(c)
 Declassify on: February 2, 2036~~

~~TOP SECRET//COMINT//NOFORN~~

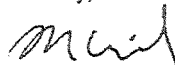
~~TOP SECRET//COMINT//NOFORN~~

The Honorable Dianne Feinstein
The Honorable Saxby Chambliss
Page Two

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that SSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the House Permanent Select Committee on Intelligence (HPSCI) under similar conditions, so that it may be made available to the Members of the House, as well as cleared leadership, HPSCI and House Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich
Assistant Attorney General

Enclosure

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Mike Rogers
 Chairman
 The Honorable C.A. Dutch Ruppertsberger
 Ranking Minority Member
 Permanent Select Committee on Intelligence
 U.S. House of Representatives
 Washington, DC 20515

Dear Mr. Chairman and Congressman Ruppertsberger:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD~~

~~Reason: 1.4(c)~~

~~Declassify on: February 2, 2036~~

~~TOP SECRET//COMINT//NOFORN~~

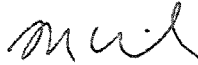
~~TOP SECRET//COMINT//NOFORN~~

The Honorable Mike Rogers
The Honorable C.A. Dutch Ruppersberger
Page Two

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich
Assistant Attorney General

Enclosure

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~~~(TS//SI//NF)~~ Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- (U) Section 215 of the USA PATRIOT Act, which expires at the end of February 2011, allows the government, upon approval of the Foreign Intelligence Surveillance Court ("FISA Court"), to obtain access to certain business records for national security investigations;
- (U) Section 402 of the Foreign Intelligence Surveillance Act ("FISA"), which is not subject to a sunset, allows the government, upon approval of the FISA Court, to install and use a pen register or trap and trace ("pen/trap") device for national security investigations;
- ~~(TS//SI//NF)~~ These authorities support two sensitive and important intelligence collection programs. These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by any person, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the FISA Court and Congress;
- ~~(TS//SI//NF)~~ Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court; and
- ~~(TS//SI//NF)~~ The National Security Agency's (NSA) bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Derived From: NSA/CSSM 1-52
Date: 20070108
Declassify On: 20360101~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~**Background**

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the NSA intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al-Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."

~~(TS//SI//NF)~~ Today, under FISA Court authorization pursuant to the "business records" authority of the FISA (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorist overseas. This and similar programs operated pursuant to FISA, including exercise of pen/trap authorities, provide valuable intelligence information.

(U) Absent legislation, Section 215 will expire on February 28, 2011, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The pen/trap authority does not expire.

~~(TS//SI//NF)~~ The Section 215 and pen/trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant use of these authorities is to support two important and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States. [REDACTED]

[REDACTED] Although these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from certain telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen/trap provision in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail, certain routing information, and the date and time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment.

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.

Checks and Balances

FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen/trap provision. Before obtaining any information from a telecommunications service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed “minimization procedures” required by the FISA Court that govern the retention and dissemination of the information obtained. Before NSA analysts may query bulk records, they must have reasonable articulable suspicion – referred to as “RAS” – that the number or e-mail address they submit is associated with [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

[REDACTED] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. The bulk data collected under each program can be retained for 5 years.

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, through hearings, briefings, and visits to NSA. In addition, the Intelligence and Judiciary Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ In 2009, a number of technical compliance problems and human implementation errors in these two bulk collection programs were discovered as a result of Department of Justice (DOJ) reviews and internal NSA oversight. However, neither DOJ, NSA, nor the FISA Court has found any intentional or bad-faith violations. [REDACTED]

[REDACTED] In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The FISA Court placed several restrictions on aspects of the business records collection program until the compliance processes were improved to its satisfaction. [REDACTED]

(U) The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed safeguards that, together with greater efforts by the Executive Branch, have resulted in significant and effective changes in the compliance program.

(U) All parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~**Intelligence Value of the Collection**

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States that may be contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and entirely domestic connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify and assess the network of contacts that a targeted number or address is connected to, whenever there is RAS that the targeted number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata – but always based on links to a number or e-mail address which itself is associated with a counterterrorism target. (Again, communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content) The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen/trap bulk collection programs provide an important capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

December 14, 2009

The Honorable Silvestre Reyes
 Chairman
 Permanent Select Committee on Intelligence
 United States House of Representatives
 HVC-304, The Capitol
 Washington, DC 20515

Dear Chairman Reyes:

~~(TS)~~ Thank you for your letter of September 30, 2009, requesting that the Department of Justice provide a document to the House Permanent Select Committee on Intelligence (HPSCI) that describes the bulk collection program conducted under Section 215 -- the "business records" provision of the Foreign Intelligence Surveillance Act (FISA). We agree that it is important that all Members of Congress have access to information about this program, as well as a similar bulk collection program conducted under the pen register/trap and trace authority of FISA, when considering reauthorization of the expiring USA PATRIOT Act provisions.

~~(TS)~~ The Department has therefore worked with the Intelligence Community to prepare the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States. We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215 and any changes to the FISA pen register/trap and trace authority. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to strict rules.

~~Classified by: Assistant Attorney General, NSD
 Reason: 1.4(c)
 Declassify on: 11 December 2034~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~(TS)~~ Therefore, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) Thank you again for your letter, and we look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,




Ronald Weich
Assistant Attorney General

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~~~(TS//SI//NF)~~ Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- ~~(TS//SI//NF)~~ Provisions of the USA PATRIOT Act affected by reauthorization legislation support two sensitive intelligence collection programs;
- ~~(TS//SI//NF)~~ These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by anyone in the government, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the Foreign Intelligence Surveillance Court ("FISA Court") and Congress;
- ~~(TS//SI//NF)~~ The Executive Branch, including DOJ, ODNI, and NSA, takes any compliance problems in the programs very seriously, and substantial progress has been made in addressing those problems.  and
- ~~(TS//SI//NF)~~ NSA's bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Classified by: Assistant Attorney General, NSD
Reason: 1.4(c)
Declassify on: 11 December 2034~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~**Background**

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the National Security Agency (NSA) intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al-Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."

~~(TS//SI//NF)~~ Today, under Foreign Intelligence Surveillance Court authorization pursuant to the "business records" authority of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorism target overseas. This and similar programs operated pursuant to FISA provide valuable intelligence information.

(U) USA PATRIOT Act reauthorization legislation currently pending in both the House and the Senate would alter, among other things, language in two parts of FISA: Section 215 and the FISA "pen register/trap and trace" (or "pen-trap") authority. Absent legislation, Section 215 will expire on December 31, 2009, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The FISA pen-trap authority does not expire, but the pending legislation in the Senate and House includes amendments of this provision.

~~(TS//SI//NF)~~ The Section 215 and pen-trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant uses of these authorities are to support two critical and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from telecommunications providers [REDACTED]

Although these programs have been briefed to [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on telecommunications companies [REDACTED]

[REDACTED] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen-trap provisions in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail and the time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment. [REDACTED]

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Checks and BalancesFISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen-trap provision. Before obtaining any information from a telecommunication service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed "minimization procedures" required by the FISA Court that govern the retention and dissemination of the information obtained. Before an NSA analyst may query bulk records, they must have reasonable articulable suspicion – referred to as "RAS" – that the number or e-mail address they submit is associated with [REDACTED]

The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. There are also limits on how long the collected data can be retained (5 years in the Section 215 program, and 4½ years in the pen-trap program).

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, to include hearings, briefings, and, with respect to the Intelligence Committees, visits to NSA. In addition, the Intelligence Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ There have been a number of technical compliance problems and human implementation errors in these two bulk collection programs, discovered as a result of Department of Justice reviews and internal NSA oversight. However, neither the Department, NSA nor the FISA Court has found any intentional or bad-faith violations. The problems generally involved the implementation of highly sophisticated technology in a complex and ever-changing communications environment which, in some instances, resulted in the automated tools operating in a manner that was not completely consistent with the specific terms of the Court's orders. In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered "end-to-end" reviews of the Section 215 and pen-trap collection programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection. In early September of 2009, the Director of NSA made a presentation to the FISA Court about the steps taken to address the compliance issues. All

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify the network of contacts that a targeted number or address is connected to, whenever there is RAS that the number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata. (Communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content.) The more metadata NSA has access to, the more likely it is that NSA can identify or discover the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen-trap bulk collection programs provide a vital capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

~~TOP SECRET//COMINT//NOFORN~~