S. HRG. 113–878

CONTINUED OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

OCTOBER 2, 2013

Serial No. J–113–32

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE
28–112 PDF WASHINGTON : 2018

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

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

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

CONTENTS

OCTOBER 2, 2013, 10 A.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

Page

ANSWERS

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

CONTINUED OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

WEDNESDAY, OCTOBER 2, 2013

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Feinstein, Whitehouse, Klobuchar, Franken, Coons, Blumenthal, Hirono, Grassley, Hatch, Sessions, Graham, Lee, Cruz, and Flake.

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

Chairman LEAHY. Good morning, everybody. It is a strange time in the Congress. I would also note before we start that we will not allow any demonstrations during a meeting of the Senate.

I know some demonstrators like to get themselves on television. I do not care whether they are in agreement—or disagreement with positions of mine. I do not want people blocking others who are here, by holding up signs, and I do not want them blocking the people who are here to watch this hearing. This is the United States Senate, and people have the ability to watch a hearing.

We are going to conduct further oversight of the intelligence community's use of the Foreign Intelligence Surveillance Act, or FISA. No one knows for sure how long the Federal Government will be shut down, but I feel strongly that the Senate Judiciary Committee has to continue its work on this important subject because it does involve the security of the United States. I consulted with Senator Grassley about this, and I appreciate that Director Clapper and General Alexander have agreed to proceed with the hearing today as scheduled. I am certain that they join me in thanking all of the dedicated intelligence community professionals who are also doing their jobs today despite the needless shutdown of the Federal Government. That said, I have decided—and, again, I discussed this with Senator Grassley—to postpone the Committee's weekly business meeting tomorrow in light of the Government shutdown. I am doing this even though we have judicial emergencies on the agenda. I am hoping that those of us who, like myself, are on the Appropriations Committee will be able to get back to passing bills. I am concerned that we are now in October. By law, by the end of last month the House of Representatives was supposed to have sent us each of the appropriations bills so that we could then vote on them,

vote up or vote down. They have yet to send over a single one. Maybe instead of looking for slogans we ought to just pass these appropriations bills and vote for them or vote against them, whichever way, but get it done and let people get back to work.

I am also going to ask General Alexander and Director Clapper at the end of their statements if they would take an extra minute and tell us, because it is going to be of interest to many of us on this Committee who are on Appropriations, what the shutdown is meaning in the number of people who are not able to come to work and do the jobs that we expect them to do in our intelligence agencies.

As we continue to reexamine the intelligence community's use of FISA authorities, let us be clear that no one underestimates the threats that our country continues to face or the difficulty of identifying and meeting those threats. We all agree that we should equip the intelligence community with the necessary and appropriate tools to help keep us safe. But—and there is always a "but"—I hope that we can also agree that there have to be limits on the surveillance powers we give to the Government. Just because something is technologically possible and just because something may be deemed technically legal does not mean that it is the right thing to do.

This summer, many Americans learned for the first time that 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. The American public also learned more about the Government's collection of Internet content through the use of Section 702 of FISA.

Since the Committee's last hearing on these revelations in late July, we have learned a great deal more. We have learned that the NSA has engaged in repeated, substantial legal violations in its implementation of both Section 215 and Section 702 of FISA. For example, the NSA collected, without a warrant, the content of tens of thousands of wholly domestic emails of innocent Americans. The NSA violated a FISA Court order by regularly searching the Section 215 phone records database without meeting the standard imposed by the Court.

These repeated violations led to several reprimands by the FISA Court for what the FISA Court called "systemic noncompliance" by the Government. The Court has also admonished the Government for making a series of substantial misrepresentations to the Court. Now, knowing this, we have seen no evidence of intentional abuse of FISA authorities, but the pattern is deeply troubling.

We have also learned that the NSA in 2011 started searching for Americans' communications in its Section 702 database—a database containing the contents of communications acquired without individualized court orders. And this past weekend—and all of you have seen the front page story—The New York Times reported that the NSA is engaging in sophisticated analysis of both domestic and international metadata to determine the social connections of Americans.

So when you have all these revelations, it is no surprise that the intelligence community faces a trust deficit. And after years of raising concerns about the scope of FISA authorities, as I and others

have, and the need for stronger oversight, I am glad that many Members of Congress in both parties are now interested in taking a close look at these programs—at both the Government's legal and policy justifications for them and the adequacy of the existing oversight regimes.

I think it is time for a change, and I think additional transparency and oversight are important parts of that change. But I believe we have to do more. So I am working on a comprehensive legislative solution with Congressman Sensenbrenner, the Chairman of the Crime and Terrorism Subcommittee in the House, as well as other Members of Congress, again, across the full political spectrum of both parties. Our bipartisan, bicameral legislation will address Section 215 and Section 702 and a range of surveillance authorities that raise similar concerns.

Our legislation would end Section 215 bulk collection. It also would ensure that the FISA pen register statute and National Security Letters could not be used to authorize bulk collection. The Government has not made its case that bulk collection of domestic phone records is an effective counterterrorism tool, especially in light of the intrusion on Americans' privacy.

In addition, I find the legal justification for this bulk collection to be strained at best. I have looked at the classified list of cases involving Section 215. I find it to be unconvincing. As the Deputy Director of the NSA himself acknowledged at our last hearing a couple weeks ago, there is no evidence that Section 215 phone records collection helped to thwart dozens or even several terrorist plots.

In addition to stopping bulk collection, our legislation would improve judicial review—and I think this is extremely important—by the FISA Court and enhance public reporting on the use of a range of surveillance activities. It would require Inspector General reviews of the implementation of these authorities—putting into law a request that Senator Grassley and I, along with eight other Members of this Committee, made last week to the Inspector General for the intelligence community. This is a commonsense, bipartisan bill, so I look forward to working on this effort in the coming months with those in the Senate, in the House, and others who care about these issues.

I do appreciate the concrete steps that both Director Clapper and General Alexander have made in recent months to brief Members of Congress—and I have been, as you know, at many of those briefings—and their move toward more transparency and further declassification of documents. I also welcome the participation of the legal and technical experts on our second panel and would note with particular pride that my alma mater, Georgetown Law, is well represented among those witnesses. So I hope this will inform our legislative efforts.

You know, we all agree we have to ensure our Nation's security, but we also have to restore the trust of the American people in our intelligence community, and fundamentally we have to protect the liberties that have kept us great and a diversified democracy and the envy of countries around the world because of our democracy.

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

Senator Grassley, do you want to say something before we go to the witnesses?

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

Senator GRASSLEY. Yes, thank you. And thanks to our witnesses for what they do for the security of our country, and to you, Mr. Chairman, for holding the hearing, a very important oversight hearing, a very important function of Congress to make sure that our laws are faithfully executed. Although the Government has been partially shut down due to partisan differences over various issues, we are continuing our oversight work, as I said, a very important matter, and in this particular instance, because national security is the first responsibility of our Federal Government.

We last held a hearing on this subject late July. At that time I expressed the view that the reports in the media had called into serious question whether the law and other regulations currently in place strike the right balance between protecting our civil liberties and our national security. This is especially so concerning the public revelation that under Section 215 of the PATRIOT Act the Government was collecting Americans' phone records in bulk. Additional public disclosures since our last hearing have underscored that concern.

Indeed, since that time, the administration has declassified legal opinions reflecting significant errors by the Government before the FISA Court in implementing 215 and 702. The good news is that these appear to have been for the most part unintentional mistakes that Government brought to the Court's attention on its own accord. Of course, the bad news is that even with all the checks and balances built into the system, these kinds of errors can still occur.

Even more unsettling, other reports since July have suggested that there have been cases of intentional and willful misuse of intelligence authorities by NSA employees to spy on their spouses and neighbors. These disclosures have created a broader crisis of trust in the legitimacy of our intelligence-gathering methods generally. In my view, had these programs been more transparent from the start, this trust deficit that the American people have would not be as severe as it is now.

This brings me to the President's response to the crisis which has been very baffling to me. The President held a news conference in early August, a news conference that should have been held, and thankfully he did, in which he defended the bulk collection of phone records as "an important tool in our effort to disrupt terrorist plots" and suggested some areas for reform. Since then, as far as I know, he has not said a word in public about these issues. If the President really and truly believes in the importance of these programs, he should be publicly defending them as part of our national debate. He should not be contracting out that job solely to the intelligence community. Simply put, as in so many other areas, the President is failing to lead where he wants others to follow.

In any event, I am pleased that we have taken a number of steps to follow up on some of these disturbing reports. Since July, a bipartisan group of Members of this Committee requested that the Inspector General of the intelligence community conduct a thor-

ough review of the implementation of these authorities. Additionally, I wrote to the NSA Inspector General and received a public accounting of the handful of documented instances where the NSA employees intentionally abused their authorities. It was heartening to see how few cases of intentional misconduct exist, but on the other hand, it is alarming to know that the possibility of employees engaging in such behavior turns out to be very real.

The NSA Inspector General's response to my letter reflected that many of these cases were referred to the Department of Justice for possible criminal prosecution. I was planning on following up with how these referrals were handled with Deputy Attorney General Cole at this hearing. The Chairman chose not to invite an administration witness to provide legal perspective on these matters. Therefore, I will be following up with the Department of Justice about these cases with a letter to the Attorney General today.

The balance between protecting individual liberties and our national security is a delicate one. Reasonable people can disagree about precisely where that balance is best struck. I probably do not agree 100 percent with any member of the two panels of witnesses that we have with us today, including Professor Cordero, whom I have invited to share her valuable perspective as a lawyer with hands-on experience in the intelligence community. But I welcome them all, and I am pleased to hear their views as we consider various reforms to FISA and related surveillance activities.

Something has come to my attention. Just yesterday there were press reports of 70 percent of the intelligence community being furloughed. I am concerned that if lawyers in the intelligence community determine that 70 percent of their employees are non-essential to the mission, which is a national security mission, the number one responsibility of the Federal Government, then the intelligence community either needs better lawyers to make big changes to the workforce or are you overemployed in those areas. I cannot believe that 70 percent of the intelligence community is being furloughed and we are still being able to meet our national security responsibilities. So that concerns me very much, and maybe you folks will touch on that.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you. And, of course, as you know, we had the Deputy Attorney General at our last hearing, and we had the Deputy Attorney General at our closed-door hearing on this, and we will be having the Justice Department testifying again. Because we are limited in time here today, we kept to these two witnesses.

Speaking of limitation of time, while this would be unusual, Senator Lee——

Senator GRASSLEY. Do you not want me to send my letter to the Attorney General?

Chairman LEAHY. Oh, you feel free to send it. You can send anything you want. But we have had him here twice now on this same subject, and I am sure we will be having him again. But, Senator Lee, did you want to make a very short statement?

OPENING STATEMENT OF HON. MICHAEL S. LEE, A U.S. SENATOR FROM THE STATE OF UTAH

Senator LEE. Yes, thank you, Mr. Chairman. I appreciate the Chairman and the Ranking Member allowing me to speak very briefly, as I have to leave for another Committee responsibility.

Congress, of course, plays an important role when it comes to overseeing our Nation's intelligence and surveillance programs. We have to balance various competing interests, and it is difficult. I just wanted to highlight a couple of concerns that I am always looking out for.

Number one is the breadth of metadata collection pursuant to Section 215 of the PATRIOT Act.

Number two, the potential for back-door searches of information on Americans that is collected, you know, some would argue indirectly, pursuant to Section 702 of the FISA Amendments Act.

And, number three, the lack of transparency within the FISA Court system.

I have worked with the Chairman in the past on legislation to address each of these, and I look forward to working with him in the future on these concerns.

Thank you very much.

Chairman LEAHY. Thank you very much.

Our first witness is—incidentally, the most senior Member on our side is the Chair of the Senate Intelligence Committee, which helps us a great deal in this deliberation, and we will also be joined later by Senator Durbin, who is the Chair of Defense Appropriations, which handles much of the budget for this.

Our first witness is James Clapper. He was sworn in as the fourth Director of National Intelligence on August 9, 2010. He served for 32 years in the United States Armed Forces, retired in 1995. He was a lieutenant general in the Air Force. He previously served as Under Secretary of Defense for Intelligence and the head of the Defense Intelligence Agency.

Director, it is good to have you here. Please go ahead.

STATEMENT OF HON. JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE, WASHINGTON, DC

Director CLAPPER. Chairman Leahy, Ranking Member Grassley, and distinguished Members of the Committee, sir, if it is all right with you, I would like to answer your question about the impacts of the Government shutdown and furloughing our civilians.

First, the legal standard against which we make decisions about who is furloughed and who is not is—and this is quoting from the law—"that which is necessary to protect against imminent threat to life or property." And so our applying that standard is what resulted across the board in furloughing roughly 70 percent. I think that will change as this—if this drags on, and we will make adjustments depending on what we see as the "potential imminent threats to life or property," to quote the law.

I will tell you as to impacts, I have been in the intelligence business for about 50 years. I have never seen anything like this. From my view, I think, this on top of the sequestration cuts that we are already taking, that this seriously damages our ability to protect the safety and security of this Nation and its citizens. I would com-

mend to you Senator Feinstein's superb statement yesterday on the floor outlining her concerns, with which I completely agree. This affects our ability—this is not just a Beltway issue. This affects our global capability to support the military, to support diplomacy, and to support our policymakers. And the danger here is, of course, that this will accumulate over time. The damage will be insidious. So each day that goes by, the jeopardy increases.

This is a dreamland for foreign intelligence service to recruit, particularly as our employees already, many of whom are subject to furloughs driven by sequestration, are going to have, I believe, even greater financial challenges. So we are spending our time setting up counseling services for employees to help them manage their finances. So from my standpoint, this is extremely damaging, and it will increase so as this shutdown drags on.

General Alexander, do you want to add anything to that?

General ALEXANDER. I was going to do it at the end.

Director CLAPPER. Go ahead.

General ALEXANDER. From our perspective, I would echo everything that——

Chairman LEAHY. Press the red button.

General ALEXANDER. Technically challenged, Mr. Chairman.

From NSA's perspective, this has impacted us very hard. We have an amazing workforce. When I look at what our folks are capable of doing, we have over 960 Ph.D.s, over 4,000 computer scientists, over 1,000 mathematicians. They are furloughed. Our Nation needs people like this, and the way we treat them is to tell them, "You need to go home because we cannot afford to pay you, we cannot make a deal here."

From my perspective, the impact, what Director Clapper points out is we went to the most specific threats against our Nation. This does not apply to all the threats against our Nation. We cannot cover all of those. So what we are doing is we are taking the most significant counterterrorism and other threats that we see and the support to our military forces in Afghanistan and overseas, that is the priority in what we are doing. That is the way the law has been interpreted, and that is what we are doing. From my perspective, it has had a huge impact on morale.

Director CLAPPER. So, sir, if you would like, we will go into our statements on the subject of the hearing.

We do appreciate your having us today to talk about the way ahead occasioned by the dramatic revelations about intelligence collection programs since their unauthorized disclosure and about the steps we are taking to make these programs more transparent while still protecting our national security interests.

I am joined today, of course, by the Director of the National Security Agency, General Keith Alexander, and following my brief statement, he will have an additional statement.

We think this hearing is a key part of the discussion our Nation needs about legislation that provides the intelligence community with authorities both to collect critical foreign intelligence and to protect privacy and civil liberties. We, all of us in the intelligence community, are very much aware that the recent unauthorized disclosures have raised serious concerns both here in Congress and across the Nation about our intelligence activities. We know that

the public wants both to understand how its intelligence community uses its special tools and authorities and to judge whether we can be trusted to use them appropriately.

We believe we have been lawful and that the rigorous oversight we have operated under has been effective. So we welcome this opportunity to make our case to the public.

As we engage in this discussion, I think it is also important that our citizens know that the unauthorized disclosures of the details of these programs has been extremely damaging. From my vantage as DNI, these disclosures are threatening to our ability to conduct intelligence and to keep our country safe. There is no way to erase or make up for the damage that we know has already been done, and we anticipate even more as we continue our assessment as more revelations occur.

Before these unauthorized disclosures, we were always conservative about discussing the specifics of our collection programs based on the truism that the more adversaries know about what we are doing, the more they can avoid our surveillance.

But the disclosures, for better or for worse, have lowered the threshold for discussing these matters in public. So to the degree that we can discuss them, we will. But this public discussion should be based on an accurate understanding of the intelligence community, who we are, what we do, and how we are overseen.

In the last few months, the manner in which our activities have been characterized has often been incomplete, inaccurate, or misleading, or some combination thereof. I believe that most Americans realize the intelligence community exists to collect the vital intelligence that helps protect our Nation from foreign threats. We focus on uncovering the secret plans and intentions of our foreign adversaries, but what we do not do is spy unlawfully on Americans or, for that matter, spy indiscriminately on the citizens of any country. We only spy for valid foreign intelligence purposes as authorized by law, with multiple layers of oversight to ensure we do not abuse our authorities.

Unfortunately, this reality has sometimes been obscured in the current debate, and for some this has led, as you alluded, to an erosion of trust in the intelligence community. And we do understand the concerns on the part of the public.

I am a Vietnam veteran, and I remember as congressional investigations of the 1970s later disclosed—and I was in the intelligence community then—that some intelligence programs were carried out for domestic political purposes without proper legal oversight or authorization. But having lived through that as a part of the intelligence community, I can now assure the American people the intelligence community today is not like that. We operate within a robust framework of strict rules and rigorous oversight involving all three branches of the Government.

Another useful historical perspective, at least I think, is that during the Cold War, the Free World and the Soviet Bloc had mutually exclusive telecommunications systems which made foreign collection a lot easier to distinguish. Now world telecommunications are unified. Intertwined with hundreds of millions of innocent people conducting billions of innocent transactions are a much smaller number of nefarious adversaries who are trying to do harm

on the very same network using the very same technologies. So our challenge is to distinguish very precisely between these two groups of communicants. If we had an alarm bell that went off whenever one terrorist communicated with another terrorist, our jobs would certainly be a lot easier. But that capability just does not exist in the world of technology today.

Over the past 3 months, I have declassified and publicly released a series of documents related to both Section 215 of the PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, or FISA. We did that to facilitate informed public debate about the important intelligence collection programs that operate under these authorities. We felt that, in light of the unauthorized disclosures, the public interest in these documents far outweighed the potential additional damage to national security. These documents let our citizens see the seriousness, thoroughness, and rigor with which the FISA Court exercises its responsibilities.

They also reflect the intelligence community's, particularly NSA's, commitment to uncovering, reporting, and correcting any compliance matters that occur. However, even in these documents, we have had to redact certain information to protect sensitive sources and methods, such as particular targets of surveillance. But we will continue to declassify more. That is what the American people want. It is what the President has asked us to do. And I personally believe it is the only way we can reassure our citizens that their intelligence community is using its tools and authorities appropriately and legitimately.

The rules and oversight that govern us ensure we do what the American people want us to do, which is to protect our Nation's security and our people's liberties. So I will repeat: We do not spy on anyone except for valid foreign intelligence purposes, and we only work within the law.

On occasion, we have made mistakes, some quite significant. But these are usually caused by human error or technical problems. And whenever we have found such mistakes, we have reported, addressed, and corrected them.

The National Security Agency specifically, as part of the intelligence community broadly, is an honorable institution. The men and women who do this sensitive work are honorable people dedicated to conducting their mission lawfully and are appalled by any wrongdoing. They, too, are citizens of this Nation who care just as much about privacy and constitutional rights as the rest of us. They should be commended for their crucial, important work in protecting the people of this country, which has been made all the more difficult by this torrent of unauthorized damaging disclosures.

That all said, we in the intelligence community stand ready to work in partnership with you to adjust foreign surveillance authorities to further protect our privacy and civil liberties, and I think there are some principles we agree on:

One, we must always protect our sources, methods, targets, partners, and liaison relationship.

Second, we must do a better job in helping the American people understand what we do, why we do it, and, most importantly, the rigorous oversight that helps ensure that we do it correctly.

And, three, we must take every opportunity to demonstrate our commitment to respecting the civil liberties and privacy of every American. But we also have to remain mindful of the potentially negative long-term impact of overcorrecting the authorizations granted to the intelligence community.

As Americans, we face an unending array of threats to our way of life, a more diverse array of threats than I have seen in my 50 years in intelligence. And I believe we need to sustain our ability to detect these threats. We welcome a balanced discussion about national security and civil liberties. It is not an either/or situation. We need to continue to protect both.

Let me turn now to General Alexander.

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

Chairman LEAHY. General Alexander serves the Director of the National Security Agency and the head of U.S. Cyber Command. He has testified before us both in open and closed sessions of this Committee and, of course, continuously in the Intelligence Committee.

General, go ahead.

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

General ALEXANDER. Chairman Leahy, Ranking Member Grassley, distinguished Members of the Committee, thank you for the opportunity to provide opening remarks.

I am privileged today to represent the dedicated professionals at the National Security Agency who employ the authorities provided by Congress, the Federal courts, and the executive branch to help protect the Nation and protect our civil liberties and privacy.

If we are to have an honest debate about how NSA conducts its business, we need to step away from sensationalized headlines and focus on facts.

Our mission is defend the Nation and to protect our civil liberties and privacy. Ben Wittes from the Brookings Institution said about the media leaks and specifically about these two FISA programs: "Shameful as it is that these documents were leaked, they actually should give the public great confidence in both NSA's internal oversight mechanisms and in the executive and judicial oversight mechanisms outside the Agency. They show no evidence of any intentional spying on Americans or abuse of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures on the part of the NSA. And they show an earnest, ongoing dialogue with the FISA Court over the parameters of the Agency's legal authority and a commitment both to keeping the Court informed of activities and to complying with its judgments on their legality."

Today I would like to discuss the facts and specifically address:

Who we are in terms of both our mission and our people;

What we do: adapt to technology and the threat; take direction from political leadership; operate strictly within the law and consistent with explicit intelligence priorities; and ensure compliance

with all constraints imposed by our authorities and internal procedures;

What we have accomplished specifically for our country with the tools we have been authorized; and,

Where do we go from here?

First, who we are, our mission. NSA is a foreign intelligence agency with two missions: We collect foreign intelligence of national security interest, and we protect certain sensitive information and U.S. networks—all this while protecting our civil liberties and privacy.

NSA contributes to the security of our Nation, its Armed Forces, and our allies.

NSA accomplishes this mission, while protecting civil liberties and privacy, because the Constitution we are sworn to protect and defend makes no allowances to trade one for the other.

NSA operates squarely within the authorities granted by the president, Congress, and the courts.

Who we are: our people.

I am proud of what NSA does and more proud of our people.

The National Security Agency employees take an oath to protect and defend the Constitution of the United States.

They have devoted themselves to protecting our Nation.

Just like you, they will never forget the moment terrorists killed 2,996 Americans in New York, Pennsylvania, and the Pentagon.

They witnessed the first responders' efforts to save lives. They saw the military shift to a wartime footing. They committed themselves to ensuring that another 9/11 would never happen and our deployed forces would return home.

In fact, they deploy with our Armed Forces into areas of hostility.

More than 6,000 have deployed in support of operations in Iraq and Afghanistan; 22 have paid the ultimate sacrifice since 9/11—sadly, adding to a list of NSA/CSS personnel numbering over 170 killed in the line of duty since our formation in 1952.

Theirs is a noble cause.

NSA prides itself on its highly skilled workforce: We are the largest employer of mathematicians—1,013; 966 Ph.D.s and 4,374 computer scientists; linguists in more than 120 languages; more patents than any other intelligence community agency and most businesses. They are also Americans, and they take their civil liberties and privacy seriously.

What we do: adapt to technology.

Today's telecommunications system is literally one of the most complex systems ever devised by mankind.

The fact that over 2.5 billion people all connect and communicate across a common infrastructure is a tribute to the ingenuity of mankind. The stark reality is that terrorists, criminals, and adversaries make use of the same infrastructure.

Terrorists and other foreign adversaries hide in the same global network, use the same communications networks as everyone else, and take advantage of familiar services: Gmail, Facebook, Twitter, et cetera. Technology has made it easy for them.

We must develop and apply the best analytic tools to succeed at our mission, finding the communications of adversaries while protecting those of innocent people, regardless of their nationality.

What we do: We take direction from political leadership.

NSA's direction comes from national security needs, as defined by the Nation's senior leaders.

NSA does not decide what topics to collect and analyze.

NSA's collection and analysis is driven by the National Intelligence Priorities Framework and received in formal tasking.

We do understand that electronic surveillance capabilities are powerful tools in the hands of the state. That is why we have extensive mandatory internal training, automated checks, and an extensive regime of both internal and external oversight.

What we do: We use lawful programs and tools to do our mission.

The authorities we have been granted and the capabilities we have developed help keep our Nation safe.

Since 9/11 we have disrupted terrorist attacks at home and abroad using capabilities informed by the lessons of 9/11.

The Business Records FISA program, NSA's implementation of Section 215 of the PATRIOT Act, focuses on defending the homeland by linking the foreign and domestic threats.

Section 702 of FISA focuses on acquiring foreign intelligence, including critical information concerning international terrorist organizations, by targeting non-U.S. persons who are reasonably believed to be located outside the United States.

NSA also operates under other sections of the FISA statute in accordance with the law's provisions.

It is important to remember that in order to target a U.S. person anywhere in the world under the FISA statute, we are required to obtain a court order based on a probable cause showing that the prospective target of the surveillance is a foreign power or agent of a foreign power.

NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order 12333.

As I have said before, these authorities and capabilities are powerful; we take this responsibility seriously.

We ensure compliance.

We stood up a Directorate of Compliance in 2009 and repeatedly train our entire workforce in privacy protections and the proper use of capabilities.

We do make mistakes. The vast majority of the compliance incidents reflect the challenge of implementing very specific rules in the context of ever-changing technology.

Compliance incidents, with very rare exception, are unintentional and reflect the sort of errors that will occur in any complex system of technical activity.

The press claimed evidence of "thousands of privacy violations."

This is false and misleading.

According to NSA's independent Inspector General—and the Vice Chairman brought up the 12 cases, so I will just go through that quickly. There were 12 cases of willful violation. All of those were under Executive Order 12333. None of those were in the Business Records FISA or under FAA 702.

We hold ourselves accountable every day.

Most of these targets involved improper tasking or querying regarding foreign persons in foreign places.

I am not aware of any intentional or willful violations of the FISA statute.

Of the 2,776 incidents noted in the press from one of our leaked annual compliance reports, about 75 percent are not violations of approved procedures at all but, rather, NSA's detection of valid foreign targets that travel to the U.S. and a record that NSA stopped collecting, in accordance with the rules. We called those "roamers," and I mispronounced that in one of the things, and it came out as "rumors," but it is "roamers."

Let me also start to clear the air on actual compliance incidents.

The vast majority of the actual compliance incidents involve foreign locations and foreign activities, as our activities are regulated by specific rules wherever they occur.

For the smaller number that did involve a U.S. person, a typical incident involves a person overseas involved with a foreign organization who is subsequently determined to be a U.S. person. All initial indications and research before collection point the other way, but NSA constantly reevaluates indications.

NSA detects and corrects and, in most cases, does so before any information is ever obtained, used, or shared outside NSA.

Despite the difference, between willful and not, we treat incidents the same: We detect, we address, we remediate, including removing or purging information from our databases in accordance with the rules. And we report.

We hold ourselves accountable and keep others informed so they can do the same.

On NSA's compliance regime, Ben Wittes said, at last Friday's Intelligence Committee hearing: "But one thing we have learned an enormous amount about is the compliance procedures that NSA uses. They are remarkable. They are detailed. They produce data streams that are extremely telling—and, to my mind, deeply reassuring."

We welcome an ongoing discussion about how the public can, going forward, have increased information about NSA's compliance program.

[The prepared statement of General Alexander appears as a submission for the record.]

Chairman LEAHY. Well, then, let us go into that discussion, because both of you have raised concerns that the media reports about the Government surveillance programs have been incomplete, inaccurate, misleading, or some combination of that. But I worry that we are still getting inaccurate and incomplete statements from the administration.

For example, we have heard over and over again the assertion that 54 terrorist plots were thwarted by the use of Section 215 and/or Section 702 authorities. That is plainly wrong. But we still get it in letters to Members of Congress; we get it in statements. These were not all plots and they were not all thwarted. The American people are getting left with the inaccurate impression of the effectiveness of NSA programs.

Would you agree that the 54 cases that keep getting cited by the administration were not all plots and, of the 54, only 13 had some nexus to the U.S.? Would you agree with that—yes or no?

General ALEXANDER. Yes.

Chairman LEAHY. Okay. At our last hearing, Deputy Director Inglis' testimony stated that there is only really one example of a case where but for the use of Section 215 bulk phone records collection, terrorist activity was stopped. Was Mr. Inglis right?

General ALEXANDER. He was right. I believe he said two, Chairman. I may have that wrong, but I think he said two. And I would like to point out that it could only have applied in 13 of the cases because of the 54 terrorist plots or events, only 13 occurred in the U.S. Business Records FISA was only used in 12.

Chairman LEAHY. I understand that. But what I worry about is that some of these statements that all is well and we have these overstatements of what is going on, we are talking about massive, massive, massive collection. We are told we have to do that to protect us. And then statistics are rolled out, and if they are not accurate, it does not help with the credibility here in the Congress, it does not help with the credibility with this Chairman, and it does not help with the credibility with the country.

And both of you feel free to answer this next one. This past weekend—I mentioned The New York Times article. When I read that, I see them reporting that for the past several years the NSA has been analyzing social networks, including those of Americans, using communications metadata as well as location information, tax records, voter registration records, and more.

Like many of us who have access to classified briefings, we sometimes find we get far more in a newspaper—and we get a crossword puzzle, too, but we get more in the newspapers than we do in the classified briefings that you give us. According to the article, it reportedly allowed the NSA to graph the interactions of associates and locations of Americans.

Now, if it is accurate, it appears to contradict earlier representations that the NSA does not compile dossiers or files on the American people.

Is the NSA compiling profiles or dossiers on American people through the use of its intelligence authorities? Gentlemen, either one of you.

Director CLAPPER. Let me comment first on the value of Section 215, where I think, unfortunately—and we may be part guilty of this—the only metric used is plots foiled. I think there is another metric here that is a very important use for Section 215. I would call it the "peace of mind metric."

In the case of the Boston Marathon bomber, we were using these tools and we were able to check out whether there was or was not a subsequent plot involving New York City.

In the case of the AQAP threat this summer that occasioned the closure of several diplomatic facilities in the Mideast.

There were a number of selectors that emerged from our collection overseas that pointed to the United States. Each one of them was checked out and was found not to be relevant to a domestic aspect of a terrorist plot.

Chairman LEAHY. Mr. Clapper, we will certainly give you time to add to that, if you like, but could you go back to my question? Is the NSA compiling profiles or dossiers on the American people through the use of its intelligence authorities?

Director CLAPPER. In every case, for valid foreign intelligence purposes, let me go to General Alexander.

General ALEXANDER. Those reports are inaccurate and wrong.

Chairman LEAHY. So The New York Times is wrong in its article?

General ALEXANDER. Absolutely. Here are the facts. What they have taken is the fact that we do take data to enrich it. What is not in front of those statements is the word "foreign," foreign information to understand what the foreign nexus is of a problem set that we are looking at. How do you know what an individual is, a terrorist, without having any data to enrich it, with just a number? In the foreign space, we need that.

The Supplemental Procedures and Guidelines Governing Communications Metadata Analysis, the SPCMA article that this was about, allows NSA to not just stop when we are tracking a terrorist if we hit a U.S. number, which is what we used to have to do. It allows us to go back and see where that goes and where it comes into or out of the country and what are the problems outside the country——

Chairman LEAHY. Which authority are you using for this analysis? First off, I just want to make sure I understand. You are saying The New York Times is flat-out wrong in their article.

General ALEXANDER. I am saying they are flat-out wrong saying that we are creating dossiers on American——

Chairman LEAHY. Are you going into social networks?

General ALEXANDER. No. Here is what we——

Chairman LEAHY. Okay. What, if anything, is accurate in The New York Times article?

General ALEXANDER. The accuracy is the Secretary of Defense and the Attorney General did approve the Supplemental Procedures Governing Communications Metadata Analysis in 2009. What that allows us to do is use metadata that we have acquired under Executive Order 12333 in chain, whether it is phone records or emails, through U.S. selectors to figure out social networks abroad.

I will tell you that there are cases——

Chairman LEAHY. That 2009 order is still being used?

General ALEXANDER. That is correct. But there are cases—I need to clarify because I want to make sure this is 100 percent accurate. There are cases where the FBI might start a terrorist threat here in the United States. If there is a terrorist threat in the United States and they get a warrant to go after that or a FISA, then we can use SPCMA to go after that. We can use this to look at hostages overseas, U.S. hostages. We can look at this to track industries, because U.S. companies are also considered U.S. persons under this law, that are the targets of terrorist communications.

What we are not doing: We are not creating social networks on our families. We are not doing that. And the insinuation that we are doing that is flat wrong. And I take exception to them taking a classified document that dealt with foreign, not understanding it and saying therefore it must apply to——

Chairman LEAHY. You told The Times this?

General ALEXANDER. Chairman?

Chairman LEAHY. Have you made this complaint or responded to The New York Times on this?

General ALEXANDER. Yes. I think the issue is, you know, here they have all these documents that they are trying to leak out without having the understanding. We did give them insights. They did not take all the data. I do not know what and why. I do not——

Chairman LEAHY. What you are doing, is it being reviewed by the FISA Court?

General ALEXANDER. Not in all cases. Some of these cases that deal with Executive Order 12333 are not reviewed by the FISA Court. Those that would fall under the Business Records 215, 702, –3, and –4 would be. So these would not be reviewed, but they are reviewed by the administration, and they are audited by our people.

Chairman LEAHY. My time is up. You have raised more——

Senator GRASSLEY. I think you ought to take more time. This transparency—because one of the problems we have with this program, there is not enough transparency.

Chairman LEAHY. Thank you. You know, I worry—you say it is Executive authority, not FISA Court authority. Does anybody have oversight other than the executive branch?

General ALEXANDER. Well, Congress, too. And let me——

Chairman LEAHY. Has this been reported to the Congress——

General ALEXANDER. They get all——

Chairman LEAHY [continuing]. Either of the Intelligence Committees?

General ALEXANDER. I believe both of these have, and I would have to go back and check, but both of these have gone to the Committee. I think you have both of these. And, Chairman, you bring out a good point, and for the complete transparency, Chairman, you brought out a good question, and if I could, I think this will help greatly.

The issue that we have here is how do you use metadata, which is the least intrusive, to understand a problem that our Nation could face. That is the Business Records. And so we use that globally, and sometimes it touches the United States.

Chairman LEAHY. Well, metadata, you say the least intrusive. Many might think it is the most intrusive, and I will tell you why. And I realize there is a lot of metadata going on. We shop at the grocery store; you use your grocery store credit card; the ads you are going to get are going to be different if you are buying things for young children or if you are buying a nice bottle of wine. We all understand that.

But do you understand the concern as more and more things come out, when it turns out, for example, the NSA, some members—and I realize not by authority—were checking their love interests through using the tools of NSA. You know, Americans like their privacy. They like their security, but they like their privacy, too. And you understand the concern that we are getting. Simply following the metadata, a lot of people think if they are on social media and whatnot that there is some expectation of privacy, less obviously but some.

General ALEXANDER. So I do agree, Chairman, but I think the differentiation that I make in terms of metadata for these purposes is the phone numbers to-from or the email addressed to-from. And the issue that I think we face in trying to figure out where we take this legislation is how do we do this in such a way that we can ensure the American people know that we are doing it exactly right and protect the Nation?

From my perspective, what we have done is set up two things. We have put this database, with tremendous oversight—this has more oversight than any program in Government—the courts, the administration, and Congress, and our IGs and everyone. And every time we make a mistake, we self-report. Why do we need it? And General Clapper brought out a great point. It is the start. It does not necessarily lead us to the end. It tells us you need to look more here. Oftentimes we give that to the FBI.

Now, yes, the FBI and we need to do better work in keeping the metrics of what resulted from that. But, in addition, it helps us looking overseas to say why is that person important and how do we tell you if this is a real threat or something that we should ignore. This summer, this was huge for us.

Chairman LEAHY. I will come back to some of my skepticism. One other thing. We have tried to make sure that it is kept—an issue like this, I want to try to maintain the bipartisan nature, and I want to thank Senator Grassley because he expressed some of these concerns. And while he would normally go next, the Chair of the Senate Intelligence Committee has to leave for another meeting, so he has yielded to her.

Senator FEINSTEIN. Thank you.

Chairman LEAHY. Chuck, I appreciate that.

Senator FEINSTEIN. Thank you very much. I appreciate that.

Chairman LEAHY. I am stepping out for a phone call, and I will be right back.

Senator FEINSTEIN [presiding]. Thank you, Mr. Chairman.

I want to use my time to say something to my colleagues. I believe maybe only Senator Hatch was on the Intelligence Committee in 2001. In mid-year, the DCI, whose name was George Tenet, came in to meet with us, and what he said was that he predicted that within 3 months there would likely be an attack on this country. He did not know what. He did not know when. He did not know how. As a matter of fact, I went on CNN on July 1, 2001, and said this: "There is a major possibility of a terrorist incident within the next 3 months." That is a direct quote from what I said.

Then something took place which I thought could never take place in this country, and that is 9/11. I never believed there could be training schools for pilots who would teach people how to fly but not to land in this country. I never thought our visa system was so weak that they could admit terrorists to this country. But I was totally wrong.

The event happened, and it was catastrophic—for people, for this Nation, for our standing, but most importantly, because of the death and destruction that it brought about this country.

And then we learned that there were stovepipes and our intelligence was inadequate and we could not collect enough data. And then we learned that there was a man by the name of Khalid al-

Mihdhar, one of the group in San Diego. I believe that if this were to happen again with this program and other programs working in combination, we have an opportunity to pick that up. Absent these kinds of technological programs, we do not have an opportunity to pick that up.

This is a very hard culture to meet with human intelligence. It is a different culture. The language is different. There are many dialects. The groups are tight. It is very difficult to permeate them.

So our great strength today, ladies and gentlemen, in protecting this homeland is to be able to have the kind of technology that is able to piece together data while protecting rights. I listened to this program being described as a surveillance program. It is not. There is no content collected by the NSA. There are bits of data—location, telephone numbers—that can be queried when there is reasonable, articulable suspicion. If it looks like it is something for an individual in this country, it then goes to the FBI for a probable cause warrant, and a full investigation takes place.

I so regret what is happening. I will do everything I can to prevent this program from being canceled out. There is going to be a bill in my Committee to do it. There is a bill in this Committee to do it. And, unfortunately, very few of us sat on that Committee when George Tenet came in in June 2001 and said, "We anticipate a strike, but we do not know what, we do not know where, we do not know when." That can never be allowed to happen in the United States of America again. And that is the basis for this program. It is legal. We are looking at increased transparency. We are looking to make some changes in it. But we are not looking to destroy it. To destroy it is to make this Nation more vulnerable.

I just wanted to say that. I had to say it. Thank you. Senator.

Senator GRASSLEY. Go ahead with your questions.

Senator FEINSTEIN. Pardon me?

Senator GRASSLEY. Do you have any questions?

Senator FEINSTEIN. I do not have any questions. Thank you.

Senator GRASSLEY. Let me make clear something I said to the Chairman to keep asking his questions, because we need more transparency. I do not know exactly how much transparency we ought to have. You folks know that. I do not know your business. Your number one responsibility is protecting our national security. But whatever that balance is between security and transparency, we ought to have it, because I firmly believe that a lot of these issues that Senator Feinstein wants to protect would not be coming up if more had been told about it over the last few years. I do not think the impact of Mr. Snowden would have—well, I do not want to comment on that. But, anyway, I think that in our system, transparency brings accountability.

I am going to start out where I left off, and it is not an accusation against the intelligence community if the information is accurate. I am going to ask a question, but before you want to answer it, I want to tell you why I am cynical about these statements about what sequestration and what the shutdown will do that you made and other people have made, and that comes yesterday with the closing down of the World War II Monument. We had World War II veterans coming in on honor flights, and they had barricades around something that I will bet 24/7/365 I could walk into

that any time. And so the show of putting barriers around because of a shutdown and spending all the money to do it and then to have every other department talk about shutdowns causes me to be a little cynical.

Now, I am not putting your work in the same category as the Park Service. Do not read me wrong. But if, in fact, 70 percent of the intelligence community is now furloughed, if that is true, is that an honest assessment that these employees are non-essential? I am concerned that if your lawyers have determined that 70 percent of your employees are non-essential to your mission, then you either need better lawyers or you need to make big changes to your workforce.

Can you tell me whether those reports are accurate or not?

Director CLAPPER. Well, first of all, sir, we do not consider any of our employees non-essential. But for purposes of this law, the criterion is "necessary to protect against imminent threat to life or property," so that causes us to make some very, very painful choices about who we keep on and who we except.

I would comment on your commentary about the monument closures, and that precisely illustrates the challenge we have in intelligence on conveying the impacts of these cuts, because obviously people see the impact of closing public parks.

In the case of intelligence, it is insidious. So capabilities that we degrade today or give up, we may not see the impact of those for weeks or months or for an extended period. Much harder to rationalize. But I do not want any doubt about the necessity—the importance of all of our employees.

And as I said earlier, as each day goes by, the impact and the jeopardy to the safety and security of this country will increase.

Senator GRASSLEY. General Alexander, my first question. FISA Court opinions show that there were significant problems implementing 215 phone records that were discovered in 2009, showing that the NSA was inadvertently assessing the phone record metadata without required reasonable and articulable connection to terrorism. Those problems were apparently not resolved with the Court until late that year.

Since then, I understand that every query of the metadata is audited by the Department of Justice, and any compliance issues must be reported immediately to the FISA Court.

My first question: Precisely when did the Department begin auditing every query of the metadata? Since then, has the Department determined on any occasion that the reasonable and articulable suspicion standard was not followed?

General ALEXANDER. So I know of—first I will answer the second first and walk backward. I know of no cases where we have not followed the reasonable, articulable suspicion standard, and it has always been auditable since the inception of the program. But the issue you bring out, if I could just take 1 minute on that, because we did make a mistake.

The way we do analysis on the foreign intelligence that we collect was to set up what we called an "alert list," and that alert list would run against the data that comes in and tell us if there was something on a terrorist that—these alert lists were terrorist numbers that we were tracking. What we had not done is reasonable,

articulable suspicion on all terrorist numbers. What we were using it for is to say there is a lot of activity on this number, you ought to go do reasonable, articulable suspicion so you can look into the data.

It was a discrepancy between our technical folks who set it up and our legal folks. And we did it wrong, and we misrepresented it to the Court several times in subsequent procedures of renewals.

That drove us to set up a Directorate of Compliance that would actually look at the technical side and the legal side and make sure we cross-walked this 100 percent. And I think that has been successful, and that is something that we worked with both the Intel Committees and the White House.

Senator GRASSLEY. Second to you, how does the NSA handle instances when a phone number may have been connected to a terrorist group in the past, but NSA knows it is no longer associated with that group? Is there a mechanism so that a query of the metadata can be done that is limited only against the records for certain time periods?

General ALEXANDER. I am not sure I understand this all the way, but let me see if I have got it right. The answer is if a number changes from Person A to Person B over the life of it, how do we adapt to that? That is a difficult technical issue and one that our analysts have to look at, because what you would actually get is two sets of called people. Senator Sessions has one set of people he talks to. You have a different set. What you would see is those sets come together in different times. And the answer is, yes, our analysts can actually delete the second part and say those are of no interest, I am only looking at this first part, because part of the Business Records FISA does have a date-time group, a duration of call, and the to-and-from number.

Senator GRASSLEY. I would like to follow up with Mr. Clapper on my first question. Does America remain safe even with the shutdown?

Director CLAPPER. I have to qualify that, sir. I do not feel that I can make such a guarantee to the American people, and it would be much more difficult to make such a guarantee as each day of the shutdown goes by. I am very concerned about the jeopardy of the country because of this.

Senator GRASSLEY. Can I have one more question?

Chairman LEAHY. Of course. I just want to make sure I—what you are saying is, it becomes cumulative? You are saying the danger and threat become cumulative?

Director CLAPPER. Yes, sir.

Chairman LEAHY. Thank you.

Senator GRASSLEY. General Alexander, I hope you are familiar with the Inspector General's letter to me in which he provides certain details about 12 documented instances of NSA employees intentionally or willfully abusing their surveillance authority. The details in it are alarming to me, so I have a follow-up question.

I noticed that almost all of these cases involved NSA employees stationed abroad. Does that suggest to you that the mechanism to catch this kind of conduct at your domestic facilities are somewhat insufficient? And what else could account for the disparity?

General ALEXANDER. So it is much more difficult to track a foreign number and understand when somebody is doing something on a foreign number that is inappropriate. Those can oftentimes be misleading statements by the analyst saying, "I am looking at this for A," and actually it is a girlfriend.

In the United States, it is different. Against a U.S. number or against an email address, those are flagged, and the system automatically sees that you are doing something against a U.S. person and the auditing procedures come in right away.

Against a foreign number overseas, you do not get those flags, but it is an extremely important point to note that even on a foreign person, if we make a mistake, we hold our people accountable. There is no call for that. It is supposed to be against a foreign intelligence purpose, and you saw the outcome of those 12 cases, what happened in each one in that letter that the Inspector General sent to you.

Senator GRASSLEY. One follow-up: One of the pieces of information I asked the Inspector General for was the law or legal authority that the employee violated. As I read the response, none of these 12 cases involved either the phone records collection program under 215 or the collection program under 702. Is that correct?

General ALEXANDER. That is correct, Senator. And if I could, also it is important to note this was over a decade. This went from 2003 forward. And, you know, when you look at the number of casualties we had in Iraq, seven of those people, as you know, were NSA, of those 12. When you look at it, you are 3 times more likely to die defending our country in Iraq or Afghanistan than committing a willful and knowing violation against a foreign or U.S. person.

Senator GRASSLEY. My last question on this is for Mr. Clapper. If you cannot tell us that America is safe, why then do you not simply use your authority to furlough fewer employees?

Director CLAPPER. Sir, we are going to look at that. In fact, we are going to do it every day to see where we need to—what is the right talent set or analytic expertise that we need. We are doing that as we speak. So I anticipate, if this thing drags out, that we will make adjustments and probably recall more people, particularly in NSA's case, since they have a heavy military population which are not furloughed. So early on, NSA has kept—has excepted a very low percentage of its civilian employees. I am confident—I am sure that over time that condition cannot continue.

Chairman LEAHY. Unfortunately—one, I happen to agree with you, Director, what you say. Unfortunately, we have a law passed in the 1800s that is creating a real problem on the furloughing. It was passed at a time when nobody could have anticipated either the size of the Government or the complexity of Government, but it is tying your hands.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman. Welcome, gentlemen.

We have identified terrorist threats to our country overseas. Correct?

General ALEXANDER. Correct.

Senator WHITEHOUSE. And we track their electronic communications. Correct?

General ALEXANDER. Correct, Senator.

Senator WHITEHOUSE. Is it important to know who they may be in touch with within the United States, those terrorist threats that are overseas?

General ALEXANDER. Yes, it is.

Senator WHITEHOUSE. And they might be using intermediaries or cutouts between the principal that they are trying to reach and themselves. Correct?

General ALEXANDER. That is correct.

Senator WHITEHOUSE. That would be Tradecraft 101. Correct? So records of call and email connections are necessary to allow you to look for those networks. Correct?

General ALEXANDER. That is correct.

Senator WHITEHOUSE. Now, in the call and email connections are information that has for decades been declared by courts and demonstrated by law enforcement practice throughout this country to be not within the warrant requirement of the Fourth Amendment to the United States Constitution. Correct?

Director CLAPPER. Correct.

Senator WHITEHOUSE. So the program is legal, but it risks abuse.

Director CLAPPER. You are right.

Senator WHITEHOUSE. You concede to that. Could you describe—and if you want to fill this out with a request for the record, an answer for the record—the various oversight mechanisms and bodies whose job it is to assure that this program is kept within bounds that protect the privacy needs of American citizens?

Director CLAPPER. Well, yes, sir. First, as General Alexander described——

Senator WHITEHOUSE. How many committees of Congress, for instance, have oversight over the metadata program?

Director CLAPPER. Well, certainly the two intelligence committees do, and I think this Committee as well.

Senator WHITEHOUSE. And here we are, so here is another one, and presumably House Judiciary Committee and subcommittees as well——

Director CLAPPER. Right, four.

Senator WHITEHOUSE [continuing]. That are relevant, presumably. Correct?

Director CLAPPER. Yes, sir.

Senator WHITEHOUSE. The Subcommittee on Crime and Terrorism would have jurisdiction?

Director CLAPPER. Could.

Senator WHITEHOUSE. How many Inspectors General have——

Director CLAPPER. Well, the NSA Inspector General certainly; my Inspector General, who was Senate confirmed, does. So starting with the level of NSA itself, with the Director of Compliance that was set up in 2009 and, additionally, before shutdown, 300 compliance officers whose exclusive duty is to oversee the legal and technical aspects of this. That in turn is overseen by my office and the Attorney General as well as, of course, the FISA Court, which oversees these processes, as well, of course, as——

Senator WHITEHOUSE. Civil Liberties Advisory Boards?

Director CLAPPER. I am sorry?

Senator WHITEHOUSE. Do you have Civil Liberties Advisory Boards?

Director CLAPPER. I do. There is a Civil Liberties and Privacy Board, although I need to mention that is only for counterterrorism purposes. I have by law also a Privacy and Civil Liberties officer whose full-time job is to serve as the conscience for the entire IC on——

Senator WHITEHOUSE. If I could ask you just to fill—there is a lot, and if you could—I will make these questions for the record, if you could get that back, because I do not think there has been a clear and simple exposition of what all the different oversight mechanisms are, and I would like to get that for the record.

I am concerned that in the wake of the Snowden incident—let me put it this way: It is not clear to me that any legal redress is being considered or sought against either Dell or Booz Allen Hamilton, the employers of Snowden at the time that he committed his unauthorized release of classified information. I do not have the information before me to make a detailed analysis of whether the basic doctrine of respondeat superior would apply, which makes the employer liable if the agent acted within the course and scope of his employment or whether this would be an ultra vires act of some kind. But my concern is that there—I am not aware of even any conversation about that. And as we have seen from classified programs in the past, there is a danger that the private contractors managing the program begin to wag the dog and that we become so dependent on our private contractors that we cannot seek legal redress for their misdeeds because, frankly, they are now the ones who we depend on to the extent that we cannot use the authorities that are pertinent to us as customers.

General ALEXANDER. Senator, when this incident broke, I flew out to Hawaii with some of our folks and talked to the people that were involved, including the contracting officer representatives, past and present, and what we had done and working with our folks on this.

I will tell you that one of the contracting officer representatives did exactly what you would expect her to do. When asked to get access to some of this, she denied it to Snowden formally. He worked around that, those procedures. But I think you can see that those things—so we have asked our folks to look at this. We do have that question from you, and I would like to take that for the record, if I could, to get you the answer.

Senator WHITEHOUSE. Good. I just want to make sure that they are not too big to sue.

General ALEXANDER. Right.

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

Chairman LEAHY. Thank you, Senator Whitehouse. You have asked the question I want to emphasize. I am very interested in that answer, too.

Senator Hatch is gone. Senator Sessions. Sorry. One of the problems of a broken rib, it is harder to turn around and check on you, but, Senator Sessions, go ahead.

Senator SESSIONS. Thank you. This is an important hearing, and I thank you all. I would just note that the House has repeatedly

passed funding, Director Clapper, to restore the Defense Department and not allow the sequester cuts to occur. And I hope you have not forgotten the way to 1600 Pennsylvania Avenue. I believe the Commander-in-Chief has a responsibility here, too, and the law, the Budget Control Act, of which sequester was a part, required us to maintain a certain level. Whole agencies and departments have gotten zero cuts and Defense has gotten too much, in my opinion. The House has tried to reconcile that, and I hope somehow we can soon alleviate some of the stress on the Defense Department and the intelligence community.

So, number one, I visited NSA, General Alexander, and I was so impressed with the leadership there and the people I met, and I have said that publicly. So I was deeply disappointed—hurt, really—to hear that somebody had looked at their girlfriend's messages and that kind of thing. Are you saying that all of that was abroad first?

General ALEXANDER. Senator, nine of those were abroad, three were CONUS but involved persons abroad on two of those, and one was on a spouse or girlfriend——

Senator SESSIONS. Well, there is a great temptation there. I trust that you stepped up your emphasis and your determination not to allow that to happen. Even though it is not a large number, it is still unacceptable.

General ALEXANDER. Absolutely. And I will tell you that what Senator Grassley brought out in the letter that we sent to him, we are also putting out to our workforce so that more people understand what has happened to those people, because when you read that——

Senator SESSIONS. They have all been disciplined?

General ALEXANDER. All but one, and in that case, the case was insufficient. I do not have the disciplinary actions in that one, but all either retired, resigned, received Article 15s, or letters of reprimand with additional consequences.

Senator SESSIONS. Well, I think Senator Whitehouse—and he is a former United States Attorney, Federal prosecutor—clarifying something, and, General Alexander, let me just ask you again: So when you are looking at the metadata, you are referring to numbers, phone numbers, email addresses perhaps. No messaging are in this data. Is that right? No substance of a communication?

General ALEXANDER. That is correct. And, Senator, in the metadata program, it is only phone numbers. There are no email addresses in it.

Senator SESSIONS. Now, Senator Whitehouse in his time as United States Attorney probably issued subpoenas, thousands, maybe ten thousand. In my 12 years as United States Attorney, no telling how many thousand subpoenas we have issued——

Senator WHITEHOUSE. Rhode Island is more law-abiding than that, Senator Sessions.

[Laughter.]

Senator WHITEHOUSE. It was just in the hundreds.

Senator SESSIONS. We had plenty of crooks in my district, I can assure you.

[Laughter.]

Senator SESSIONS. The point of which is, it does not require a search warrant to obtain from the telephone company the person's call records. That is done by simple subpoena without—it is simply—and the test is: Is it relevant to the investigation? So if somebody is thought to be a member of a gang and he says he does not know Bad Guy 1 and you subpoena his records and he has got 50 phone calls and 20 of them were within an hour of the crime occurring, then that is hugely valuable, and that is just done all the time.

So we need to understand that the fundamental process here is well within, it seems to me, the traditions of our ability to subpoena—the records are in the possession of the phone company. They are the phone company's records. They are not your personal records. And that is the difference in it.

Senator Feinstein's story was so fabulous, Mr. Clapper. It just laid the whole structure out for us. I know you have said this before, but could you tell us, did these leaks negatively impact your ability to be as effective as otherwise if they had not happened, and did it hurt our ability to identify an attack in the future?

Director CLAPPER. To my mind, there is absolutely no question about that. We are already seeing signs of changes in target behavior because of their awareness as a result of the revelations in these unauthorized leaks. It has done great damage to partners overseas and our relationships with them. People's lives are at risk here because of data that Mr. Snowden purloined. So the damage, the full extent of it is yet to be measured.

Senator SESSIONS. Well, I thank you for your work, and my impression from the people I have met at NSA is that they are dedicated, wonderful Americans who are working every day to preserve and defend this country, unlike Mr. Snowden, who damaged this country. And, fundamentally I think that we can do a better job of monitoring it, and the American people, I am glad to say, are alert. They are not going to tolerate abuses, and they should not. And the press has a right to do their job within the realm of law. But I hope that—it is unthinkable that we would dismantle this program, and I would certainly oppose that.

Thank you, Mr. Chairman.

Chairman LEAHY. It appears a lot of it is being dismantled by the Government shutdown, but that is just my view.

Senator Klobuchar.

Senator KLOBUCHAR. Well, thank you, Director and General.

Chairman LEAHY. And I would note that in about 15 minutes I am going to be slipping out, not because—I am telling you in advance so you will not think it is because of anything you said. Senator Blumenthal is going to take over the chair.

Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Director and General. I want to go back to some of your earlier comments about the effect of the shutdown on the intelligence community. I think it is very important as we sit here today. I note that in your testimony you talked about how 966 Ph.D.s, 4,374 computer scientists, really 72 percent of the civilian workforce in the intelligence community are not going to be able to do their jobs right now, and that includes people who are connecting and collecting signals, engineers

who put the systems back together, people who are on the ground across the world.

You indicated that the law requires you to furlough employees not involved in addressing an imminent threat. Is that right, Director Clapper?

Director CLAPPER. That is correct: against an imminent threat to life or property.

Senator KLOBUCHAR. But is it not true that a threat that is not considered imminent today could be imminent tomorrow?

Director CLAPPER. Exactly. That is why we have to manage this on a day-to-day basis as best we can.

Senator KLOBUCHAR. So you would have to figure out if a threat is imminent and spend time doing that with your lawyers and then add someone back in?

Director CLAPPER. That is exactly right, and we will have to shuffle people in and out depending on what we believe the concern of the day is.

Senator KLOBUCHAR. But you clearly see it as a risk to security?

Director CLAPPER. Absolutely.

Senator KLOBUCHAR. And in your assessment, how much risk are we exposed to because we have had to furlough our intelligence professionals who are covering issues that you cannot define right now as "imminent"?

Director CLAPPER. Well, I do not know if you want mathematical quantification, but certainly on a percentage of our civilian professionals, you know, the risk is, you know, 75 percent more than it was yesterday, I guess.

Senator KLOBUCHAR. Thank you very much. I think that is pretty significant. I appreciated Senator Feinstein's comments she made on the floor about this, and I know she cannot give out all the information, nor can you. But I think people have to understand that this is a significant layoff that we are dealing with right now, temporary as it may be. These threats, as I have learned, change from day to day, and you need people on the ground to be able to respond to them. So thank you for that.

I wanted to go back. I thought our July 31st hearing was good and informative on the surveillance programs, and then right after that, I was a little surprised—and I know the Chairman mentioned some of this, but in mid-August the media began reporting about an internal audit from May 2012 which found that the NSA violated privacy rules over 2,000 times. We have gotten into some of those facts and what that really means, and I am just concerned about why that did not come out during the hearing.

General ALEXANDER. So, Senator, every quarter, internal to NSA, we put together compliance reports that track both under the Business Records FISA, 702, 703, –4, and our Executive order. We compile that because we hold our people accountable to it.

Included in there are incidents. These are not privacy violations. These are incidents. And then we pass those up to the Department of Justice, to DNI, so that everybody knows that everything that we see has been tracked. It is important to note that the majority of those, roughly 75 percent, of those incidents are not privacy violations. Those are us tracking——

Senator KLOBUCHAR. No, I understand that. My point is more of a process one, that we have a hearing and then we find out a week later that these audits were out there that we did not learn about at the hearing.

General ALEXANDER. Yes, so I think what we were going over, we have a number of incidents that we track on 702 and 215. That is what we are talking about here. Most of these incidents that are in these reports reflect us typing in a wrong number, doing a search on Individual A overseas. So these are what we will call minor violations. The major ones were the ones that we brought up, which were——

Senator KLOBUCHAR. Okay. I actually do understand——

Director CLAPPER. I think the answer to your question, Senator, is that the subject matter of the hearing was 215 and 702, and these 12 violations over 10 years occurred under—the foreign collection under the auspices of Executive Order 12333.

Senator KLOBUCHAR. All right. It is just that I thought we were kind of broadly asking questions, and it would have been nice to have heard about it there, but that is behind us now, and I want to talk about some of the reforms that have been suggested. You know, there is legislation out there. One of the reforms that President Obama has supported is the idea that we would have a privacy watchdog installed at the NSA, and an intelligence community website would be created to disseminate public information on the activities. What is the status of these reforms?

General ALEXANDER. So on the first one, we do have a hiring action out on the street. It is probably stopped right now because of the furlough, but we do have one for our civil liberties privacy advocate for NSA.

Director CLAPPER. And we have activated a web page under my office to put out this data.

Senator KLOBUCHAR. Okay. And you suggested a court-appointed amicus for cases that involve novel and significant questions of law. I am just interested in how this would work in practice. What is an example of a novel and significant case?

Director CLAPPER. Obviously, we are getting a little out of our compartment here and more into the Department of Justice, but some form of an advocate or amicus who would be a participant when called upon by the court to address issues of law or major surveillance questions. But I think we would need to defer to the Department of Justice on exactly the mechanics of how the administration would recommend that work.

Senator KLOBUCHAR. Okay. Thank you. And did you want to add anything, General?

General ALEXANDER. I agree with what he said. I learned what an amicus was during these briefings, so it has got to——

Senator KLOBUCHAR. Okay. Well, I will have some follow-up questions on the record, but I did want to again emphasize that it is really important that people understand that 72 percent of the civilian workforce of the intelligence agencies is now on furlough and the effect that that could have on our national security and the reason that we have to end this shutdown.

Thank you.

Chairman LEAHY. Senator Graham.

Senator GRAHAM. Thank you both for your service. From my point of view, I am sure every organization makes mistakes, and if anybody has abused these programs to spy on their spouse or to spy on their neighbor or to do something in that fashion, I hope they go to jail, because I think most of the people in the NSA would like that outcome, because that is not exactly what you are there to do. Do you agree with that, General Alexander?

General ALEXANDER. Senator, I agree that they should be punished, and depending on the action, how harsh——

Senator GRAHAM. Yes, I mean, whatever the appropriate punishment is, but they are outliers.

General ALEXANDER. That is right, Senator. In fact, two of them were done under Field Grade Article 15s.

Senator GRAHAM. Right.

General ALEXANDER. And when you actually look at what they did, you can see that, okay, we trained them, they immediately did something wrong, they got no return. Oh, by the way, they just asked the question. They did not get information back. But they did something wrong, and they were held accountable.

Senator GRAHAM. Good. The point is that when you do things wrong, you should be held accountable. When you do things right, you should be appreciated. I think both of you are trying to do things right to protect our Nation, and I appreciate everybody that works for you, because I know many of them, and they are patriots as much as anybody who criticizes the program.

All right. Did you tell the President of the United States what you just told us, that because of the Government shutdown, our Nation is less secure?

Director CLAPPER. Yes, I did.

Senator GRAHAM. What did he say?

Director CLAPPER. We discussed it yesterday.

Senator GRAHAM. Well, you just scared the hell out of all of us—at least I am scared, when you are telling me that 70 percent of the NSA is unable to go to work, not because they are necessary but because of the statute, the way it is worded. Both of you made very clear presentations to this Committee that the Government shutdown in a post-9/11 world is making this Nation less safe. Is that right, General Alexander?

General ALEXANDER. That is correct, Senator.

Senator GRAHAM. Is that right, Mr. Clapper?

Director CLAPPER. Absolutely. Yes, sir.

Senator GRAHAM. Well, to Mr. Gibbs, who told the President—his political adviser, former press secretary, he advised the President to just watch the shutdown. Do you think that is a responsible thing for the President to do as Commander-in-Chief, to not negotiate or just watch the shutdown?

Director CLAPPER. Well, I am not going to—I would like to avoid the——

Senator GRAHAM. Well, you do not have to. I will give you my own opinion. I think it is irresponsible for all of us to let it continue, but where the hell is the Commander-in-Chief? If you really told him that, that our Nation is less safe and every day that goes by we are being less capable of detecting potential terrorist attacks against the homeland and the approach is to just watch time go by,

why are the Members of the House and the Senate not in the White House right now to try to solve this problem?

One of two things is true: You are telling us the truth, and the Federal Government leadership on both sides are ignoring it, particularly the Commander-in-Chief; or, you are overstating the case. I think you are telling us the truth, so I am not even going to go down the road you are overstating the case. But I want the American people to know there are shutdowns before 9/11 and there are shutdowns after 9/11, and there is a huge difference. And for the President of the United States, for our House Democrats to not negotiate, is irresponsible. For our Republican Party not to try to find a way to end this mess is irresponsible. So I hope that the President will do more than watch.

Now, about 9/11, General Alexander, if we had had the technology and the programs in place today before 9/11, what would be the likelihood that we would have detected that attack?

General ALEXANDER. Senator, in my professional opinion, it would have been very high.

Senator GRAHAM. Do you agree with that?

Director CLAPPER. I do.

Senator GRAHAM. I am here to tell the American people, if we had in place today before 9/11, the 19 hijackers who were here in the country, most of them in legal status, talking to people abroad, we would have known what they were up to. We would have known why the guy was just taking flying lessons to take the plane off and did not care about the part of the flying lessons to land it, which was kind of odd to me—I want to pay for flying lessons, but I do not care to learn to land the plane.

So at the end of the day, my question to both of you is simple. Let us reform this program where it has gotten out of line. Let us be sensitive to the political—to the constitutional rights we all have. But here is my question: What is being proposed in terms of reform, will it make us less able to detect the next 9/11? Are we going back to that pre-9/11 mentality? That is the question for me. Is the Congress taking us back to a time when we could not pick up a threat that was right in front of us?

Director CLAPPER. Well, Senator, there are several proposals that have been proposed in the form of bills, and I guess our basic reaction to this is we are open to changes to make this more transparent, for more oversight, but in doing so we do not want to overcorrect such that we lose the operational utility and the agility of these programs.

Senator GRAHAM. Same for you, General Alexander. Will you tell me when you think we have crossed that line?

General ALEXANDER. Senator, absolutely. I feel it is my responsibility to tell you and the Director of National Intelligence and the President that they are going to hurt us.

Senator GRAHAM. Very quickly. About the times in which we live, are there active efforts by terrorist organizations to penetrate the United States?

General ALEXANDER. Yes.

Director CLAPPER. Absolutely, yes, sir; as we speak.

Senator GRAHAM. Do you believe there are people probably already here as part of a fifth column movement?

Director CLAPPER. There are sleeper—there is sleeper presence, absolutely. I would not call it a unified fifth column. There are various entities——

Senator GRAHAM. Fair enough, and I will end with this thought. My goal is to make sure that if a known terrorist, al-Zawahiri, who took bin Laden's place, if he is calling someone in the United States, I want to know who he is talking to. Is that a fair thing for me to want for my country?

Director CLAPPER. Yes, sir, and I think it is a fair requirement for any citizen.

Senator GRAHAM. And is it also fair to say that before you can keep the content or do something with the content, you have to get a warrant?

Director CLAPPER. Yes.

Senator GRAHAM. Last thought. Are we at war as a Nation with radical Islam, or are we fighting a crime? And what is the difference when it comes to gathering intelligence between fighting a war and fighting a criminal enterprise?

Director CLAPPER. Well, one difference—and it is more of a tradecraft difference—is the evidentiary standard that we struggle with since we are dealing with wispy hints, bits and pieces of information that probably do not necessarily meet the probable cause standard. That is another consideration we have with changes to these laws.

General ALEXANDER. Senator, I do believe it is a war on terrorism, my words, and that what we are seeing today is going to get worse with what we are seeing go through the Middle East, what is going on in Syria, the actions in Iraq over the last week, and in Afghanistan. The week concluding 23 September, 972 people were killed in Kenya, Yemen, Syria, Iraq, Afghanistan, and Pakistan, and over 1,000 injured. When you look at what we—the relative safety we have here, it is no accident. It is the work of our military and our intelligence community keeping this country safe, and we need the tools to do that.

Senator BLUMENTHAL [presiding]. Thank you, Senator Graham.

Senator KLOBUCHAR. Mr. Chairman, I just wanted, in response to Senator Graham, to let him know that a few minutes ago the White House just announced that the congressional leaders had accepted their invitation to come and meet today. So they must have heard you from here, but also, again, if we would pass the Senate bill, the House would pass the Senate bill, then the shutdown would end. I think that is important for people to know.

Senator BLUMENTHAL. Thank you, Senator Klobuchar.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Director Clapper, General Alexander, you and your employees protect our country, and I am grateful for that. Thank you.

I have a bill, the Surveillance Transparency Act, that will address what I think is the central problem in this debate, and that is the fact that, despite the large amount of Americans' information that is being collected under the foreign intelligence law, those laws lack any substantial public reporting requirements. The Government does not have to give even a rough estimate of how many Americans' information is being collected, and it does not have to

tell Americans how much of their information is actually seen by national security officials.

What's more, the companies that get information requests are under strict orders, strict gag orders, so they are not allowed to give the public information.

The American people are smart. They understand that we need to give weight to both national security and civil liberties. But when the public lacks even the most basic information about the scope of these programs, they have no way of knowing if we are getting that balance right.

My bill would change this. It would make the Government give annual statistics on the number of Americans' information collected and the number whose information is actually reviewed. It would also let companies disclose agreements and disclose aggregate statistics on the number of requests they get and the number of accounts affected.

I am very pleased to report that yesterday morning America's leading tech companies from Apple to Google to Microsoft to Facebook to Twitter to Yahoo, all of these companies sent a letter supporting my bill, urging this Committee and Congress to pass it. And, without objection, Mr. Chairman, I will enter a copy of this into the record.

Senator BLUMENTHAL. Without objection.

[The letter appears as a submission for the record.]

Senator FRANKEN. For my first question, I just want to give an example of why I think greater transparency is so desperately needed. As Senator Grassley and Senator Leahy indicated, this past Saturday, The New York Times ran a story alleging that NSA gathers data on the social connections of U.S. citizens. The article gave a series of examples of the kind of sensitive data that is allegedly collected to create detailed graphs of some Americans' social connections. Both of you have clarified some of the inaccuracies in that story.

But here is the thing. If Americans knew that this kind of collection was limited to a small number of people, people who we have reason to believe are foreign agents or involved in terrorism, I frankly think that most of them would be fine with that. But there is nothing in that article that gives any sense of whether this affects tens or hundreds or thousands or millions of people, and that is because the information just is not out there. This lack of information, frankly, scares people and causes distrust. It makes them distrust our Government.

Director Clapper, General Alexander, don't you think that this just underscores the need for greater transparency about our surveillance programs?

Director CLAPPER. Absolutely, sir, it does, Senator Franken, and just a couple comments about the bill.

We were already, I think, in agreement on releasing the total number of orders or other process issued under various national security authorities, including FISA, and the total number of targets affected by those orders. And we are fine with allowing the providers to release annually the total number of Government requests or orders they receive for information about their customers

and the total number of targets affected by those orders and certifications.

What we are concerned about, just to be up front here, is the stipulation on a company-by-company basis, because then that gives the adversaries, the terrorists, the prerogative of shopping around for providers that are not covered.

I do agree with you about doing all we can to assure the public of what a small proportion of these records are actually looked at. A case in point with 215, while the metadata stood at rest in essentially a lockbox, there were, I think, only 288 queries that were actually made, which is actually in the total scheme of things a minuscule part of the records.

Senator FRANKEN. That is sort of the point. I will let you answer the question, General, but I just want to respond to that. Those are good, positive steps that you are talking about. But I have to be honest. I think it is just too little and it is not permanent. You know, first of all, the numbers of orders will not tell us all that much.

For example, in 2012, there were only 212 orders issued under Section 215 of the PATRIOT Act. That seems like a small number, but now it has been declassified that a small number of those orders allowed the Government to collect substantially all of the telephone metadata handled by most of the country's leading telephone companies. What is more, these disclosures do not reveal even an estimate of how many Americans had their information collected, which you just mentioned. So I do not understand why we cannot mention that as part of the law. And what you are doing is sort of voluntary, and it is not permanent. So if you would change policy and we get another administration in that wants to change the policy, then that does nothing.

General ALEXANDER. Could I add to this? On the 288, the 288 numbers were approved for reasonable, articulable suspicion to then do queries on.

Senator FRANKEN. Okay. So queries are the higher number.

General ALEXANDER. You might do it twice in a week, so that would actually be—but only 288 numbers. I think that is a key point.

I agree with transparency and with what Director Clapper has put out. There are two parts of this. He mentioned the first part. The second is those companies that are compelled, especially under 702, are compelled to cooperate with the Government. They are not throwing NSA any information. They are not doing something inappropriate. And it is interesting to note that other countries demand the same of them.

And so what our companies are doing is what our Nation needs them to do to help us stop terrorists and other acts. They are compelled in other countries in a lawful intercept way just the same. And so I think out of this, one of the things that concerns me is those companies who have acted on good faith—and you mentioned several of them—they are trying to do the right thing that we as a Nation have asked them to do, and it is being blown way out of proportion as if they have opened up their servers and stuff, and you now know that is not true.

So I do think the transparency is very important because it tells you the numbers, and I think people would stop and say, "Well, that is it?" And I think—so we have just got to figure out how to do that in such a way as to not tip the bad guys off to go to Point A or B. Does that make sense?

Senator FRANKEN. Yes. Mr. Chairman, could I—I know others have gone over their time. We do not get these two witnesses before us very often. Can I just ask one last quick question?

Senator BLUMENTHAL. I know if I denied you that opportunity, I would hear about it forever, so I am going to say yes.

Senator FRANKEN. I am not sure what that says about me, or you, but——

[Laughter.]

Senator BLUMENTHAL. I just thought I would be your straight man, as usual.

Senator FRANKEN. Yes, thank you.

I think one of the issues—there is trust and distrust, et cetera, that issue. One of the issues is the ability to—we see Snowden, a contractor, and he releases all this stuff. Has there been any thought given to doing—and where are we on thinking about this—two key or three key situations where, you know, I know that on some of the stuff that has been leaked that there is—and I have been briefed that we have used backups where someone does something, other people are alerted to it. Is there any change that we are making, we are talking about making in the way that stuff is accessed?

General ALEXANDER. We are making significant changes, and we can send you the complete report, because some of it gets into a classified area, but we have implemented the two-person control on devices into certain rooms and stuff, and we are piloting part of that for the intelligence community, but I will let the Director——

Director CLAPPER. Well, there are two things underway, sir, that we have to—which are not going to be fixed by close of business next Friday. One is to go to a system of continuous evaluation for people who are cleared as opposed to the current system where someone is given an initial clearance and then they go 5 years or more for a top secret clearance or 10 years for a secret clearance. That system has got to change so we can do this continuously.

Moreover, we have to finish what was started in the aftermath of WikiLeaks for insider threat detection. So we have more comprehensive means of detecting anomalous electronic behavior of people on the job. I can give you a lot more detail on that if you would like for the record.

Senator FRANKEN. Thank you. And thank you, Mr. Chairman.

Senator BLUMENTHAL. Thank you, Senator Franken.

Senator Flake.

Senator FLAKE. Thank you, Mr. Chairman. Thank you both.

Let me follow a little bit on the lines of Senator Graham's comments. I was not here for your initial testimony, but I understand and I read from the press reports, Director Clapper, that you talked about the furloughs and about the shutdown and the negative impact that is having on the intelligence services, and I certainly get that.

As you are aware, 2 days ago we passed through legislation quickly, very quickly, unanimously, to protect the military from this shutdown. Have you recommended to the President that he recommend to the Congress that we do something similar for the intelligence services? If this is, as you have put it, a "dreamland" for our enemy here, would that not be appropriate?

Director CLAPPER. I certainly think it would be, and, of course, the support to the military, particularly in the case of DOD, involves three combat support agencies, one of which is NSA, who, although funded in the National Intelligence Program, are providing support to the military day in and day out. So I would be a strong supporter of that.

Senator FLAKE. Right. I understand there is some overlap. But where there is not, and you are mentioning 70 percent of civilian employees in the intelligence agencies have been furloughed. Is that correct?

Director CLAPPER. That is as of yesterday. Now, as I also hasten to point out, we are going to manage that on a day-by-day basis.

Senator FLAKE. Right.

Director CLAPPER. Right now, for example, NSA has a very low number of excepted civilians, depending on their military population, which, of course, was not furloughed. To the extent that this shutdown drags on, we are going to have to make some daily adjustments and make judgments about bringing people back on a day-to-day basis.

Senator FLAKE. Well, I would hope, if the situation is as dire—and only you know. We do not have access day to day to the intelligence here. But if it is as you say—and I believe that it probably is—then I would believe it would warrant the President saying, okay, whatever you do, however long this is going to last, we have got to make sure that we are collecting the necessary intelligence. I can guarantee you both the House and the Senate would move expeditiously to do this, so if it really is a problem—and I believe it is—I trust that you will make that recommendation to the President.

Director CLAPPER. Yes, sir, I will. And, again, I would—I am not sure you were here, but I would again commend the statement that Senator Feinstein made on the floor yesterday about this.

Senator FLAKE. Thank you.

General Alexander, last June I questioned the FBI Director with regard to the retention of data collected under—the metadata under 215. He testified that data collected under 215 is scrubbed every 5 years, or after 5 years, I think on a rolling basis. Is all metadata collected under other authorities also discarded after 5 years?

General ALEXANDER. So for NSA, it depends on the type of data. So in the metadata repository for 215, as you stated, it is aged off after 5 years by court direction. If there is a report, that, of course, would not be aged off. That report will stand just like other intelligence activities.

Within the Executive Order 12333 metadata repositories, it depends on the size of the repository and the type of data that is being done, but generally speaking, it is 5 years. There may be pieces of information that we retain longer than are of intelligence

value overseas that are different than the ones we have in the United States. But that is all that NSA has in those areas.

Senator FLAKE. I understand that foreign is handled differently. But if you have metadata that is collected under separate authorities, not just 215, is that bunched together in a way that it is retained beyond 5 years? Or how do you separate it? Do you hold it separately? How does that work?

General ALEXANDER. So NSA—I do not know of any other programs that would collect metadata in the United States outside of 215. We do not have any that I know of, and none have come up. So from my perspective, those would be with other agencies—yes, and the overseas is the one I explained. Does that make sense?

Senator FLAKE. Okay.

General ALEXANDER. So I do not have any other. Telephone, there was an old program that we talked about, you know, that was stopped a few years back, and all that data was destroyed. That was on email. So we do not have any——

Senator FLAKE. I trust when you say that there are no programs that I know of that you would know of them.

General ALEXANDER. Hopefully so, especially after the last 3½ months.

Senator FLAKE. Thank you, Mr. Chairman.

Senator BLUMENTHAL. Thank you, Senator Flake.

Senator Coons.

Senator COONS. Thank you, Mr. Chairman, and thank you, General Alexander and Director Clapper, for your testimony and for your service. I do think that the way for us to proceed is not to have—sort of carve out simple exceptions for different pieces of the National Government that we all consider vital to our security, but to end the shutdown, which Speaker Boehner can do at any moment by simply taking to the floor what has been passed by the Senate and allowing an open vote on it. But I will take seriously into account your expressed concerns. It does seem to me alarming if more than 70 percent of your civilian workforce is furloughed, and it is my hope that you will be reviewing on a rolling basis whether or not this is exposing us in any significant way. Your comments at the outset were a reminder.

I, as you may know, also chair the Africa Subcommittee and recently spoke to our Ambassador in Kenya about the ongoing investigation and things we need to learn and be more attentive to that comes out of that tragically significant event in Nairobi.

I do think that the work of the intelligence community is valuable, but as many of my colleagues have spoken about, events over the last few months have raised real concerns across the country, and I appreciate your stated interest in finding a better balance between transparency, civil liberties, a commitment to privacy, and yet fulfilling your duties.

So let me, if I might, turn to that because there are a number of pieces of legislation introduced, being considered by Members of this Committee, that I think can make some positive contribution to resolving the legitimate anxiety many Americans feel about whether their privacy is being appropriately taken into account.

General Alexander, you have argued both here and in other contexts in support of bulk collection that, in order to find the needle

in the haystack, you have to have the haystack. But the very fact the NSA can tell so much about a target through detailed analysis of non-content bulk data, metadata, indicates to me that there is at least some privacy interest at stake—maybe not a constitutional privacy interest given current constitutional doctrine, but a privacy interest in the sense that the NSA can cobble together through these random threads, can weave a profile of a person that can ultimately contain quite private details.

Shouldn't Congress be concerned about protecting that sort of privacy interest against unwarranted intrusion, or you? And what do you suggest we should do about this together?

General ALEXANDER. Well, I think given the standard and the way it has been written, this is a lower standard than probable cause. Now, I am not a lawyer, so I would defer to Justice. But what we are talking about is in each case, when we go to query the Business Records FISA, we start out with a selector: Is it associated with al Qaeda or associated terrorist groups? So that is the nexus of our question. And it is really what you would want us to do, and it is the least intrusive.

What we are doing is, we will look at that, create one, two, and potentially three hops out, and see if there are other nexus and numbers of interest. We know no names on the U.S. side. It is just numbers. If we see that, and other connections to foreign from some of those numbers, we would then tip that to the FBI. The FBI would then go through the appropriate process, and in this case they would have to come up with a probable cause standard to go after the content there.

That was a long-winded answer to say—and I apologize for that—I believe the appropriate standard is there, and the courts agree with it. And I think Judge Eagan's statements were really pretty good in this area. They were excellent. We try to do that by ensuring that every time we look at it, you and others can audit, see what we did. You know, we audit it, we document it, and it is from my perspective very precise in what we do. Then and only then do we look into the data.

So what that means from my perspective is the chances of my number being looked at are so many zeroes out that I am comfortable. My data, I am sure, is in there.

Does that make sense?

Senator COONS. That is a helpful answer.

Director Clapper, I would be interested then, given the answer just given by General Alexander, if you can articulate for the American people why the Government ought not to be required to show that the information, such as bulk data, that it seeks under our surveillance authorities pertains to an agent of a foreign power, his activities, or persons with whom he is in contact, rather than this mere relevance standard?

Director CLAPPER. Well, as we mentioned earlier—and, again, we are getting into the lawyer area here, but——

Senator COONS. This is the Judiciary Committee. We have a tendency——

Director CLAPPER. I understand. I think the difference here is in the evidentiary threshold or evidentiary standard for a probable cause versus what we deal with in intelligence. And all we are

looking for here are investigatory leads which may not necessarily meet the probable cause standard. Ergo, we have relied on this reasonable, articulable suspicion as the basis for that.

Now, one of the proposals that has been made is to have greater court scrutiny of these RAS determinations. I think we would be fine with doing that after the fact on a regular periodic basis so that any of these queries made under a reasonable, articulable suspicion standard as opposed to probable cause, which is higher, we would be fine with.

Senator COONS. Well, what we are going to pursue is sort of reasonable suspicion of what, and so one of the ways that I think we can deal with this yawning gap of sort of trust and confidence by the American people about their privacy and your charge to defend our security is by narrowing in on exactly what is the standard under which these searches are being conducted. And I also will simply repeat what I think was Senator Franken's solid point, that you have made some very significant progress in terms of transparency and commitment to response to congressional oversight, but temporary changes in policy and practice do not provide lasting assurance. Changes in statute will.

Director CLAPPER. I completely agree with that, that if these changes, whatever they are, are embedded in law, that will instantiate a degree of permanence that our doing it administratively would not.

Senator COONS. Thank you.

Thank you, Mr. Chairman.

Senator BLUMENTHAL. Thank you, Senator Coons.

Senator Cruz.

Senator CRUZ. Thank you, Mr. Chairman.

Director Clapper, General Alexander, I thank you for being here. I thank you for your service to our Nation.

I would like to address two topics: one, the issue of the impact of the Government shutdown on the intelligence community, and then I would like to follow up with some specific questions about the many privacy concerns that have been raised.

With respect to the shutdown, I think the testimony that the two of you have provided today is deeply disturbing. That 70 percent of the civilian intelligence force has been furloughed is reason for concern to everyone, and I very much agree with Senator Lindsey Graham who observed that the person who should be most out front correcting this is our Commander-in-Chief. And I do not believe President Obama should be playing politics with this. He should not be refusing to negotiate or compromise. He should be stepping forward to correct this problem right now.

As Senator Flake noticed, this week we saw what Congress can do when there is a bipartisan cooperation to address a need, namely, earlier this week the United States unanimously—the United States Senate unanimously passed legislation that the House had already passed to fund the men and women of our military. It was the right thing to do. I took to the Senate floor to commend Majority Leader Harry Reid for not objecting to that legislation, for agreeing not to hold the men and women of our military hostage regardless of what happens in this Government shutdown.

Director Clapper has presented a recommendation here to this Committee today that the intelligence community needs to be funded, and I have heard the concerns raised by my friend Senator Klobuchar, my friend Senator Coons. I hope we can see bipartisan cooperation today, Republicans and Democrats in the Senate agree to come together today to pass a clean continuing resolution funding the Department of Defense and our intelligence communities. If the Senate cooperates, we could get this passed by the end of the day. We could respond to the national security threat these two gentlemen have laid out. And the only impediment to doing so is the prospect that Majority Leader Harry Reid would object to doing so.

If, God forbid, we see an attack on the United States because the intelligence community was not adequately funded, every Member of this Committee would be horrified. So I hope that issues of partisan politics can be set aside and we can all come together and pass right now by the end of the day a continuing resolution to fully fund the Department of Defense and the intelligence community. I hope President Obama, I hope Majority Leader Harry Reid hear and respond to the candid and heartfelt recommendation, Director Clapper, that you presented here today.

Let me move on to the second topic: the issue of privacy. General Alexander, in a recent Senate Intelligence Committee hearing, when asked about whether the agency wants "the phone records of all Americans," you testified, "I believe it is in the Nation's best interest to put all the phone records into a lockbox that we can search when the Nation needs to do it."

Besides phone records, what other records of all American citizens do you believe the Federal Government should be collecting?

General ALEXANDER. I cannot think of any right now. There has been—so thanks, Senator, for that question, because earlier this came up about the Saturday article. We do not collect in bulk all those things that were said. Those were focused on foreign, but they did not have foreign vote or foreign X in front of it.

From my perspective, I cannot think of other bulk records that we would need, like phone. I do think as we look at the phone data, we are going to have to look at how that changes as we bring mobility, and that has been the question of it, and so we released to the Intelligence Committees today clarification so they understood the difference on locational data and those requirements.

I do think that right now we are going to have to evolve as the threat evolves, but I cannot think of any, and that was a long-winded—I cannot think of any. I apologize.

Senator CRUZ. Also before the Intelligence Committee, General Alexander, you declined to answer whether the NSA had ever tried to gather data about the location of phone calls, and there was some suggestion from Senator Wyden that this was a classified matter.

My question to you is: In your personal opinion, do you believe the NSA needs to collect GPS location information on American citizens to prevent terrorism?

General ALEXANDER. So we did send a statement to the Intelligence Committees, and if I could just read it real quick, because it addresses what your question is:

"As NSA has previously reported to the Senate and House Intelligence Oversight Committees, NSA does not collect locational information under Section 215 of the PATRIOT Act. In 2010 and 2011, NSA received samples in order to test the ability of its systems to handle the data format, but that data was not used for any other purposes and was never available for intelligence analysis purposes. In a 25 June 2013 closed hearing with the Senate Select Committee on Intelligence, NSA promised to notify the Congress before any locational data was collected. Moreover, as noted in the Foreign Intelligence Surveillance Court's most recent opinion"—I think it is called Footnote 5—"on the program, the Government would also be required to seek the Court's approval of the production of locational data before acquiring it under this program."

I would just say that this may be something that is a future requirement for the country, but it is not right now, because when we identify a number, we can give that to the FBI. When they get their probable cause, then they can get the locational data that they need. And that is the reason we stopped in 2011.

Senator CRUZ. Thank you, General Alexander.

If I may ask one brief follow-up question?

Senator BLUMENTHAL. Sure.

Senator CRUZ. Thank you, Mr. Chairman.

Absent a search warrant particularized to an individual suspected terrorist, does the NSA currently have the ability and access to voicemail content, to text messages, or to financial records that are now being collected by the CFPB on millions of American citizens?

General ALEXANDER. I apologize. I am not familiar, Senator, with CFPB.

Senator CRUZ. The Consumer Financial Protection Bureau.

General ALEXANDER. Not that I know of, Senator, no. In fact, to be clear, if we have to go after any U.S. person—and it would almost always be an FBI not an NSA lead—it has to have a probable cause warrant, and you would have to go through the probable cause, whether it is under a regular court or the FISA Court, depending on the type of action.

Senator CRUZ. And is that answer the same for voicemail content and text messages?

General ALEXANDER. Voicemail—all content, any targeting of a U.S. person would have to be done that way. For metadata, it is always started with a nexus with al Qaeda or related—the queries and reasonable, articulable suspicion.

Senator CRUZ. Thank you, General Alexander. Thank you, Director Clapper.

Senator BLUMENTHAL. Thank you, Senator Cruz.

Before I ask my questions, I am going to recognize Senator Hirono.

Senator HIRONO. Thank you very much, Mr. Chairman.

I understand the serious concerns and consequences to our intelligence program with 70 percent plus of your people furloughed as a result of the shutdown. I would say that every day of the shutdown creates dire consequences for our families and our economy. So, of course, the answer to that is not to have had a shutdown in

the first place, and we need to open Government, all of Government.

We talked a bit in today's hearing about some individuals who had asked inappropriate or illegal queries, and, General Alexander, you mentioned what happened to these people. My question is: How did these inappropriate queries come to light in the first place? Do you have something in place that detects when these kinds of illegal actions are taken by your employees?

General ALEXANDER. Two ways, Senator, for us to detect those. If it is on a U.S. person phone number or email, a flag automatically goes up and says somebody is querying that. In the audit process, that makes it very quick to see.

Under the foreign side, if you have somebody working overseas on a foreign number, it is much more difficult. Oftentimes that is found when we have a security update, when we go through the person's security update, because detecting a foreign number—so most of these were on a foreign friend, girl or boy friend, in a foreign place. And the number may be construed to a valid intelligence target or identified as such, and it is difficult for an auditor to see that. So that is the issue. So what we have done is, I think, highlighting the punishments that go along with this really will help cut that down.

Now, to be really candid, if you think about the number of people that we have—and you are familiar with this, I know, from NSA Hawaii and others—when you look at the numbers of people doing queries and the few mistakes that we have had over a decade, that is 12. That is too many. We agree. But I think actually we do a good job of holding these—of detecting and holding people accountable.

Senator HIRONO. So you feel that we have the processes, the technology in place that will identify these kinds of inappropriate queries? I mean, nothing is foolproof.

General ALEXANDER. That is right. Nothing is foolproof. I think on the U.S. persons, we have a great track record there. And in some of these, that is how it was detected, in the minority of the cases where it involved that. The more difficult one I explained.

Senator HIRONO. I want to turn to The New York Times recent article where you have many systems in place that collect metadata. There is reference to MAINWAY. In the article it says that, in 2011, MAINWAY was taking in 700 million phone records per day, and it also began to receive, in 2011, 1.1 billion cell phone records daily, and then it goes on to say that the agency is pouring money and manpower into creating a metadata repository capable of taking in 20 billion record events daily and making them available to NSA analysts within 60 minutes. So, clearly, the surveillance technology is evolving.

My question is: Do we also have a developing—are we also developing the technology to protect privacy?

General ALEXANDER. Senator, I think we are, and I would note that what was missing in The New York Times article is almost all of those should have said "foreign" in front of it. So here is the issue that we face, and it goes right to metadata, and it is for our allies as well as for us.

A terrorist threat that spans from the Middle East to Europe to the United States, how do you track that and identify the key people. You could try to do this on content, but that would be too labor-intensive. So metadata tracking the connections is the first and the best way to start. And so the collection of metadata to track some of these individuals is the most important and the least intrusive way of doing it.

In the United States, what was conflated was a couple of different programs. So the fact that Facebook and social networks and all those things, they jumped to the conclusion that that is done on Americans, that is factually incorrect. Only when the Americans are a subject of an investigation, like a terrorist investigation—so in this case it is called "a U.S. person"—a terrorist in the United States is treated as a U.S. person. In that case, we would have the FBI have a court order—the FBI would have done that. Then we could go do the check on that.

So I would just be clear that I think our rules for ensuring the privacy both of Americans and our allies is actually better than any country in the world.

Senator HIRONO. I have one more question, Mr. Chairman. General Alexander, is PRISM the only intelligence program NSA runs under FISA Section 702?

General ALEXANDER. Well, PRISM was a—yes, essentially the only program was that that you know as PRISM under 702, which operates under that authority from the Court. But we also have programs under 703, 704, and 705.

Senator HIRONO. So what are all of the programs run by NSA or other Federal agencies under FISA 702 or of the PATRIOT Act Section 215?

General ALEXANDER. So, generally speaking—and I am going to give you the general statements on this. So you have two sets: the Business Records FISA program, 215, authorizes the use of metadata; Section 702 allows us with one and foreign to go after content, so 702 is content data, which means the communications of a foreign person, reasonably believed to be foreign, outside the United States to get their communications. So it is a different set of things, but we may use U.S. infrastructure to help us gather that information. 703, –4, and –5 deal specifically with U.S. persons and are a much smaller subset.

Did I get those right? I have got to ask the lawyer.

So that is, generally speaking—and then there is upstream collection that allows us to collect the same information. We go through the Court; we do the same thing on that. That was one of the violations that we had in 2011. We worked that through with the Court. But it is essentially the same process, going after a foreign piece of information.

So how do you track a terrorist? And these are the tools that you have. One is to identify in metadata who it is. And the second, if we identify it is a foreign target, a foreign terrorist piece of information, gathering more information on that becomes increasingly more important. All of those are available to this Committee, all of the information on those, and our Executive Order 12333, and none of that is hit.

Senator HIRONO. Thank you.

Mr. Chairman, I think my time is up. I may be submitting further questions to our witnesses. Thank you.

Senator BLUMENTHAL. Thank you, Senator Hirono.

Thank you both for being here, and thank you for your service to our Nation and to the men and women who work under your command. I think all of us share the view that the work that these dedicated patriots do for our Nation is absolutely vital. I think also I at least share the sense of alarm and astonishment not only about the percentage that you have given, 70-plus percent of our intelligence community being furloughed, but also the very dire and dangerous impact on the capability of the Nation to protect itself during this time of shutdown. And you were asked, I believe, Director Clapper, whether you recommended to the President a change in that percentage or in the policy and practice. Have you made a recommendation?

Director CLAPPER. I have not made directly a recommendation to the President, no.

Senator BLUMENTHAL. I understand your view that that policy should be changed and that more of our intelligence community should be at work during this shutdown. But would it not be advisable to make that recommendation?

Director CLAPPER. It would. Also——

Senator BLUMENTHAL. I hope you will do it.

Director CLAPPER. In fairness, though, I need to—I am here, we are here representing, perhaps parochially, intelligence. But the shutdown has a very negative impact on lots of other segments of the national security apparatus, to include the Department of Defense. I am worried, most concerned about the intelligence components of the Department of Defense, for example, but there are many other parts of the Department which also have an impact on national security who are also civilians who work in those——

Senator BLUMENTHAL. I understand that point, but in your parochial task—and I would respectfully disagree with the use of the word "parochial." I think it is a very profoundly significant task. I would respectfully suggest that you make that recommendation.

Let me move on to say to you both, we know and you know that we need to both protect national security and preserve our civil liberties, and that is the balance that a democracy requires to be made. And protecting our security enables us to have the freedoms and liberties that we also want to protect in the course of collecting that data.

One of the suggestions that I have made, in order to protect the trust and confidence of our Nation in our national security system, is that there be an adversarial process. As you know, we have talked about it before, and you have responded to Senator Klobuchar's question about what she referred to as an "advocate" or an "amicus."

My proposal very simply would provide for a constitutional advocate that would enable the Court to hear both sides, and the principle behind it is really one of common sense. Before you authorize a mission or assignment, you do not have a formal trial, but you hear both the upsides and the downsides, the negatives and the positives, and my feeling is that the Nation would be better protected by a constitutional advocate with security clearance that

would potentially raise questions and challenge a security practice or procedure after it is ongoing, so there would be no delay.

Let me pose to both of you, do you see a disadvantage, assuming that there would be no delay and no threat to security during that challenge, from that kind of adversarial procedure?

Director CLAPPER. Let me start, sir. First, I have read your Harvard Law School treatise, which, speaking personally, I thought was excellent. I thought it was very well written, very temperate, and very balanced.

Senator BLUMENTHAL. Thank you.

Director CLAPPER. And it does recognize the two poles.

I think our general view on an advocate or your other set of recommendations pertaining to the composition of the Court and how it is appointed, the diversity, our—again, I hate to use the word "parochial," but from our standpoint, as long as the Court can function operationally for us, that is the main concern we have, that it can move with agility, protect those aspects that require classification, as the Court has. I think our view is the Court has been a rigorous overseer, a very robust overseer of all these processes. But for the sake of enhanced transparency and trust and confidence of the American people, some arrangement like this I think from our standpoint is more than acceptable.

Having said that, I think the official spokesperson for this would be the Department of Justice.

Senator BLUMENTHAL. General Alexander.

General ALEXANDER. I agree with everything Director Clapper said, and I would just add that there are certain cases, I think, that you have also noted that would not require an amicus or somebody to stand up and say in these—just like you would have in a subpoena, there are times that you go to a judge and do things that you do not have an adversary in the criminal side. I think you would model it perhaps after that, and your discussions with the Justice Department I think have already walked down that lane. So given all that, yes.

Senator BLUMENTHAL. And the model would be indeed the criminal process modified so as not to impede in any way the legitimate and pressing security concerns that might arise.

I want to say for myself as to the potential legal action against contractors who failed in their duties to prevent the leaks that occurred or to do more adequately the screening and security clearance that was required that my hope is that legal redress will be pursued. My colleague Senator Whitehouse said he wanted to make sure that they were not too big to sue. I want to make sure that they are too big not to sue, too big in their responsibilities and the very profound harm to the Nation that has been caused by their failure to fulfill those responsibilities. They are very big in terms of the role and responsibility that they were legally required to fulfill and apparently failed to fulfill. And so I hope there is serious consideration underway and that you will recommend as appropriate that legal action is taken.

Let me just finally ask you a couple of questions to clarify, General Alexander, what you said about The New York Times report, specifically the social network graphing that The Times reported.

Is it your testimony here that there has been no social network mapping or graphing that involves American residents or citizens?

General ALEXANDER. I gave the cases in which that would not be true. For example, there are cases that you would graph an American number if that is the subject of a terrorist investigation, is a great example, if they are the target or if they are a hostage someplace, when you would expect us to look into those communications for those types of things. So there are cases where you would do that. But it does not——

Senator BLUMENTHAL. You would—I apologize for interrupting. You would map the phone numbers.

General ALEXANDER. The phone numbers, correct.

Senator BLUMENTHAL. I am talking about the social network emails and Facebook and other connections or information that——

General ALEXANDER. So our information is foreign, and all the information that we bring in, foreign, that even has U.S. data in it, we do the maximum that we can to filter out any U.S. data. So we would not have that in our repository.

So the belief—what they jump to is a conclusion because we did not articulate perhaps in a classified slide that what we are talking about here is all foreign stuff. Everybody knows that who works there. But what they jump is, well, then, that must be on U.S. persons. That part is wrong. We do not do that. And the fact that people assume that we are out there mapping the social networks of U.S. persons is absolutely wrong.

What we do go after is those that are the subject of a terrorist investigation or something like that. And even then we do not have all that data in there. We do not have the Facebook and other stuff on those people here in the U.S. It would have to come from the foreign side or from an FAA 702 collection.

Senator BLUMENTHAL. If they became a target and only if they became a target would you do any of the social network——

General ALEXANDER. Then it would be the FBI. Then it would go over to the FBI. You know, so we are looking for the foreign nexus here, not the U.S. part.

Senator BLUMENTHAL. Well, let me ask you, The Times reports that in November 2010, SIGINT Management Directive 424 authorized the adoption of a practice that had been tried on a pilot basis for about a year and a half before. Is that inaccurate?

General ALEXANDER. I am not sure, Senator, what that refers to on 424, to be honest. Is this the Supplemental Procedures Governing Communications Metadata Analysis? I am not sure what that means. But I will take that for the record.

Senator BLUMENTHAL. If you could take it for the record, I would appreciate your response.

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

General ALEXANDER. And just to be clear, you know, I am answering questions on Business Records FISA 215 from NSA's perspective because that is what I am familiar with. You know, that is, of course, a global thing that others use as well. But for ours, it is just that way.

Senator BLUMENTHAL. And you would agree with me, would you not, that this practice, to the extent it requires authorization from

FISA—and apparently this program did—would and should be reviewed by the FISA Court?

General ALEXANDER. I think all things that are authorized by the FISA Court should be—is reviewed by them. You mean the actual queries themselves?

Senator BLUMENTHAL. Well, the claim of social network mapping that went beyond perhaps the targeting of foreigners.

General ALEXANDER. It did not happen. So that is the part that I take exception to. If there is anything that goes on there, it is done under the 702, and that would be targeting a foreign into the U.S.

So I do think—you know, this might be, Senator, a great opportunity for you to come out and actually see some of this. I think it would be very helpful in helping to shape the laws that are so important to the future of this country, because I think when you see it and you can sit down with the people and they go through what we do and how this was conflated on one slide, that all these documents that are foreign, like voter registration, well, we all vote here, but it is not U.S., it was foreign, to understand who the number that goes to this person and what they are all about to help us understand is this a threat or not.

Senator BLUMENTHAL. And the only point I would make—and I would be happy to accept your invitation and your recommendation—is that a constitutional advocate could bring this claim to the attention of the Court. It could be reviewed factually and legally so that the American people would not have to rely on a Senator, whether it is Richard Blumenthal or any other Senator, or an official in charge, as you are, but could be assured that there was some independent objective review after an adversarial process that tested it. And just as one last point, when I say "tested it," we are dealing here with a construct, a constitutional construct, that relies on a 1979 case, *Smith v. Maryland*, involving a pen register system, which I think you would agree is the Stone Age of surveillance, and technology has moved so rapidly and so profoundly, there may be some need for the Supreme Court to interpret and advise as to how these constitutional principles apply to modern technology.

General ALEXANDER. Senator, if I could also add, you know, the Supplemental Procedures Governing Communications Metadata Analysis, what I would like to do is—because that article is so long and there are so many things interwoven, I would like to take that for the record and give you back a detailed set of responses so every point—because, you know, what I do not want you to believe is I made this assertion here on what we do with respect to FAA 702, and that gets conflated to Business Records or something else. So, for clarity, we will take that for the record, if that is okay, and give you both an unclassified version so you can share that more widely with whomever you would like, and then a classified version that shows you why some of those technical details are absolutely incorrect.

Senator BLUMENTHAL. Not only is it okay and acceptable, but actually you read my mind because I was going to suggest that an analysis of the article, because it raises very important and impressive questions as to what the practices were and what the constitu-

tional implications are, really would be very useful for this Committee, and I will ask that the Chairman make it part of the record, if you would submit it. Thank you.

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

Senator BLUMENTHAL. Thank you to both of you for being here today. Thank you again for your service and for your very helpful testimony. With that, we will go to the next panel.

[Pause.]

Senator BLUMENTHAL. As is the practice of this Committee, first of all, I welcome you here and, second, I have the duty to administer the oath so that you can be sworn. If you would please stand and raise your right hand? Do you affirm that the testimony that you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Professor DONOHUE. Yes.

Professor FELTEN. Yes.

Professor CORDERO. Yes.

Senator BLUMENTHAL. Thank you. I am going to give very abbreviated introductions in the interest of time because we are running a bit late, but I will ask that the full summary of your résumé be submitted for the record.

Senator BLUMENTHAL. First of all, Laura Donohue is a professor of law at Georgetown Law School and the director of Georgetown's Center on National Security and the Law. She writes on national security and counterterrorist law in the United States and the United Kingdom, and I understand that your most recent book is entitled "The Cost of Counterterrorism: Power, Politics, and Liberty," and that you are currently at work also on an article or a book on the NSA's metadata collection program as well as drones and the War Powers Resolution.

Professor Felten is a professor of computer science and public affairs at Princeton University and the founding director of Princeton Center for Information Technology Policy. I understand that you were the first chief technologist at the United States Federal Trade Commission and that you are a member of various scientific bodies and that your research includes interest in computer security and privacy, especially relating to consumer products and media technology law and policy.

And, finally, Carrie Cordero, who is the director of national security studies and an adjunct professor of law at Georgetown University Law Center. I understand that you also have written and studied in the areas of national security and counterterrorism as well as counterintelligence investigations. You have had a number of very significant positions in the Department of Justice and helped to formulate American policy in these areas before your service now in the private sector. I will not go into all of the positions, but they are extremely impressive.

So maybe we can begin with you Professor Donohue. You will have to turn your microphone on.

STATEMENT OF LAURA K. DONOHUE, PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER, AND DIRECTOR, GEORGETOWN'S CENTER ON NATIONAL SECURITY AND THE LAW, WASHINGTON, DC

Professor DONOHUE. Thank you. Thank you for inviting me here today to discuss really much needed reforms to FISA, with particular reference to Sections 215 and 702.

I have submitted detailed written remarks for the record, so for now what I would like to do is just highlight what I see as the most pressing concerns.

Specifically, it is my view that the bulk collection of U.S. citizens' metadata is both illegal and unconstitutional. The Government argues that the metadata program complies with the Constitution. In so doing, it relies in part on the case that you mentioned that held that individuals lack a reasonable expectation of privacy in the numbers that they dial.

The Government also suggests that the national security interests at stake override whatever privacy intrusions might result. For two reasons these arguments are problematic.

First, the metadata program amounts to a general warrant, the use of which by the English played a key role in the American Revolution and led directly to the Fourth Amendment. A general warrant was a writ. It was issued by a court. It did not expire. And it allowed officials to collect information to search anywhere without any particularized suspicion.

In 1760, the British Prime Minister, William Pitt, directed colonial Governors to use these writs of assistance to crack down on illegal behavior. James Otis famously challenged them as the worst instrument of arbitrary power. And John Adams later wrote that this oration breathed life into this Nation. "Then and there," John Adams reported, "was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."

The Virginia Declaration of Rights subsequently included a clause outlawing general warrants. Similar language was adopted by Massachusetts and New Hampshire in their State constitutions and later the ratifying conventions, the most important ones—New York, Virginia, and North Carolina—they required that a prohibition on general warrants be incorporated into the Bill of Rights.

James Madison wrote the Fourth Amendment to prevent the use of general warrants. They were the definition of "unreasonable search and seizure."

The FISC order, authorizing the telephony metadata program, is a general warrant. It authorizes the Government to collect and then to rummage through our papers and effects in the hope of finding wrongdoing. There is no prior suspicion of criminal activity, and almost none of the information obtained actually relates to illegal behavior.

Second point: In defending the program, the Government relies on the 1979 case called *Smith v. Maryland*. In that case, Patricia McDonough was robbed in Baltimore. After giving the police a description of the man who robbed her and the 1975 Monte Carlo car that he drove, she started receiving threatening and obscene phone calls in her own home from a man who said he had robbed her.

Then he phoned her and had her come out on her front porch while he drove slowly by the house in the Monte Carlo. The police saw the car in the neighborhood, got the license plate number, and identified that the car was registered to Michael Lee Smith. The police asked the telephone company if it would put a pen register on Smith. That day he called Patricia McDonough's home. On the basis of this and other information, the police obtained a search warrant. They went into the house and they found a phone book turned down to Patricia McDonough's name.

Michael Lee Smith had robbed, threatened, intimidated, and harassed Patricia McDonough. The police placed the pen register consistent with reasonable suspicion of criminal wrongdoing. The NSA would treat every American as though they were Michael Lee Smith, and it would collect not just the numbers dialed from the home of the suspected criminal, but all law-abiding citizens' metadata—whom we call, who calls us, how long we talk. Calls to a rape crisis line, a suicide hot line, or political party headquarters reveal much more than what was sought in *Smith*.

The Government's argument could be extended to any sort of metadata: email, banking records, financial transactions, and Internet use. The extent to which we rely on electronic communications to conduct our lives is fundamentally different in scale and scope than what happened in 1979, and the NSA would do this indefinitely.

Americans reasonably expect that their movements, communications, and decisions will not be recorded and analyzed by the Government. A majority of the Supreme Court seems to agree.

In 2012 the Court considered a case involving 28-day surveillance using GPS chips. This case recognized that *Katz*'s reasonable expectation of privacy test does not supplant the rights that existed when the Fourth Amendment was written. At a minimum, Justice Scalia wrote, the "18th century guarantee against unreasonable searches . . . must provide . . . the degree of protection it afforded when it was adopted." The protection against the general use of warrants thus stands.

In addition, at least five of the Justices indicated unease with the intrusiveness of modern technology. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, suggested that in most criminal investigations, long-term monitoring "impinges on expectations of privacy."

Justice Sotomayor went one step further. She suggested that disclosing information to a member of the public for a limited purpose does not divest that data of Fourth Amendment protections.

The telephony metadata program also violates the express statutory language of the Foreign Intelligence Surveillance Act in at least three ways:

First, the Government argues that the NSA's telephony metadata program is consistent with the statute in that all telephone calls in the United States, including those of a wholly local nature, are relevant to foreign intelligence investigations. The use of the word "relevant" here is so absurd as to render the term and the qualifying statutory language meaningless.

Second, tangible goods subject to the order must be obtainable by subpoena duces tecum, but no grand jury or court would allow the

bulk collection of all Americans' metadata. It is illegal to use subpoenas for fishing expeditions. Subpoenas, moreover, are specific. They relate to a particular individual or crime, and they deal with current or past bad behavior. The metadata program in contrast is broad, non-specific, forward-looking, not tied to a crime, and looks to anticipate future acts.

FISC itself has recognized the illegality of the program. In March 2009 Judge Reggie Walton acknowledged that metadata could not otherwise be captured in bulk.

Third, and finally, as a statutory matter, all of the information at issue in the bulk collection program is already provided for in FISA Subchapter 3 dealing with pen registers and trap and trace. Using Subchapter 4, the Government appears to be doing an end run around the restrictions that Congress placed on the NSA.

The system, in my view, is badly broken. The NSA is engaging in activities that are illegal and unconstitutional. Congress has an opportunity to fix the problem and to do so in a way that recognizes the benefits of new technologies, the real threats the Nation faces, and the demands of the U.S. Constitution.

Thank you.

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

Senator BLUMENTHAL. Thank you, Professor Donohue.

And I might just say that all of your full statements will be made a part of the record, without objection.

Professor Felten.

STATEMENT OF EDWARD W. FELTEN, PROFESSOR OF COMPUTER SCIENCE AND PUBLIC AFFAIRS, PRINCETON UNIVERSITY, AND DIRECTOR, CENTER FOR INFORMATION TECHNOLOGY POLICY, PRINCETON, NEW JERSEY

Professor FELTEN. Mr. Chairman, Ranking Member Grassley, and Members of the Committee, I thank you for the opportunity to testify about technical issues related to surveillance.

I am not an expert on the law, and I offer no opinion on the legal status of any program. Nor do I presume to say how best to balance the legitimate goals of conducting foreign intelligence surveillance against the legitimate goals of protecting privacy and promoting civil liberties. I hope that my testimony will help you appreciate the power of metadata and control its use appropriately, consistent with the need for effective foreign intelligence.

The NSA has acknowledged that it is collecting metadata—who called whom, when, and for how long—about nearly all phone calls in the U.S. Earlier, General Alexander said that the NSA is not currently collecting location data, but if it were to begin collecting location data, this would raise additional serious issues.

With today's analytic tools, metadata often amounts to much more than just a list of numbers dialed. Often it reveals information that could traditionally be obtained only by examining the contents of communications.

Metadata can now yield startling insights about individuals and groups, particularly when collected in large quantities across the population. It is no longer safe to assume that metadata is less revealing or less sensitive than the content it relates to. Just by

using new technologies such as smartphones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many of the details of our lives can be gleaned by examining those trails. And the only reliable way to avoid creating those trails would be to avoid using these technologies altogether.

Metadata can be highly personal. A series of calls to an oncologist or an obstetrician or to a suicide hotline or to an alcoholism counselor or to a competitor's personnel office or to an Inspector General, the pattern of calls reveals content.

Metadata also reveals relationships. Frequent late-night calls can reveal an intimate relationship. Calls to a counselor or divorce lawyer can reveal the state of a marriage. Calls to parents or siblings, or a lack of calls, can reveal the status of family relationships.

Metadata is naturally organized in a way that lends itself to analysis. By contrast, content is unstructured and can be difficult to analyze and understand. Today a growing set of computing tools can turn metadata trails into penetrating insights, and given limited resources, analyzing metadata is often a far more powerful analytical strategy than investigating content, yielding more insight with the same amount of effort.

When focused on intelligence targets, metadata collection can be a valuable tool. At the same time, unfocused collection of metadata across the whole American population gives Government access to many of the same sensitive facts about the lives of ordinary Americans that have traditionally been protected by limits on content collection. Metadata might once have seemed much less informative than content, but this gap has narrowed dramatically and will continue to close.

Today's hearing is a vital step in a process that should continue. Technical expertise is essential for effective oversight of these technologically complex programs, and I would respectfully urge you to consider how best to integrate technical expertise into the oversight process.

As an example, the Foreign Intelligence Surveillance Court in its declassified opinions expressed frustration that the NSA had not disclosed significant technical information. The NSA's good faith effort to summarize the technology for the Court's benefit could have led to the omission of information that the Court later found highly relevant.

Technologists within the NSA surely knew how their program operated, but this information had to pass through other people, some of them less attuned to the significance of certain technical details before it could reach the Court. And the Court, without access to technical advice, was not able to ask the sort of probing technical question that might have elicited the missing information.

The United States has the world's strongest pool of technology experts, many of whom are available to assist in the oversight process. I look forward to your questions today and, more broadly, to continued constructive engagement between oversight officials and technical experts.

Thank you.

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

Senator BLUMENTHAL. Thank you, Professor Felten.

Professor Cordero, I want to apologize. I have to step out for a very quick visit with a group that has been waiting to meet with me. I have read your testimony. It is excellent. If I am not back in time, Senator Grassley can proceed to questions, and I should be out for just a few minutes. So please proceed.

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

Professor CORDERO. Thank you, Mr. Chairman, Ranking Member Grassley, Members of the Committee. Thank you so much for the opportunity to be here today.

In my written statement, I have provided the Committee with information about my previous experience as a national security law practitioner, and that statement also recounts my experience working at the Department of Justice on September 11, 2001, and includes examples of how pre-9/11 law and interpretations of the law led to significant bureaucratic processes inconsistent with the speed and agility needed in national security activities.

Indeed, in the years leading up to and then after 9/11, the FISA process was subject to the exact opposite criticism that it seems to be today: The Department of Justice was accused of being too reticent, too cautious, too unwilling to be aggressive under the law in order to protect national security. Subsequently, I had an up-front view regarding how the intelligence reform laws passed by Congress over the next several years vastly improved the intelligence community's ability to protect the Nation from another attack on the scale of September 11th.

So I am here today to urge caution in implementing quick fixes that may sound appealing but that could have lasting consequences at a practical level that could negatively impact intelligence community operations and the Nation's security for years to come. I do not want to see us go backward.

Since the unauthorized leaks of this summer and subsequent reactions, I have observed three main critiques of the current FISA activities. Let me take each one along with some of the proposed reforms.

First, with respect to the proposals to restrict collection under FISA, my perspective these arguments—that these programs—and I am referring to both the 702 and the 215 program—are illegal are mostly arguments about what the law should be, not what the law is. That said, the Government's interpretation of 215 is a more forward-leaning interpretation of the law than is its implementation of 702.

The 702 collection is targeted against non-U.S. persons reasonably believed to be outside the United States. These are not individuals with constitutional protections, and the collection against them is conducted in accordance with the statutory framework debated extensively and passed by Congress in the FISA Amendments Act of 2008.

The metadata collection under 215 is obviously large in scale, but I would submit that the Government's arguments in this are con-

sistent with existing precedent, no matter what direction the courts may go in the future.

I would comment to the Committee the recently declassified opinion and order by FISC Judge Claire Eagan dated August 29, which offers a straightforward analysis of the law that explains why the Court continues to approve this collection.

In addition, senior leaders of the intelligence community continue to advise that the 215 program remains a valuable part of the protective infrastructure that was implemented after September 11th. Therefore, in my view, it would be premature for Congress to abruptly end the 215 program through legislation.

Second, with respect to the proposals to enhance public confidence, two themes emerge in proposals to add a special advocate or public interest advocate to the FISA process. One view is that the Court could benefit from an additional view, particularly in cases involving technical complexity or novel legal issues. A second view is that a special advocate would go a long way in restoring public confidence. I have concerns about both proposals.

If what the Court seeks—and it would be helpful to hear from the current Court on this issue—is simply an additional view beyond that which is presented by the Justice Department on behalf of the intelligence community, then I would submit that empowering the existing Civil Liberties Protection Officer, a position created by Congress, to present his views directly to the FISC would serve that purpose. This proposal would address the substantive concern that the Court could benefit from an additional view, and it would do so without adding substantial layers of additional bureaucracy.

On the public confidence point, I would suggest that an outside advocate would not carry the weight that is hoped it might provide with the public in the longer term. If done in a manner protective of classified information, the advocate would necessarily work in secret, alongside the executive branch. With the passage of time, outside observers will just see the advocate as another participant in a secret process.

So what would enhance public confidence? Perhaps the most frustrating part of the reaction to the leaks from my perspective has been the nearly complete lack of confidence in or comfort by the existing oversight mechanisms, particularly with respect to 702 collection. I can personally attest that the oversight is extensive and exhaustive. So I will offer a few suggestions of what might be some steps in the right direction to bolster both congressional and public confidence.

One, Congress can ensure that the offices conducting oversight are staffed and funded appropriately to their responsibilities. The internal executive branch oversight process that has been built requires a lot of man-hours to do it right, and the quality of oversight will suffer if any of these offices are stretched beyond their capabilities.

No doubt there is an irony here in making this point in the midst of the Government shutdown.

Two, Congress could consider requiring an annual or semiannual public report that produces information currently contained in the classified joint compliance assessment. This report might help bet-

ter inform Members of Congress beyond the Judiciary and Intelligence Committees regarding the oversight and compliance process.

Three, Congress should focus its efforts in working with the NSA, the Justice Department, and other components in the intelligence community to reduce the complexity of internal procedures. I have explained the reasons for this recommendation in greater detail in my written statement, but to summarize, one aspect of reducing compliance incidents is reducing the complexity of internal operating procedures to ensure that operators at the working level understand the rules they are operating under.

Third—and I will hit this point quickly—with respect to the proposals to enhance transparency, this seems to be an area where there is clearly room for Congress to act. My own view is that the seemingly ad hoc nature of the recent Government declassification releases is not actually helping as much as they might think. If declassification is the new norm, then there needs to be a more regularized and consistent method of releasing information. This might include amending the reporting provisions in FISA to provide additional public information, whether it is statistics, declassified legal opinions, summaries of implementation actions, or reports on compliance matters—semiannually, quarterly, or at some other appropriate regular interval. In my view, this might cut back on each release being an event unto itself.

Thank you very much for inviting me here today to share my views, and I look forward to your questions.

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

Senator GRASSLEY [presiding]. Senator Whitehouse, Senator Blumenthal said I could go ahead.

Senator WHITEHOUSE. And I think you should.

Senator GRASSLEY. Thank you. You are in the majority, do not forget.

Professor Donohue, I understand that you concluded that the bulk collection of phone records under 215 is illegal. I call to your attention that President Obama is a former constitutional law professor, editor of the Harvard Law Review, and you probably know that he has concluded that the program is legal both under statute and as a matter of constitutional law.

Is it your view then that President Obama is wrong?

Professor DONOHUE. Yes.

Senator GRASSLEY. Okay. A further question, this time of Professor Felten. You testified that telephone call metadata can reveal an incredible amount of information about a caller when aggregated with other data and analyzed. For example, you mentioned that metadata can reveal sensitive information about the caller's relationship, lifestyle, and activities. But under the FISA Court order, bulk telephone metadata collected under Section 215 can only be assessed and searched by the Government when it has reasonable and articulable suspicion that the phone number is connected to terrorism.

Question: Does your testimony underscore what a valuable—no, let me start over again. Doesn't your testimony underscore what a valuable tool the collection of metadata under Section 215 is to

keep the country safe? Aren't the relationships and the activities of suspected terrorists precisely the kind of information that the Government should be trying to learn about them as rapidly as possible?

Professor FELTEN. I certainly agree, Senator, that it is important for the intelligence agencies to have the ability to get this information about terrorists and their associates, and this I think goes to the issue of focus that I discussed in my testimony where, when focused on terrorists and their associates, certainly I think few Americans, if any, would object to this sort of program. But when it is unfocused across the whole population, it does raise the same kinds of privacy and civil liberties issues that arise with content. And, therefore, I think it makes sense to think about how best to balance those issues in order to make sure that the collection and analysis of that data is limited—is available where necessary, but is also not without bound.

Senator GRASSLEY. Thank you. And I will go to Professor Cordero. I would like to describe a few aspects of how Government attorneys practice before FISA. For example, do Justice Department lawyers who appear before FISA Courts have an obligation to present both sides of an argument, including law or facts that run counter to the Government's position? And would you say that their presentation of opposing views is as vigorous as would be accomplished by an independent advocate?

Professor CORDERO. Thank you for the question. With respect to the practice before the Court, the practice is ex parte, in camera, and what that means for the attorneys for the Justice Department who do that practice is that they have a heightened obligation in the FISA Court practice. In addition, with respect to their ethical obligations as members of the bar, whenever attorneys practice ex parte, in camera, they have a heightened obligation to bring both the facts that are supportive of their case but also derogatory information or contrary information that might be relevant to the Court's judgment. And so certainly my experience at the Department of Justice was that that was how we conducted our business.

In addition, the Court has legal advisers who conduct independent review, and then there are the members of the Court themselves who are independent district court judges.

I would also commend to you Judge Walton's letter to this Committee in July where he explained the process between which the Government works with the Court and when the Court asks questions and how the Government responds to those questions. And it is a very extensive and probing process.

Professor DONOHUE. Excuse me, Senator. May I add something to that particular response, please?

Senator GRASSLEY. Certainly.

Professor DONOHUE. Thank you very much. I just want to mention in regard to the Foreign Intelligence Surveillance Court, they are not performing the function that they were originally envisioned to perform under FISA. They were supposed to narrowly grant orders. And what we are seeing are dozens of secret opinions which we have not seen. Some, as we found out in July, are hundreds of pages long and make rulings on very complex, difficult constitutional questions. There is, for instance, a special exception

that the Foreign Intelligence Surveillance Court has carved out for foreign intelligence out of the Fourth Amendment. The Supreme Court has never recognized in the Special Needs Doctrine a special exception for foreign intelligence.

In order to adequately air these views, having opposing counsel or, what Senator Blumenthal has suggested, a constitutional advocate, would be of great assistance.

The recently released opinion that Judge Eagan put out is only three double-spaced pages on the constitutional questions that are far more complex than are encapsulated in that opinion. So, to adequately air what the Court has become, it is important to have somebody there as a constitutional advocate.

Thank you.

Senator GRASSLEY. Could I ask one more question? This will be my last question for you, Professor Cordero. In your experience, how often does FISA Court challenge proposed Government applications by signaling that they may be insufficient? Describe the process by which Government lawyers attempt to resolve possible insufficiencies for the Court, including the role of legal staff. And does the high rate at which the Court ultimately approves Government applications reflect the process?

Professor CORDERO. Thank you. So with respect—I do not have a numerical sort of number to give you with respect to how frequently the Court questions the Government presentations. In my experience, which ended in Government in 2009, however, it was a very frequent occurrence that there would be exchanges and question-and-answer periods between the Government lawyers and the Court on a very frequent basis, and it could happen at various levels.

So, for example, if there was just a routine matter and there might need to be sort of small clarification questions, that might occur at the level between the Court's legal advisers and staff attorneys. If there were more significant issues that might be at issue in a particular application or request, then that might involve sort of more senior levels of the Department of Justice engaging with either the legal advisers again or members of the Court. And this process can continue. If there were extraordinarily significant issues raised in a particular request, that might raise the attention and sort of the involvement in the discussions with the Court up to the level of the Assistant Attorney General for National Security or even the Attorney General.

So it would be an exchange of questions and answers and an iterative process that, depending on the complexity of the matter or the judge's concerns, could either be resolved quickly or go on for some length of time.

That being said, the overall numbers, as Judge Walton's letter had explained this summer in his letter to the Chairman, the overall numbers of approved applications does not reflect that process at all. And it also does not reflect the scenarios in which the Court might request changes be made to applications or proposed orders, whether the Court modifies the proposed orders, or requires that the Government proceed in a different way. And it also does not indicate in that statistic whether or not there was a circumstance that the Court indicated informally to the Government that I might

deny an application and the Government then would withdraw that application.

Senator GRASSLEY. Thank you.

Senator BLUMENTHAL [presiding]. Thank you, Senator Grassley.

Let me begin by pursuing the line of questioning that Senator Grassley just introduced about the constitutional advocate, which, as you know, I have proposed. And I know, Professor Cordero, you have outlined your concerns in depth, and I do not know whether some of those concerns would be addressed by the fact that the challenge or the questions to be raised would be done after in time the authorization of whatever surveillance might be indicated. Would that address some of your concerns? Because I think in your testimony you indicated that it would be a sea change for this kind of advocacy to be done before the authorization of whatever the surveillance might be.

Professor CORDERO. Thank you, yes, and in my written statement I did have in mind sort of at the FISC level prior to collection, the idea of adding an adversarial process at that level.

With respect to adding an advocate at an appellate level, it raises some different issues. Certainly it would reduce the concerns about impeding operational speed and agility, so it certainly would, from my perspective, be better in that sense. But I guess the question I would ask is sort of which—what problem is it trying to solve and who the client would be of this constitutional advocate. Because I know from my experience, which, again, is a few years dated, but from my experience as the lawyers presenting these cases to the Court in the ex parte, in camera fashion, we operated in a culture that we were operating in the public interest and that our client was the American public and the American citizen. And that was sort of the culture that permeated that office at the time, and I do not have any reason to suggest that that has changed since.

In addition——

Senator BLUMENTHAL. And I do not dispute that that culture existed then and existed now, and what we have seen, if you read Judge Walton's opinion about what resulted from perhaps an inadvertent failure to communicate—and you were here when General Alexander described the lack of communication between two areas of the intelligence community—that could happen again. The problem to be addressed is potentially that kind of mishap which constituted a violation of law and was very significantly criticized by Judge Walton. In fact, he criticized the misrepresentation. And either the violation of law or misrepresentation certainly could have been addressed not only at the appellate level but at the FISA Court level as well. So that is the kind of problem that could be addressed.

And I recognize—and I was a Government lawyer myself and represented the United States as well as the State of Connecticut—that Government lawyers generally try to do the right thing, represent the American public, but their view may be affected by what they see as the public interest, which may be skewed to one side of an argument for granting a warrant or another or approving metadata collection or not. And the adversarial process traditionally operates to bring out the truth. So that is my question to your question, what is the problem or what is the issue or need for some

constitutional advocate? And very simply, who is the client? The Constitution and the constitutional rights of the American public.

Professor CORDERO. So I guess sort of two thoughts on that. One would be with respect—if part of the concern then is addressing the Court's—what might be the Court's desire, sort of as expressed by Judge Carr when he has testified before and in his op-ed, that the Court would benefit from an additional view on constitutional issues, then on that point that is why I have suggested that it might be appropriate to consider whether or not the existing Civil Liberties Protection Officer, who was a position created by Congress to consider matters of civil liberties and privacy, that that person might simply be more formally empowered to present an independent view to the Court, and that way that would be a person who is up to speed, knowledgeable, and aware of all the complexities of the issues, but might have a slightly different view that it could inform the court about versus that presented by the Justice Department on behalf of the intelligence community.

Senator BLUMENTHAL. Thank you.

My time has expired. I have additional questions. If there is no objection, I am going to turn to my colleague Senator Whitehouse rather than keep him here and then return to my questions.

Senator WHITEHOUSE. I think it is within the Chairman's right to have as many rounds as he pleases, so have at it. But thank you for recognizing me.

Let me start by saying to Ms. Cordero that I think your practical experience in this area gives, at least to me, your testimony additional weight, and I appreciate it And I thought you made a very significant point when you talked about the need for "more regularized and consistent methods of releasing information." I think that was the phrase that you used.

We are still looking into it, but it appears to me that our intelligence community was caught flat-footed by the sudden, unexpected, unauthorized disclosure of classified information. And in the early days it had all of the outward appearance of a mad and unprepared-for scramble.

An air crew prepares for the eventuality of a sudden, unexpected decompression of the aircraft, for instance, and I do think it is important that our intelligence community consider what we now know to be the virtual inevitability of these types of releases taking place, and have a more robust, immediate response to that eventuality, but also bet on it happening in the future and be more candid with the American people in the run-up, because I think a good deal of what has been disclosed could have been disclosed earlier, and I think the downside of classification in this area is very real. There is always an upside. It protects our sources, it protects our methods, it protects people who are helping us. It makes successful programs continue to be successful because people do not avoid them. If you disclosed who you were wiretapping, obviously your wiretap would fail, and we do not do it that way for very obvious reasons.

So there is some real value to things being classified, but there are also all sorts of oversight and other issues that are raised, and I think you have a very balanced and sensible suggestion about try-

ing to do that on a regular way, and I look forward to working with you to develop that further.

Professor Felten, you said it was important that this information be available where necessary to our national security officials. Given the nature of the operation, that means it has to be somewhere. You have to be able to have the information. You do not get the luxury of being able to go back after the fact and figure out what you should have collected. So by your hypothesis that it needs to be available where necessary, I take the implication that collecting the whole haystack is necessary because otherwise it is not available where necessary. You cannot know that in advance.

The second part of your point was that it must be available where necessary, but it has to be limited to help protect the privacy interests that are here at stake.

Now, the way we have customarily done that over the years has been through mitigation techniques that go originally all the way back to wiretaps where the FBI agent listening in on the wiretap with the headphones would listen to the conversation, and if it looked like somebody was ordering pork chops from the butcher or talking to their Mom, you would flip off the conversation for a while, and then you would flip it back on to see if it was still unrelated to the criminal investigation, and then you flip it back off. And, obviously, it has gotten a lot more sophisticated since then in this new environment.

But do you concede that the whole haystack method protected by adequate mitigation is actually necessary to accomplish the result that you have indicated is ideal, which is that the data to protect our country should be available where necessary?

Professor FELTEN. I do not think it is necessary to collect all of the data immediately. My view is that the policy with respect to metadata, the policy tradeoffs with respect to metadata are becoming more similar to those with respect to content, and the example that you gave of minimization on a traditional wiretap even while the wiretap went on is a non-collection of data because there is not enough reason to believe that it is relevant to the purpose. And this is a balance that has been going on with content for a long time.

Senator WHITEHOUSE. The difference, of course, is that that is one thread of information, and the necessary protection purpose is accomplished by staying in real time, by listening to that conversation as it develops. When you are trying to connect a network of contacts that a terrorist overseas might have, it is too late in the game to build that network if you do not have the information necessary to do that; otherwise, you are working—I mean, you may eventually be able to do it, but you risk a timing problem with by the time you have developed that network, you have missed important players in it, and the event that you are trying to prevent has taken place already. And it is the preparedness, I think, that is an important part of this. So I guess I would put myself on record as disputing that the haystack plus mitigation modality is not adequate.

Let me ask all of you another question. We have talked a little bit about the—you know, it has been long established that the kind of metadata that is collected through these programs is not pro-

tected by the warrant requirement. Everybody who has been in law enforcement here—Chairman Leahy, Chairman Blumenthal, myself, Senator Klobuchar, former U.S. Attorney Jeff Sessions—we have all gotten access to this data without a warrant, and it actually is achieved pretty readily. And, in fact, in the early days, it was done almost informally with the phone company, and now it has been regularized more. So there is an unquestionably vast amount of both legal and practical precedent for that proposition.

At the same time mitigation has taken place for a very, very long time and is also equally well established, both as a legal protection and as a practical means of doing this.

So there you have got long-established legal and practical precedent, and I think it is reasonable to draw conclusions from that looking forward.

Now, to my question, there is another long-established precedent, which is that if you are the police chief and you want to put a tail on somebody you suspect, you do not need a warrant for that either. You can take a police officer, a plainclothes officer, and say, "Look, we need to know where this guy is going. You tail him and let us find that out." And that has been true for as long as there has been law enforcement. So, again, another long-established precedent.

Then along comes *United States v. Jones*, and in *United States v. Jones*, the police decided that instead of just tailing Antoine Jones, they would put a beacon on his car, and they would track that beacon, which would obviously save law enforcement resources, take advantage of new technologies, be the smart thing to do, et cetera, et cetera, et cetera.

The Supreme Court in that case said that that was a search and that that required a warrant, even though following him around would not have required a warrant. And while the constitutional basis for that decision I do not think is fully settled yet, there was a bare majority that said it is because of the physical trespass by putting the beacon on the car, but there was another majority that said, no, actually you have got to look at—they were unfortunately in the form of a concurring opinion and another concurring opinion, so they did not form five. But if you read Justice Sotomayor's concurring opinion and the concurring opinion of four, they are all saying, look, just under the expectation of privacy test, this is a search also.

So I deduce from that that there is a point, in fact, where new technology and scale change the underlying nature of what had forever been a non-warrant-requiring search. And so I think it is an actually very live constitutional question how *United States v. Jones* should apply to these programs. I have yet to see an opinion of the FISA Court that addresses that.

The Eagan opinion came out very recently and did not address it—came out since the *Jones* decision and did not address it. So I am interested in each of your views as to how you would expect the FISA Court to rule when a case came up that obliged it to look at the application of *United States v. Jones*, the beacon decision. Let me start with Professor Cordero.

Professor CORDERO. Okay. Thank you, Senator. Certainly the *Jones* case is on the minds of everybody who considers these issues. With respect to——

Senator WHITEHOUSE. Except Judge Eagan, evidently.

Professor CORDERO. Well, with respect, though, to Judge Eagan's opinion, so what she said is—and I will quote. She said that the production order under the 215 is "squarely controlled by the Supreme Court decision in *Smith v. Maryland* and the *Smith* decision and its progeny have governed Fourth Amendment jurisprudence with regard to telephony communications metadata for more than 30 years."

There have been 14 judges of the Court who have approved the 215 program since 2006 34 times. The *Jones* case came after 2006, but there still have been at least some of those judges who have continued to approve the 215 case subsequent to the *Jones* case, and so that might be perhaps one suggestion that the Court is still satisfied.

Judge Eagan also said that the fact that the data was not collected in bulk in the *Smith* case or, if you take the inverse of that, that it currently is conducted in bulk, she said that that would not change her analysis.

So that being said, as I mentioned in my written statement, this is certainly an area where the law may change in the future. In the *Jones* case, as you mentioned, the majority that held that the GPS surveillance was a search, held it on the trespass grounds, not on the grounds that actually following the person around through the GPS surveillance was the search. It was the second sort of concurring majority part that said that had they decided the decision, they would have held on that grounds. But as you noted earlier in your remarks, that actually turns what are traditional investigative techniques of physical surveillance on its head from formerly being one of the most least-intrusive techniques to now all of a sudden flipping it up to a warrant requirement.

Senator WHITEHOUSE. I think rather than ask the other two to respond, I have now gone so far over my time that it is really impolite to the Chairman, and I will——

Senator BLUMENTHAL. You can go further.

Senator WHITEHOUSE. Then we will finish with their answers, and I will yield, but I appreciate very much the Chairman's patience with this.

Professor FELTEN. Well, I do not have the legal expertise to predict how a court would rule on—interpret *Jones*, but with respect to your discussion of law enforcement and police access to metadata, certainly this has been going on for a long time, and appropriately so.

The modality there has not been one of transferring all data to law enforcement and then having them pull out the pieces they want later. Law enforcement and prosecutors have been able to go to the phone company and get the records they need when they need them.

Certainly I would agree that technology provides new ways of managing this process, and one of those ways is to allow an intelligence agency to get the data that they need in a targeted and fo-

cused way in real time, without needing to transfer all of it from the beginning.

Senator WHITEHOUSE. Professor Donohue.

Professor DONOHUE. Thank you for your question. I would like to address just briefly the minimization technique point that you raised and then move to the question that you pose.

On the mitigation techniques, minimization was only one of many protections that was built into the statute. FISA also had prior targeting before you could place intercepts. You had probable cause that an individual was a foreign power or an agent of a foreign power. You had the Foreign Intelligence Surveillance Court, and you had a higher standard for U.S. persons. All of that has been swept aside for the 215 metadata program. Now there is a general order, the NSA determines RAS, whether there is reasonable, articulable suspicion. There is not a different standard——

Senator WHITEHOUSE. Well, it has not extremely been swept aside for the metadata program. The metadata program faces the reality that unless you are gathering the information, you do not have a haystack to search in. But it does not mean that a search actually ever gets done of the haystack, and the steps required to search the haystack are far more rigorous than all the ones that you just mentioned.

Professor DONOHUE. So the problem is that in building the haystack, all of the protections have been thrown out. And with the type of information that you can get from this telephony metadata——

Senator WHITEHOUSE. And that is kind of the question, isn't it? Is the building of the haystack the search or not? Even if nobody knows what is in it. Even if nobody knows it, is there a privacy interest that is lost when nobody knows that you made those calls, but there is a haystack out there and under the right circumstances somebody could find out?

Professor DONOHUE. And there are two responses to that——

Senator WHITEHOUSE. That is an interesting—that is kind of the crux of the question we have got.

Professor DONOHUE. There are two responses to that. One is the Foreign Intelligence Surveillance Act is about the acquisition of information, which is when that information is acquired. And, second, I would go back to the general warrant. The purpose of the Fourth Amendment was to prevent general warrants, which was to search for information and to conduct searches indefinitely without any particularized showing. And there is a constitutional violation that goes on in that case.

Senator WHITEHOUSE. Although there are lots of things that people do in law enforcement and have since the dawn of time that they do not even need a general warrant for because there is no warrant requirement. And so you cannot use the warrant requirement as a criticism of the way in which that has been done. It has never been within it. So things that were not subject to a warrant requirement do not require a general—the general warrant problem I do not see as being pertinent here.

Professor DONOHUE. No, this goes to the reasonableness or unreasonableness of the search itself. That was the point of the Founders. That was why Jefferson included this. This is why Madi-

son was talking about this. This is why it was in the Virginia Declaration of Rights. This is why New Hampshire, Massachusetts—it was the actual reasonableness.

Senator WHITEHOUSE. And that takes us back to the question of what is a search.

Professor DONOHUE. Of what is a search. Well, the reasonableness——

Senator WHITEHOUSE. Does human knowledge——

Professor DONOHUE. And unreasonableness.

Senator WHITEHOUSE. Does human knowledge define the search or does its availability in the haystack define the search. And that is, I think, a really interesting and important question that we need to address. But I do not think you can jump across back and forth between those two definitions and still have a logical and practical discussion.

Professor DONOHUE. Okay. Let me address your second point as well, which is this broader question, if you can use these powers in law enforcement, and there are two parts to this. One is the pen register abilities that law enforcement has, and second is the subpoena powers. And just on the subpoena power point, you cannot go on fishing expeditions. You cannot, for instance, convene a grand jury in Bethesda and just see what is happening in town and start mining it for information. You cannot use a subpoena to obtain generalized information. It has to be material and specific to a particular suspected crime or individual or series of activities.

This is not what we are discussing. This is not what could be otherwise obtained by a subpoena duces tecum, which the statute requires and which the FISC judge, Judge Walton, said there is no other legal way you could get this information. So it is very different from the kind of subpoena power that somebody would have in law enforcement.

On the pen register side, I think you are exactly right to highlight what is going on with *Jones* and the extent to which metadata and the types of things that Professor Felten is discussing have changed the incursions into privacy that are possible. In the case of *Smith v. Maryland*, Michael Lee Smith had robbed, harassed, threatened, made obscene phone calls, drove in front of her house, and tried to intimidate her. And on that basis, they got one pen register that, within a 24-hour period, recorded that he called her again. They went into his house. They got a general—or not a general, they got a specific warrant. They went into his house. They found the phone book turned down to her name. That is a completely different situation than collecting bulk information.

Senator WHITEHOUSE. The holding of the Supreme Court in that case—if we are going to talk about the case, the holding of the Supreme Court in that case was not because he behaved in those awful ways you are entitled to get this. The holding was this is not Fourth Amendment—warrant requirement protected in the first instance. And it did not matter whether he had been awful and engaged in all sorts of abusive and ghastly conduct or not. There is a constitutional line that it drew, and the holding was that that kind of pen register information simply does not require a warrant, period.

Professor DONOHUE. And I would respond to that, you are absolutely right. In that situation it did not require a warrant. What we are talking about is the wholesale collection——

Senator WHITEHOUSE. Nor has in any situation since, right? It was not——

Professor DONOHUE. Well, certainly. Certainly the shadow majority in *Jones* found exception to that. Justice Alito's opinion joined by three——

Senator WHITEHOUSE. Now we are back to my question about the shadow majority in *Jones*, and I will accept that. But I do not think it is fair to say that *Smith* was a case that is defined by its facts in any way. It has been one of the cases that has had the broadest practical and judicial acceptance in real law enforcement life of anything. It has gone on for——

Professor DONOHUE. And yet Justice Sotomayor in *Jones* goes on to say that she would not extend to third-party data the same protections that they would otherwise not deserve under the Fourth Amendment precisely because of technology. We have seen this also in the Circuits at an appellate level. We have seen a number of judges express this same——

Senator WHITEHOUSE. So to summarize, because I have now gone way too far, to summarize, you do think that it would be incumbent upon the FISA Court to consider the *Jones* decision at a minimum, and in your view, in considering it they would likely further restrict the capabilities of this program.

Professor DONOHUE. Not only should they consider it, but this also goes back to Senator Blumenthal's point of the necessity of having a constitutional advocate there who can bring up *Jones* and these other cases—as you note, it is nowhere in Eagan's opinion—and to have somebody there who can bring this up so that the Court does have to wrestle with this and address this directly.

Senator WHITEHOUSE. Thank you, Chairman. You have been immensely patient.

Senator BLUMENTHAL. Thank you.

I want to thank Senator Whitehouse for raising *Jones* and this issue of technology having to be considered by the FISA Court because it does revive the point that I made in the previous panel that a lot of the constitutional jurisprudence seems to depend on the *Smith v. Maryland* case, and the technology there was really very primitive compared to what we have now. And if at least a number of you feel that *Jones* may be relevant and should be considered by the FISA Court—let me go back to Professor Cordero—would it not be useful to have an advocate to, in effect, present in an adversarial way the implications of the *Jones* case in testing surveillance conducted under this very, very different, profoundly different technology?

Professor CORDERO. Well, as this Committee is aware and as the Intelligence Committees also, this Committee is in a position to receive information that is not available to the public that involves pleadings or opinions that the Court has made beyond that which has been identified. So I do not know whether or not *Jones* has ever been considered by the FISA Court in any of its decisions. It may be that it has, and it may be that that is information that

would be available to the Committee or the Intelligence Committees.

But that being said, the Court has a rule that when there are new or novel issues of technology or law that are being presented to the Court, it requires a Memorandum of Law from the Government. And so the Government needs to explain and bring to the Court's attention, "Court, this is something that you have not seen before, and here is our Memorandum of Law explaining sort of the parameters of that." And whether that would involve the *Jones* case or some other relevant case law, certainly it would be the practice of the Department as a general matter to inform the Court and bring to the Court's attention relevant case law.

Again, I cannot speak to whether or not this specific case has been an issue that has arisen in a Memorandum of Law that the Department has provided, but I certainly——

Senator BLUMENTHAL. Well, you say——

Professor CORDERO. Would not be surprised.

Senator BLUMENTHAL [continuing]. You cannot speak to it. Are you saying that to your knowledge *Jones* has not been presented? Because I am not aware of *Jones* having been part of any——

Professor CORDERO. I simply do not know, sir, because I left Government at the end of 2009.

Senator BLUMENTHAL. Okay.

Professor CORDERO. So I simply do not have that information. Perhaps the Committees do, or perhaps the other Committees do.

Senator BLUMENTHAL. But so far as you know—and you cited a certain number of judges and a certain number of opinions, 14 judges in 34, did you say——

Professor CORDERO. Instances, right, where the 215 program was affirmed by the Court. But speaking more——

Senator BLUMENTHAL. None to your knowledge has considered *Jones*?

Professor CORDERO. Well, when I am saying they have—whether or not they have considered *Jones*, I am speaking a little bit more generally, so not just with respect to 215. As a general matter, if the Government were presenting novel issues of technology or law, they would brief the Court on those issues, and I would expect that they would bring important cases to the Court's attention.

Senator BLUMENTHAL. And I understand your point that the Government has, as you have referred to it, a "heightened obligation" because there is no one on the other side. But there is an institutional interest and maybe even a national security interest in the Government not raising for the Court, "By the way, Judge, you know, here are the ways that *Jones* could really challenge this whole construct of jurisprudence on which the warrant procedure rests, and here are the"—in other words, it may not be directly raised by a specific request of the Court, and it would take a great deal of heightened scrutiny or heightened obligation for counsel to, on its own initiative, raise a challenge of that kind.

So we both know that courts always make better decisions if they hear both sides of the argument through an adversarial process. It is a theme that runs through our court system. It is one of the underpinnings of our jurisprudential system. And you have indicated just now that perhaps the office of—the Civil Liberties Pro-

tection Officer could provide some kind of substitute. But, of course, that Officer now under statute reports to the Director of National Intelligence. There is no way that that Officer could present an objective or independent view, either in litigation or even in advising the Court.

So I come back to the question: Doesn't the question that Senator Whitehouse has been raising about the implications of *Jones* raise again—shouldn't the FISA Court have been hearing exactly these kinds of questions?

Professor CORDERO. Well, I guess, Senator, what I am suggesting is that I think there is a reasonable possibility that the Government, in fact, would brief the Court on a decision of such import in its capacity of providing a Memorandum of Law regarding the issues that it would provide in its ex parte, in camera process.

In addition, with respect to the special advocate, I think there also could be some consideration to the relationship that exists currently between the Government and the FISA Court, and I think that relationship and sort of the exchange of information and the process that goes back and forth is explained in Judge Walton's letter.

In considering the proposals for the advocate, I would hope that the Committee would sort of take into advisement whether or not adding an adversarial process might actually disrupt in some way that relationship of trust and working together that the Department and the Court have developed over a course of decades.

Professor DONOHUE. Senator, may I add something to that?

Senator BLUMENTHAL. Yes. I was actually going to ask both Professor Donohue and Professor Felten to comment.

Professor DONOHUE. Thank you. So I want to recognize at the outset, in 2009 it was the Department of Justice that actually recognized that there were noncompliance incidents going on, and they were the ones that reported it to the Foreign Intelligence Surveillance Court, that for the first 3 years the program operated, that actually of 18,000 inquiries per day as of January, only 1,800 or so had reasonable, articulable suspicion. It was DOJ that was performing its due diligence and reported that to the Court.

With that said, you know, as Justice Jackson reminded us in *Irvine v. California*, the executive is hardly a disinterested, neutral observer when its own interests are on the line. We read in Federalist 47 and 48, Federalist 51, when Madison says the ambition of the man must be aligned with the ambition of the office; if Government is to govern man, we must find a way to get it to control itself; that these checks and balances are very important. And as you note, within our judicial system, we have adversarial processes to ensure that individual interests do not taint the outcome of cases.

And so I think it is terribly important to have somebody there to represent constitutional concerns that does not have an interest that might otherwise be swayed, and that provides another voice to the Court, especially if they are going to be considering such weighty constitutional questions and then issuing opinions secretly, hundreds of pages long that carve out exceptions to the Fourth Amendment. You absolutely have to have an adversarial process involved in that.

Senator BLUMENTHAL. Thank you.

Professor Felten.

Professor FELTEN. Whether it is through an adversarial process or through the Government presenting the full scope of information to the Court, when it comes to issues of complex technology, it is important that the Court has access to the kind of expertise that it needs to make a well-informed decision. And perhaps that takes the form of the Court being able to use a court-appointed expert or a special master, perhaps if there is an adversarial process, whoever it is that is arguing on behalf of civil liberties or the public also has access to the expertise that they need to do that well.

Senator BLUMENTHAL. Thank you.

Senator Whitehouse, did you have other questions?

Senator WHITEHOUSE. Mr. Chairman, I just wanted to observe that actually in our own procedures here we do our very best to try to create that adversarial exchange of views. Clearly, Professor Cordero and Professor Donohue have very different views about what should be done here. Each has acquitted themselves I think with very great ability in this particular forum, and it is a virtual constant that in our hearings we have witnesses from different points of view so that we can hear those.

In my years on the Intelligence Committee, I really felt that we were—a difficulty was created for the Committee by the fact that in deeply classified programs there was no way that you could bring a different view in. And so in the same way that the Government has a heightened standard, I think we all felt very keenly the heightened standard of inquiry necessary because there was not public inquiry and there was not exchange of views. And that to me is—we vote with our feet sometimes, and in Congress, I think we have voted with our feet in favor of as close to an adversarial type method as we can in the way we conduct our hearings in the ordinary course.

And so I am not sure that the mechanism of an independent body that is all on its own is exactly the right one, but I am firmly in your camp that improving that ability for the FISA Court to have a broader range of views presented to it and to build in the adversary process is an important step in the right direction.

Senator BLUMENTHAL. Thank you. I appreciate those comments and your questions earlier, and I want to say that this is a very difficult and challenging issue or set of issues, and I really appreciate the testimony that has been given by this panel. I have been enlightened by the somewhat adversarial exchanges here with some of you, and I think that the subject bears a lot more thought and consideration. I would invite each of you to submit additional comments and hope that I can consult with you, because you bring a set of experiences as well as expertise that I think will be very valuable as we move forward, and particularly to my colleagues, I will encourage them as well to consider all of your views.

So thank you for being here. Thank you for your excellent testimony. This hearing is adjourned. We will keep the record open for 10 days, and please submit additional comments if you have any.

Thank you very much.

[Whereupon, at 1:38 p.m., the Committee was adjourned.]

[Additional material submitted for the record follows.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

UPDATED Witness List

Hearing before the
Senate Committee on the Judiciary

On

"Continued Oversight of the Foreign Intelligence Surveillance Act"

Wednesday, October 2, 2013
Dirksen Senate Office Building, Room 226
10:00 a.m.

Panel I

The Honorable James R. Clapper
Director of National Intelligence
Washington, DC

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

Panel II

Laura K. Donohue
Professor of Law, Georgetown Law
Director, Georgetown's Center on National Security and the Law
Washington, DC

Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University
Director, Center for Information Technology Policy
Princeton, NJ

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

JOINT STATEMENT FOR THE RECORD
OF

JAMES R. CLAPPER
DIRECTOR OF NATIONAL INTELLIGENCE

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

BEFORE THE
SENATE COMMITTEE ON THE JUDICIARY

OCTOBER 2, 2013

Joint Statement for the Record
of

James R. Clapper
Director of National Intelligence

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

Before the
Senate Committee on the Judiciary

October 2, 2013

Thank you for inviting us to discuss the Administration's efforts to enhance public confidence in the important intelligence collection programs that have been the subject of unauthorized disclosures since earlier this year: the collection of bulk telephony metadata under the business records provision found in section 215 of the USA PATRIOT Act, and the targeting of non-U.S. persons overseas under section 702 of FISA. We remain committed, as we review these activities, both to ensuring that we have the authorities we need to collect important foreign intelligence to protect the country from terrorism and other threats to national security, and to protecting privacy and civil liberties in a manner consistent with our values. We also remain committed to working closely with this Committee as any modifications to these activities are considered. We understand that some of the initiatives announced by the President in his

statement on August 9 are of interest to the Committee, and we welcome the opportunity to discuss them with you and to work together in moving forward.

The first step in promoting greater public confidence in these intelligence activities is to provide greater transparency so that the American people understand what the activities are, how they function, and how they are overseen. As you know, many of the reports appearing in the media concerning the scope of the Government's intelligence collection efforts have been inaccurate, including with respect to the collection carried out under sections 215 and 702. In response, the Administration has released substantial information since June to increase transparency and public understanding, while also working to ensure that these releases are consistent with national security.

We have worked to provide the public greater insight into the operation of the bulk telephony metadata business records collection program under section 215. In early June, the Director of National Intelligence (DNI) released a public statement explaining that the program is carried out only pursuant to orders of the Foreign Intelligence Surveillance Court (FISC) and is subject to executive, judicial, and Congressional oversight. The DNI emphasized that, under this program, we do not collect the content of any telephone calls or any information identifying the callers, nor do we collect cell phone locational information. Rather, the Government obtains business records created and retained by telecommunication companies for their own internal purposes, such as billing. The DNI also explained that the Government is authorized to query the bulk metadata only when there is a reasonable, articulable suspicion, based on specific facts, that the identifier—e.g., a telephone number—used to query the data is associated with a foreign terrorist organization previously approved by the FISC. Subsequently, the DNI declassified and

released the FISC's primary order that accompanied the secondary order that had been disclosed in the media, so that the American people could have a more complete picture of the legal parameters under which this activity occurs and the extensive oversight that the FISC requires. The primary order confirms that the Government must adhere to strict limitations on querying, retaining, and disseminating the business records acquired through this program. The Director of NSA also released information concerning the value of the bulk telephony metadata collection program in support of a number of counterterrorism investigations.

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

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

In August, the DNI declassified and released three opinions from the FISC concerning the section 702 program. As was the case with the section 215 opinions, these opinions concerned a significant compliance incident that caused the Court to criticize the manner in which the section 702 program was being carried out. And, similarly, these opinions provide the

public with considerable insight into the nature and functioning of section 702 collection, while also displaying the detailed and intricate extent of the FISC's review. Indeed, while the FISA statute describes the basic procedures by which the Intelligence Community seeks various authorizations from the FISC, the opinions released reveal fully the thorough, thoughtful, independent review that the FISC provides.

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

Overall, this is a lot of activity for three months. As we have worked toward greater transparency, we have been mindful of the need to protect intelligence sources and methods. Unfortunately, because of the unauthorized disclosures, a great deal of information that was previously classified about these intelligence programs is now in the public domain. These unauthorized disclosures have already caused significant harm to national security, and

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

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

In his speech in August, President Obama also announced the establishment of a Review Group on Intelligence and Communications Technologies. The Review Group's task is to advise the President "on how, in light of advancements in technology, the United States can employ its

technical collection capabilities in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure." The group is charged with conducting an independent review and will report to the President. Group members have received briefings from Administration officials and have met with privacy and civil liberties experts, as well as information technology companies and experts. The group will also be soliciting public comments. The Review Group has been directed to submit an interim report to the President within 60 days and a final report by the end of the year.

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

Moreover, as the President discussed in his August 9 statement, the executive branch stands ready to work with Congress to pursue appropriate reforms to section 215, to discuss certain changes to practice before the FISC to ensure that civil liberties concerns have an independent voice in appropriate cases, and to consider efforts at strengthening the transparency of these and other intelligence activities, all in ways consistent with protecting national security. Regarding section 215, we are open to a number of ideas that have been proposed in various quarters to address concerns about the business records program. For example, we would consider statutory restrictions on querying the data that are compatible with operational needs, including perhaps greater limits on contact chaining than what the current FISC orders permit.

We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced oversight and transparency measures, such as annual reporting on the number of identifiers used to query the data. To be clear, we believe the manner in which the bulk telephony metadata collection program has been carried out is lawful, and existing oversight mechanisms protect both privacy and security. However, there are some changes that we believe can be made that would enhance privacy and civil liberties as well as public confidence in the program, consistent with our national security needs.

On the issue of FISC reform, we believe that the *ex parte* nature of proceedings before the FISC is fundamentally sound and has worked well for decades in adjudicating the Government's applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA. However, we understand the concerns that have been raised about the lack of independent views in certain cases, such as cases involving bulk collection, that affect the privacy and civil liberties interests of the American people as a whole. Therefore, we would be open to discussing legislation authorizing the FISC to appoint an *amicus*, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons. Establishing a mechanism whereby the FISC could solicit independent views of an *amicus* in a subset of cases that raise broader privacy and civil liberties questions, but without compromising classified information, may further assist the Court in making informed and balanced decisions and may also serve to enhance public confidence in the FISC process.

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

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

We look forward to working with you on these important issues, and we remain grateful for this Committee's support for these particular intelligence collection programs, which we continue to believe play an important role in our broader foreign intelligence collection efforts. We hope that, with the assistance of this Committee, we can ensure that these programs are on

the strongest possible footing, from the perspective of both national security and privacy, so that they will enjoy broader public and Congressional support in the future. Thank you.

Opening Statement of GEN Keith B. Alexander, Director, NSA
before the Senate Committee on the Judiciary
2 October 2013

- Chairman Leahy, Ranking Member Grassley, distinguished members of the Committee, thank you for the opportunity to provide opening remarks.

- I am privileged today to represent the work of the dedicated professionals at the National Security Agency who employ the authorities provided by Congress, the federal courts and the Executive Branch to help protect the nation and protect our civil liberties and privacy.

- If we are to have an honest debate about how NSA conducts its business, we need to step away from sensationalized headlines and focus on facts.

- Our mission is defend the nation and to protect our civil liberties and privacy. Ben Wittes from the Brookings Institution said about the media leaks and specifically about these two FISA programs: "shameful as it is that these documents were leaked, they actually should give the public great confidence in both NSA's internal oversight mechanisms and in the executive and judicial oversight mechanisms outside the Agency. They show no evidence of any intentional spying on Americans or abuse of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures on the part of the NSA. And they show an earnest, ongoing dialogue with the FISA court over the parameters of the Agency's legal authority and a commitment both to keeping the court informed of activities and to complying with its judgments on their legality."

- Today I'd like to present facts to specifically address:

  - Who we are in terms of both our mission and our people;

  - What we do: adapt to technology and the threat; take direction from political leadership; operate strictly within the law and consistent with explicit intelligence priorities; and ensure compliance with all constraints imposed by our authorities and internal procedures;

  - What we have accomplished specifically for our country with the tools we have been authorized; and

  - Where do we go from here?

<u>Who We Are – Our Mission</u>

- NSA is a foreign intelligence agency with two missions:

  - We collect foreign intelligence of national security interest and

  - We protect certain sensitive information and U.S. networks.

- All this while protecting our civil liberties.

- NSA contributes to the security of our nation, its armed forces, and our allies.

- NSA accomplishes this mission, while protecting civil liberties and privacy – because the constitution we are sworn to protect and defend makes no allowances to trade one for the other.

- NSA operates squarely within the authorities granted by the president, congress and the courts.

Who We Are – Our People

- I'm proud of what NSA does and more proud of our people.
  - National Security Agency employees take an oath to protect and defend the constitution of the United States of America.
  - They have devoted themselves to protecting our nation.
  - Just like you, they will never forget the moment terrorists killed 2,996 Americans in New York, Pennsylvania, and the Pentagon.
  - They witnessed the first responders' efforts to save lives. They saw the military shift to a wartime footing. They committed themselves to ensuring that another 9/11 would not happen and our deployed forces would return home safely.
  - In fact, they deploy with our armed forces into areas of hostility.
    - More than 6,000 deployed in support of operations in Iraq, Afghanistan, and CT.
    - 22 paid the ultimate sacrifice since 9/11; sadly adding to a list of NSA/CSS personnel numbering over 170 killed in the line of duty since NSA's formation in 1952.
    - Theirs is a noble cause.
- NSA prides itself on its highly skilled workforce.
  - We are the largest employer of mathematicians in the U.S. (1,013).
  - 966 PhDs and 4,374 computer scientists.
  - Linguists in more than 120 languages.
  - More patents than any other Intelligence Community agency and most businesses.
  - They are also Americans and they take their privacy and civil liberties seriously.

What We Do – Adapt to Technology and the Threat

- Today's telecommunications system is literally one of the most complex systems ever devised by mankind.
- The fact that over 2.5 billion people all connect and communicate across a common infrastructure is a tribute to the ingenuity of mankind. The stark reality is that terrorists, criminals and adversaries make use of the same infrastructure.
- Terrorists and other foreign adversaries hide in the same global network, use the same communications networks as everyone else, and take advantage of familiar services: Gmail, Facebook, Twitter, etc. Technology has made it easy for them.
- We must develop and apply the best analytic tools to succeed at our mission; finding the communications of adversaries while protecting those of innocent people, regardless of their nationality.

What We Do – Take Direction from Political Leadership (NIPF)

- NSA's direction comes from national security needs, as defined by the nation's senior leaders.
- NSA does not decide what topics to collect and analyze.
- NSA's collection and analysis is driven by the national intelligence priorities framework and received in formal tasking.
- We do understand that electronic surveillance capabilities are powerful tools in the hands of the state. That's why we have extensive mandatory internal training, automated checks, and an extensive regime of both internal and external oversight.

What We Do – Use Lawful Programs and Tools to Do Our Mission

- The authorities we have been granted and the capabilities we have developed help keep our nation safe.
- Since 9/11 we have disrupted terrorist attacks at home and abroad using capabilities informed by the lessons of 9/11.
- The Business Records FISA program, NSA's implementation of Section 215 of the PATRIOT Act, focuses on defending the homeland by linking the foreign and domestic threats.
- Section 702 of FISA focuses on acquiring foreign intelligence, including critical information concerning international terrorist organizations, by targeting non-U.S. persons who are reasonably believed to be located outside the United States.

- NSA also operates under other sections of the FISA statute in accordance with the law's provisions (such as Title 1 and Section 704).

- It is important to remember that in order to target a U.S. person anywhere in the world under the FISA statute, we are required to obtain a court order based on a probable cause showing that the prospective target of the surveillance is a foreign power or agent of a foreign power.

- NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO) 12333.

- As I have said before, these authorities and capabilities are powerful; we take this responsibility seriously.

What We Do – Ensure Compliance

- We stood up a Director of Compliance in 2009 and repeatedly train our entire workforce in privacy protections and the proper use of capabilities.

- We do make mistakes. The vast majority of compliance incidents reflect the challenge of implementing very specific rules in the context of ever-changing technology.

- Compliance incidents, with very rare exception, are unintentional and reflect the sort of errors that will occur in any complex system of technical activity.

- The press claimed evidence of "thousands of privacy violations."

- This is false and misleading.

- According to NSA's independent Inspector General, there have been only 12 substantiated cases of willful violation over 10 years – essentially one per year from a population of NSA/CSS personnel numbering in the tens of thousands. But the relatively small number of cases does not excuse any infraction of the rules. We took action in every case referring several to the department of justice for potential prosecution; appropriate disciplinary action was taken in others.

- We hold ourselves accountable every day.

- Most of these cases involved improper tasking or querying regarding foreign persons in foreign places.

- I am not aware of any intentional or willful violations of the FISA statute, which is designed to be most protective of the privacy interests of U.S. persons.

- Of the 2,776 incidents noted in the press from one of our leaked annual compliance reports, about 75% are not violations of approved procedures at all but rather NSA's detection of valid foreign targets that travel to the U.S. and a record that NSA stopped collecting, in accordance with the rules (roamers).

- Let me also start to clear the air on actual compliance incidents.
- The vast majority of the actual compliance incidents involve foreign locations and foreign activities, as our activities are regulated by specific rules wherever they occur.
- For the smaller number that did involve a U.S. person, a typical incident involves a person overseas involved with a foreign organization who is subsequently determined to be a U.S. person. All initial indications and research before collection point the other way, but NSA constantly re-evaluates indications.
- NSA detects and corrects and – in most cases – does so before any information is even obtained, used, or shared outside of NSA.
- Despite the difference, between willful and not, we treat incidents the same: we detect, we address, we remediate – including removing or purging information from our databases in accordance with the rules. And we report.
- We hold ourselves accountable and keep others informed so they can do the same.
- On NSA's compliance regime Ben Wittes said at last Thursday's Intelligence Committee hearing: "but one thing we have learned an enormous amount about is the compliance procedures that NSA uses. They are remarkable. They are detailed. They produce data streams that are extremely telling – and, to my mind, deeply reassuring."(26 September)
- We welcome an ongoing discussion about how the public can, going forward, have increased information about NSA's compliance program and its compliance posture, much the same way all three branches of the government have today. From our perspective, additional measures that will increase the public's confidence in these authorities and our use of them, can and should be open for discussion.

<u>What We have Accomplished for Our Country</u>

- NSA's existing authorities and programs have helped "connect the dots," working with the broader Intelligence Community and homeland and domestic security organizations, for the good of the nation and its people.
- NSA's programs have contributed to understanding and disrupting 54 terror related events: 25 in Europe, 11 in Asia, 5 in Africa, and 13 related to the homeland.
- This was no accident nor coincidence.
- These were direct results of a dedicated workforce, appropriate policy, and well scoped authorities created in the wake of 9/11 to make sure 9/11 never happened again.

- This is not the case in other countries. In the week ending 23 September there were 972 terror-related deaths in Kenya, Pakistan, Afghanistan, Syria, Yemen and Iraq. [Kenya, 62; Pakistan, 75; Afghanistan, 18; Syria, 504; Yemen, 50; and Iraq, 263].

- Another 1,030 were injured in the same countries.

- We need these types of programs to protect against having these types of statistics on our soil.

- NSA's global system is optimized for today's technology on a global network.

- Our analytic tools are effective at finding terrorist communications in time to make a difference.

- This global system and analytic tools are also what we need for cybersecurity.

- This is how we see in cyberspace, identify threats there, and defend networks.

Reforms

- On 9 August the President laid out some specific steps to increase the confidence of the American people in our foreign intelligence collection programs.

- We are always looking for ways to better protect privacy and security. We have improved over time our ability to reconcile our technology with our operations and with the rules and authorities. We will continue to do so as we go forward and strive to improve how we protect the American people – their privacy and security.

- Regarding NSA's telephone metadata program, 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 – privacy and civil liberties are protected.

  - Agility – queries can be made in a timely manner so that, in the most urgent cases, results can support disruption of imminent terrorist plots.

  - Duration – terrorist planning can extend for years, so the metadata repository must extend back for some period of time in order to discover terrorist plans and disrupt plots.

  - Breadth – repository of metadata is comprehensive enough to ensure query responses can indicate with high confidence any connections a terrorist-associated number may have to other persons who may be engaged in terrorist activities.

- As you consider changes in metadata storage location, length of storage, who approves query terms, and the number of hops, we must preserve these foundational attributes of BR FISA.

- Similarly as you entertain reforms to the FISC, operational and practical considerations must be weighed so that there are no inherent delays; emergency provisions are maintained; and any reform to the FISC structure is respectful of the nature of classified information.

Conclusion

- NSA looks forward to supporting the discussion of reforms. Whatever changes are made, we will exercise our authorities dutifully, just as we have always done.

- The leaks of classified NSA and partner information will change how we operate and what people know about us.

- However, the leaks will not change the ethos of the NSA workforce, which is dedicated to finding and reporting the vital intelligence our customers need to keep the nation safe, in a manner that is fully compliant with the laws and rules that authorize and limit NSA's activities and sustain the privacy protections that we as a nation enjoy.

- I look forward to answering your questions.

Oral Remarks Prepared for the Oct. 2, 2013 Hearing on
Continued Oversight of the Foreign Intelligence Surveillance Act
Senate Committee on the Judiciary

Professor Laura K. Donohue
Georgetown Law

Thank you for inviting me to discuss the NSA's collection of telephony metadata under Section 215 and its acquisition of international communications under Section 702. It is my view that the bulk collection of U.S. citizens' metadata is illegal and unconstitutional. I have submitted more detailed written remarks for the record. For now I will highlight what I see as the most pressing concerns.

I. Unconstitutionality of Bulk Collection

The government argues that the telephony metadata collection program complies with the Constitution. In doing so, it relies, in part, on a case called *Smith v. Maryland*, in which the court held that participants in telephone calls lack a reasonable expectation of privacy in the telephone numbers dialed and received on one's phone. The government also argues that the national security interests at stake override whatever privacy intrusion arises from the bulk collection of metadata. For two reasons, these arguments are problematic.

First, the telephony metadata program amounts to a general warrant, the use of which by the English played a key role in the American Revolution and led directly to the creation of the Fourth Amendment.

A general warrant was a writ, issued by a court, that did not expire and that allowed officials to collect information and to search anywhere, without any

particularized suspicion. In 1760 British Prime Minister William Pitt directed the colonial governors to use such writs of assistance to crack down on illegal behavior. In one of the most famous orations in American history, James Otis challenged such "instruments of slavery on one hand and villainy on the other". He considered them "the worst instrument of arbitrary power", in part because no prior evidence of wrongdoing need be involved in their execution. John Adams, who was present at the time, later wrote that Otis' remarks "breathed into this nation the breath of life." "Then and there," Adams reported, "was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."

The Virginia Declaration of Rights subsequently included a clause (Article 10), outlawing "general warrants, whereby an officer. . . may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence." Similar language was adopted by Massachusetts and New Hampshire in their state Constitutions. Some of the most important ratifying conventions (Virginia, New York, and North Carolina) required that a prohibition on general warrants be incorporated into the Bill of Rights in order for the states to agree to the U.S. Constitution. Accordingly, James Madison wrote the Fourth Amendment to prevent the use of general warrants in the future. They were the very definition of "unreasonable search and seizure."

The FISC Order authorizing the telephony metadata program is a general warrant. It authorizes the government to collect and then to rummage through our papers and effects in the hope of finding wrongdoing. There is no previous suspicion of criminal activity

required. FISC admits that almost none of the information obtained relates to illegal behavior.

It matters little whether one stores ones papers in a filing cabinet in one's den, or places documents on the iCloud—the digital equivalent, in modern times, of a filing cabinet. The sheer volume of information we manage in our daily affairs requires individuals to arrange for storage of everything from medical records to family photos. Email, in turn, holds our correspondence—papers that we place on a server with a company with whom we have a contractual relationship. Banking records may be similarly accessible over the Internet.

This is our modern day equivalent of papers and effects, and allowing the government to obtain records of all of this information is the equivalent of a digital trespass on our private lives. The trespass in which the NSA is engaging is not supported by probable cause, it is not even supported by reasonable suspicion—indeed, no suspicion of any wrongdoing whatsoever is contemplated by the collection of myriad records of all U.S. persons. It is the equivalent of a general warrant and, as such, it is odius to the Fourth Amendment.

Second, in defending the telephony metadata program, the government relies on the Court's construction of a reasonable expectation of privacy in *Katz v. United States* (1967) and argues that, consistent with *Smith v. Maryland* (1979), third party information is not constitutionally-protected. This argument fails to appreciate the facts of *Smith* and the manner in which society now operates. It also ignores a more recent case, *U.S. v. Jones* (2012), which suggests that the Supreme Court is poised to re-evaluate the level of

protection afforded to U.S. citizens' right to privacy, consistent with the Fourth Amendment.

First, the facts. On March 5, 1976, a woman, Patricia McDonough, was robbed in Baltimore. After giving the police a description of the man who assaulted her and a 1975 Monte Carlo car she had seen near the scene of the crime, she started receiving threatening and obscene phone calls in her home from a man who identified himself as the robber. At one point, the caller told her to go out on her front porch. When she did so, she saw the Monte Carlo driving slowly past her house. On March 16, the police observed a car of the same description in her neighborhood. Tracing the license plate, police discovered that the car was registered to Michael Lee Smith. The following day, the police asked the telephone company to install a pen register to trace the numbers called from Smith's home telephone. The company voluntarily consented, and that day Smith called Patricia McDonough's home. On the basis of this and other information, the police applied for and obtained a search warrant. Upon executing the warrant, police found a telephone book in Smith's home, with the corner turned down to Patricia McDonough's name and number. In a subsequent six-man lineup, McDonough identified Smith as the person who robbed her.

Michael Lee Smith had robbed, threatened, intimidated, and harassed Patricia McDonough. The police, accordingly, placed a pen register, consistent with their reasonable suspicion that Michael Lee Smith was engaged in criminal wrongdoing.

The NSA would treat every American as though they were Michael Lee Smith.

And it would collect not just the numbers dialed from the home of a suspected criminal, but all law-abiding citizens' metadata: whom we call, who calls us, how long

we talk, and where we are located when we do so. Calls to a rape crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in *Smith*.

And the NSA would do this indefinitely.

The sheer amount of information available is significantly different from what was at stake in the pen register placed for a 24-hour period on Michael Lee Smith's line.

Let us be clear: it is not just telephony metadata that is of issue. The government's argument could be extended to any sort of metadata—email, banking records, Internet usage, financial transactions—the list continues. The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed in 1979. Resultantly, the extent of information that can be learned about not just individuals, but towns, neighborhoods, school boards, political parties, girl scout troops—indeed, any social, political, or economic network, is light years ahead of what the Court contemplated at the time.

Americans reasonably expect that their movements, communications, and decisions will not be recorded and analyzed by the government. A majority of the Supreme Court seems to agree.

In 2012 the Court considered a case involving 28-day surveillance. The government had obtained a search warrant permitting it to place a Global-Positioning System (GPS) tracking device on a car registered to the wife of a suspected drug dealer. The day after the warrant expired, agents installed the device and followed the car's movements for nearly a month. Information obtained allowed the government to indict

Antoine Jones and others on drug trafficking conspiracy charges. The Supreme Court held that attaching the GPS device to the car and tracing its movements amounted to a search within the meaning of the Fourth Amendment.

This case is important for determining the constitutionality of the telephony metadata program in two important ways. First, it recognized that *Katz's* reasonable expectation of privacy test did not supplant the rights in existence at the time the Fourth Amendment was forged. "[A]t a minimum," Justice Scalia wrote, the "18th century guarantee against unreasonable searches. . . . must provide. . . the degree of protection it afforded when it was adopted." The protection against the use of general warrants thus stands.

Second, at least five justices indicated unease with the intrusiveness of modern technology. Justice Samuel Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investigations, long-term monitoring "impinges on expectations of privacy." Justice Sotomayor went one step further. She suggested that, in light of the level of intrusiveness represented by modern technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." She noted:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to the cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

Disclosing information to a member of the public for a limited purpose does not divest that data of Fourth Amendment protection.

II. ILLEGALITY

The telephony metadata program also violates the express statutory language of the Foreign Intelligence Surveillance Act in at least three ways: first, with regard to the language "relevant to an authorized investigation"; second, in relation to the requirement that the information sought must be otherwise obtainable via subpoena duces tecum; and third, in its violation of the restrictions specifically placed on pen registers and trap and trace equipment.

First, the relevance standard. The government argues that the NSA's telephony metadata program is consistent with the language of 50 U.S.C. § 1861 in that *all* telephone calls in the United States, including those of a wholly local nature, are "relevant" to foreign intelligence investigations.

This use of the word "relevant" is so absurd as to render the term – and the qualifying statutory language – meaningless.

The statute requires, for instance, that there be "reasonable grounds" to believe that the records being sought are relevant. Although FISA does not define "reasonable grounds", it has been treated as the equivalent of "reasonable suspicion". This standard requires a showing of "specific and articulable facts, which, taken together with rational inferences from those facts, reasonably warrant" an intrusion into an individual's right to privacy.

According to Verizon Communications News Center, as of last year, the company has 107.7 million wireless customers, connecting an average of 1 billion calls per day. There is simply no way that the government provided specific and articulable facts relevant to each one of those customers or calls, sufficient to establish reasonable grounds to establish their relevance. The government is thus interpreting "relevant" in a manner that makes the qualifying condition of "reasonable grounds" obsolete.

The government's interpretation is so broad that it establishes a dangerous precedent. If all telephony metadata is relevant to foreign intelligence investigations, then so is all email metadata, and all GPS metadata, all financial information, all banking records, all social network participation, and all Internet use. Indeed, FISC has hinted that there may be other, similar programs, and on September 28, 2013, the *New York Times* reported that the NSA began allowing analysis of phone call and email logs in November 2010 to begin examining American's networks of associations. If all telephony metadata is relevant, then so is all other data—which means that very little would, in fact, be irrelevant to such investigations. If this is the case, then such an interpretation radically undermines not just the limiting language in the statute, but the very purpose for which Congress introduced FISA in the first place.

FISA, in addition, specifically contemplates the use of such information for use in an "authorized investigation". This suggests a particularized, currently existing investigation. The FISC Order, in contrast, directs the collection of data for use in "authorized investigations"—both now and into the future. How could the court possibly anticipate that the data will be relevant to investigations not yet approved?

The second source of statutory illegality relates to the requirement that tangible goods subject to an order under Section 215 "can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."

There is no way, however, that any grand jury or court would allow the bulk collection of all Americans' metadata. It would be the equivalent of a grand jury being convened in Arlington, Virginia, and issuing a subpoena "just to find out what is going on." Such fishing expeditions are patently illegal. Subpoenas, moreover, are specific in that they relate to a particular individual or crime, and they deal with current or past bad behavior. The telephony metadata program, in contrast, is broad, non-specific, not tied to any particular crime, and forward-looking, with the aim of anticipating future acts.

Remarkably, FISC itself has recognized the illegality of the program. In March 2009 Judge Reggie Walton wrote:

> Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (U.S.) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata *could not otherwise be legally captured in bulk*, the government proposed stringent minimization procedures that strictly controlled the acquisition, accessing, dissemination, and retention of these records by the NSA and FBI.

By acknowledging that the metadata "could not otherwise be legally captured in bulk", Walton recognized that the program violated the statute. Nevertheless, the court had approved it based, in part, upon "the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States." So, the government had promised that it was important for U.S. national security—therefore, FISC agreed to allow the program to continue.

Third, and finally, as a statutory matter, all of the information at issue in the bulk collection program is already provided for in subchapter three, relating to pen registers and trap and trace equipment. Using subchapter four, the government appears to be doing an end run around the restrictions that would otherwise apply.

III. Concluding Remarks

In conclusion, I would just like to underscore that the system is badly broken. The NSA is engaging in activities that are both illegal and unconstitutional. Congress has been given an opportunity to fix the problem, and to do so in a way that recognizes the benefits of new technologies, the real threats that the nation faces, and the demands of the U.S. Constitution. I would be happy to discuss possible ways in which this could be done in more detail. Thank you for your time.

Remarks Prepared for the Oct. 2, 2013 Hearing on
Continued Oversight of the Foreign Intelligence Surveillance Act
Senate Committee on the Judiciary

Professor Laura K. Donohue
Georgetown Law

I. INTRODUCTION

Congress introduced the 1978 Foreign Intelligence Surveillance Act to make use of new technologies and to enable the intelligence community to obtain information vital to U.S.

national security, while preventing the National Security Agency and other federal intelligence-gathering entities from engaging in broad domestic surveillance. The legislature sought to prevent a recurrence of the abuses of the 1960s and 1970s that accompanied the Cold War and the rapid expansion in communications technologies.

Congress purposefully circumscribed the NSA's authorities by limiting them to foreign intelligence gathering. It required that the target be a foreign power or an agent thereof, insisted that such claims be supported by probable cause, and heightened the protections afforded to the domestic collection of U.S. citizens' information. Initially focused on electronic surveillance, the Foreign Intelligence Surveillance Act gradually expanded over time to incorporate physical searches, pen registers and trap and trace, and business records and tangible goods. The addition of these provisions took place within the same general framing that Congress had adopted in enacting the legislation in the first place.

Documents related to the recently revealed telephony metadata program, conducted under the auspices of the Foreign Intelligence Act and its subsequent amendments, suggests that the National Security Agency is now interpreting the statutory provisions in a manner directly contrary to Congress' intent. It reflects neither the particularization required by Congress prior to acquisition of information, nor the role anticipated by Congress for the Foreign Intelligence Surveillance Court and Court of Review.

The specific legal reasoning offered in defense of the program, moreover, violates the statutory language in three important ways: (a) it contradicts the requirement the records sought "are relevant to an authorized investigation"; (b) it violates the statutory provision that requires that information sought could be obtained via subpoena duces tecum; and (c) it bypasses the statutory framing for pen registers and trap and trace devices. In addition, the program raises serious constitutional concerns. The FISC order amounts to a general warrant, which the Fourth Amendment is designed to preclude. Efforts by the government to save the program on grounds of third party doctrine are similarly unpersuasive in light of the unique circumstances of *Smith v. Maryland*, new technologies, and changed circumstances. An end to the telephony metadata program and FISA reform are necessary to bring surveillance operations and emerging technologies within the bounds of the Constitution.

II. ORIGINS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

In the early 1970s, a series of news stories broke detailing the existence of covert domestic surveillance programs directed at U.S. citizens. These revelations led, *inter alia*, to the creation of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Chaired by Senator Frank Church, the Committee uncovered a range of deeply concerning domestic surveillance operations, prompting Congress to pass the Foreign Intelligence Surveillance Act.

A. Initial Revelations

One of the first public indications that the executive branch was engaging in broad domestic intelligence gathering came in January 1970. Writing in the *Washington Monthly*, Christopher Pyle charged that the Army was engaged in the surveillance of American citizens.[1] The following year, an organization calling itself the Citizens' Commission to Investigate the FBI broke into a two-person FBI office in Media, Pennsylvania, stealing 1000 classified documents, all of which WIN Magazine

[1] Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, WASHINGTON MONTHLY, Jan. 1, 1970, at 4, *reproduced in* 91 CONG. REC. 2227-2231 (1970).

subsequently published.[2] A code word on these documents, "COINTELPRO", (for "counterintelligence program"), prompted Carl Stern, a reporter for NBC, to initiate a Freedom of Information Act lawsuit.[3] On December 6, 1973, Stern filed a story that ran on the NBC Nightly News, detailing extensive domestic surveillance and disruption undertaken by the FBI for national security purposes.[4]

Following these initial disclosures, in 1974 Seymour M. Hersh, an investigative reporter, published a detailed report in the *New York Times* that immediately captured public attention. The article stated that during the Nixon Administration the Central Intelligence Agency ("CIA") had conducted a massive intelligence operation "against the antiwar movement and other dissident groups in the United States."[5] Intelligence files on more than 10,000 Americans – including members of Congress – had been maintained by a special unit that reported directly to the Director of Central Intelligence.[6] The CIA had also engaged in dozens of other illegal operations since the 1950s, such as "break-ins, wiretapping, and the surreptitious inspection of mail."[7] One official reported that the requirement to keep files on U.S. citizens stemmed, in part, from the so-called Huston plan.[8] Agency officials claimed at the time that although directed at U.S. citizens, everything they had done had been under the auspices of foreign intelligence gathering.[9]

These new revelations came as quite a surprise, not least because the 1947 National Security Act forbade the Director of the Central Intelligence Agency from having any "police, subpoena, law enforcement powers or internal security functions."[10] The report, moreover, came on the heels of a Senate Armed Services Committee report condemning the Pentagon for spying on the White House National Security Council.

These public allegations, related to intelligence agencies' impropriety, illegal activities, and abuses of authority, prompted both Houses of Congress to create temporary committees to investigate the accusations: the House Select Committee on Intelligence, and the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.[11]

The latter, Chaired by Senator Frank F. Church (D-ID), with the assistance of Senator John G. Tower (R-TX) as Vice Chairman, was a carefully-constructed, bipartisan initiative. Its membership included eleven Senators, six drawn from the majority party and five from the minority party.[12] The Republican leadership in the Senate chose

---

[2] *The Complete Collection of Political Documents Ripped-off from the FBI Office in Media PA, March 8, 1971*, WIN MAG., Mar. 1972. Note that the original FBI files are now located at the Swarthmore College Peace Collection, Swarthmore College, Swarthmore, Pennsylvania.

[3] Memorandum from C.D. Brennan to W.C. Sullivan (Apr. 27, 1971); Letter from FBI headquarters to All SAC's (Apr. 28, 1971), *cited in* SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III: FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP NO. 94-755, at 3 (1976) *available at* http://archive.org/stream/finalreportofsel03unit#page/n3/mode/2up.

[4] 91 CONG. REC. 26,329 (1970).

[5] Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N. Y. TIMES, Dec. 22, 1974, at 1.

[6] *Id.*

[7] *Id.*

[8] *Id.* at 26. Named for Tom Charles Huston, the Presidential aide who conceived the project, the plan called for the use of burglaries and wiretapping to counter antiwar activities and student turmoil ostensibly "fomented" by black extremists. President Nixon and senior officials claimed that it had never been implemented.

[9] *Id.* at 26.

[10] National Security Act of 1947 § 104A(d)(1) (2013).

[11] H.R. Res. 138, 94th Cong. (1975); *replaced and expanded by* H.R. Res. 591, 94th Cong. (1975); S. Res. 21, 94th Cong. (1975).

[12] *Intelligence Activities: Hearing on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States,* 94th Cong. ii (1975).

legislators representing a range of views within their party, as did the Democratic leadership.[13] Further thought was given to diversity of experience, incorporating both senior members of the Senate, as well as some of the most junior members—including one Senator, who had only begun his service a few weeks prior to the formation of the committee.[14] The Senate overwhelmingly supported the establishment of the Select Committee, endorsing its creation by a vote of 82-4.[15]

The Senate directed the committee to do two things: first, to investigate "illegal, improper, or unethical activities" in which the intelligence agencies engaged; and, second, to determine the "need for specific legislative authority to govern" the NSA and other agencies.[16] The Church Committee subsequently took testimony from hundreds of people, inside and outside of government, in public and private hearings. The NSA, FBI, CIA, IRS, Post Office, and other federal agencies submitted documents. In 1975 and 1976 the Committee issued seven reports and 6 supplemental volumes, classifying another 60 reports for future release.[17]

The committee found that broad domestic surveillance programs, conducted under the guise of foreign intelligence collection, had undermined the privacy rights of U.S. citizens.[18] The NSA figured largely in these concerns.

B. NSA Domestic Surveillance

Although the NSA maintained a definition of foreign intelligence that focused on threats external to the United States, a key contributor to the agency's decision to intercept Americans' communications was the question of whether the definition of foreign communications prevented the acquisition, or merely the analysis, of information not related to foreign intelligence. The NSA adopted—and the Church committee rejected—the latter approach.

In October 1952, President Truman issued a classified memo that laid out the future of U.S. signals intelligence and created the NSA.[19] Truman's aim was to (a) strengthen U.S. signals intelligence capabilities, (b) support the country's ability to wage war, and (c) generate information central to the conduct of foreign affairs.[20] The NSA's mission, accordingly, was to obtain foreign intelligence from foreign electrical communications.[21]

From the beginning, the agency understood foreign intelligence to involve the interception of communications wholly or partly outside the United States and not

---

[13] Interviews with Senator Walter Mondale and Senator Gary Hart, Washington, D.C. (Sept. 23, 2013).
[14] *Id.*
[15] 121 CONG. REC. 1416-34 (1975).
[16] S. Res. 21, 94th Cong. (1975).
[17] Interview with Senator Gary Hart, Washington, D.C. (Sept. 24, 2013). Since 1992, another 50,000 pages of the records have been declassified and made publicly available at the National Archives. History Matters, *Rockefeller Commission Report*, *available at* http://history-matters.com/archive/contents/church/contents_church_reports_rockcomm.htm; Press Release, National Security Agency Central Security Service, The National Security Agency Releases Over 50,000 Pages of Declassified Documents (June 8, 2011), http://www.nsa.gov/public_info/press_room/2011/50000_declassified_docs.shtml.
[18] *Intelligence Activities: Hearing on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong. vol. 1-7 (1975).
[19] Presidential Memorandum, Oct. 29, 1952, *amending* National Security Council Intelligence Directive No. 9, Mar. 10, 1950 (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195).
[20] 5 *Intelligence Activities: Hearings on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong. 9 (1975) (hereinafter *Church Committee Report, Vol. 5*). For an informative discussion of MI-8 and the NSA's predecessor agencies, see HOUSE COMM. ON GOV'T OPERATIONS, INTERCEPTION OF INTERNATIONAL TELECOMMUNICATIONS BY THE NATIONAL SECURITY AGENCY (DRAFT REPORT) 1-12, *available at* http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=14.
[21] *Id.* at 6 (statement of General Lew Allen, Jr., Director, National Security Agency).

targeted at U.S. persons. Neither the Presidential directive of 1952, nor the National Security Council Intelligence Directive ("NSCID") No. 6, which authorized the CIA to engage in Foreign Wireless and Radio Monitoring, defined the term "foreign communications."[22]

NSCID 9, however, entitled Communications Intelligence, defined "foreign communications" as "all communications and related materials . . . of the government and/or their nationals or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor." It included "all other telecommunications and related material of, to, and from a foreign country which may contain information of military, political, scientific or economic value."[23] "Foreign communications" thus turned upon the nature of the entity engaged in communications: i.e., a foreign power, or an individual acting on behalf of a foreign power.

The NSA did not (indeed, could not) discuss NSCID 9 during the Church Committee's public hearings. However, the Director of Central Intelligence had issued a directive that the NSA did discuss, which employed a definition of foreign communications that *excluded* communications between U.S. citizens or entities.[24] In keeping with these understandings, the NSA ostensibly focused on communications conducted wholly or partly outside the United States and not targeted at U.S. persons. The distinction was drawn, however, at the point of analysis—not the point of communication.

Testifying in 1975 before the Church Committee, NSA Director Lieutenant General Lew Allen, Jr. could thus assert that the NSA did not at that time, nor had it (with one exception—i.e., individuals whose names were contained on the NSA's watch list) "conducted intercept operations for the purpose of obtaining the communications of U.S. citizens."[25] Whether such communications were incidentally intercepted, however, was another matter: "some circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location."[26]

Central to Allen's assertion was the understanding that, to constitute foreign communications, and to legitimate the collection of information on U.S. citizens, the target of the surveillance must be a foreign power, or an agent of a foreign power, and at least one party to the communications must be outside the country.

Importantly, the Senate considered this approach, in light of the broad swathes of information obtained about U.S. citizens, to run afoul of the Fourth Amendment. Two NSA programs, in particular, generated significant concern. The first, Project MINARET, introduced to collect foreign intelligence information, ended up intercepting hundreds of U.S. citizens' communications. The second, Operation SHAMROCK, involved the large-scale collection of U.S. citizens' communications from Private Companies.

---

[22] NSCID No. 6 (Dec. 12, 1947) (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lott 66 D 148, Dulles-Jackson-Correa Report, Annex 12); *see also Church Committee Report, Vol. 5, supra*, at 6.

[23] NSCID No. 9 (Jul. 1, 1948) (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195); *see also* NSCID No. 9, Mar. 10, 1950, *supra*.

[24] *Church Committee Report, Vol. 5, supra*, at 9.

[25] *Id.*

[26] *Id.*

1. Project MINARET

In the late 1960s, the NSA, like the Internal Revenue Service ("IRS"), the FBI, and the CIA, constructed a list of U.S. citizens and non-U.S. citizens subject to surveillance.[27] The program, which operated 1967-1973, started out by narrowly focusing on the international communications of U.S. citizens traveling to Cuba. It quickly expanded, however, to include individuals (a) involved in civil disturbances, (b) suspected of criminal activity, (c) implicated in drug activity, (d) of concern to those tasked with Presidential protection, and (e) suspected of involvement in international terrorism.[28]

In 1969 the collection of information on individuals included in the watch list became known as Project MINARET.[29] When details about the program emerged, senators and members of the public expressed alarm about the privacy implications. Central to the legislators' concern was the potential for such programs to target communications of a wholly domestic nature. Senator (later Vice President) Walter Mondale, articulated the Committee's disquiet:

> Given another day and another President, another perceived risk and someone breathing hot down the neck of the military leader then in charge of the NSA: demanding a review based on another watch list, another wide sweep to determine whether some of the domestic dissent is really foreign based, my concern is whether that pressure could be resisted on the basis of the law or not . . . [W]hat we have to deal with is whether this incredibly powerful and impressive institution . . . could be used by President 'A' in the future to spy upon the American people. . . [W]e need to . . . very carefully define the law, spell it out so that it is clear what [the Director of the NSA's authority is and is not].[30]

Senator Mondale asked NSA Director General Lew Allen whether he would object to a new law clarifying that the NSA did *not* have the authority to collect domestic information on U.S. citizens. Allen indicated that he did not object.[31] FISA became the instrument designed to limit the NSA's collection of information on U.S. citizens.

2. Operation SHAMROCK

During the Senate hearings, much concern was expressed about whether to make public a second, highly classified, large-scale surveillance program run by the NSA.[32] The committee decided to discuss the program in open session on the grounds that it was both illegal and violated the Fourth Amendment.[33]

Operation SHAMROCK was the cover name given to a program in which the government had convinced three major telegraph companies (RCA Global, ITT World Communications, and Western Union International) to forward international telegraphic traffic to the Department of Defense.[34] For nearly thirty years, the NSA and its

---

[27] *Church Committee Report, Vol. 5, supra*, at 3.
[28] *Id.* at 10-11.
[29] *Id.* at 30.
[30] *Id.* at 36.
[31] *Id.* at 36.
[32] *Church Committee Report, Vol. 5, supra*, at 48-57, 60-61, 63; *see also* HOUSE COMM. ON GOV'T OPERATIONS, INTERCEPTION OF INTERNATIONAL TELECOMMUNICATIONS BY THE NATIONAL SECURITY AGENCY (DRAFT REPORT) 2-6, *available at* http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=4 (discussing pressures on the Church Committee from the House side).
[33] *Church Committee Report, Vol. 5, supra*, at 57 (statement of Senator Frank Church, Chairman, Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate).
[34] *Id.* at 57-58.

predecessors received copies of most international telegrams that had originated in, or been forwarded through, the United States.[35]

Operation SHAMROCK stemmed from wartime measures, in which companies turned messages related to foreign intelligence targets over to military intelligence. In 1947, the Department of Defense negotiated the continuation of the program in return for protecting the companies from criminal liability and public exposure.[36]

Like Project MINARET, the scope of the program gradually expanded. Initially, the program focused on foreign targets. Eventually, however, as new technologies became available, the NSA began extracting U.S. citizens' communications.[37] It selected approximately 150,000 messages per month for further analysis, distributing some messages to other agencies.[38]

Senators expressed strong concern at the resulting privacy violations, inviting the Attorney General before the Select Committee to discuss "the Fourth Amendment of the constitution and its application to the 20th century problems of intelligence and surveillance."[39] Senator Frank Church explained:

> In the case of the NSA, which is of particular concern to us today, the rapid development of technology in the area of electronic surveillance has seriously aggravated present ambiguities in the law. The broad sweep of communications interception by NSA takes us far beyond the previous fourth amendment controversies where particular individuals and specific telephone lines were the target.[40]

General Lew Allen sought to reassure the committee that although some circuits carried personal communications, the interception was "conducted in such a manner as to minimize the unwanted messages." Nevertheless, the agency might obtain many unwanted communications; it thus undertook procedures to process, sort, and analyze the relevant data. "The analysis and reporting is accomplished only for those messages which meet specified conditions and requirements for foreign intelligence."[41] Elaborating further, Allen noted, "[t]he use of lists of words, including individual names, subjects, locations, etc., has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest."[42]

The question that confronted Congress was how to limit the NSA's ability to acquire broad swathes of information up front, in the process obtaining access to private communications of individuals with no connection to foreign intelligence concerns. Congress would have to find a way to control new, sophisticated technologies, to allow intelligence agencies to perform their legitimate foreign intelligence activities, without also allowing them to invade U.S. citizens' privacy by allowing them access to information unrelated to national security.[43]

---

[35] *Id.* at 58.
[36] *Id.*
[37] *Id.* at 58-59.
[38] *Id.* at 60.
[39] *Id.* at 65.
[40] *Id.*
[41] *Church Committee Report, Vol. 5, supra*, at 19. Former CIA Director William E. Colby provided similar testimony before the Pike Committee August 6, 1975: "On some occasions, (the interception of U.S. citizens' communications) cannot be separated from the traffic that is being monitored. It is technologically impossible to separate them." *U.S. Intelligence Agencies and Activities: Intelligence Costs and Fiscal Procedures: Hearings Before the Select Committee on Intelligence U.S. House of Representatives*, 94th Cong. 241 (statement of William E. Colby, acting Director of CIA).
[42] *Church Committee Report, Vol. 5, supra,* at 20.
[43] *Id.*

In the absence of any governing statute, Attorney General Edward H. Levi's approach had been to authorize the requested surveillance only where a clear nexus existed between the target and a foreign power.[44] The Attorney General sought to distinguish the process from the British Crown's use of writs of assistance, in the shadow of which James Madison had drafted the Fourth Amendment.[45] The Founders' objection to such instruments was simple: were the government to be granted the authority to break into and to search individuals' homes without cause, the private affairs of every person would be subject to inspection.[46] In contrast, Levi argued, the exercise of electronic wiretaps for foreign intelligence gathering fell subject to Attorney General review. Nevertheless, he recognized the need for new laws to address the ambiguity that attended the use of modern technologies. The Senators agreed.[47]

C. Broader Context

The NSA was not the only federal entity making use of new technologies to collect significant amounts of information on U.S. citizens. The FBI, CIA, IRS, U.S. Army, and other federal entities similarly engaged in broad, domestic intelligence-gathering operations. Details relating to many of these programs, such as the FBI's COINTELPRO and the CIA's Operation CHAOS, were uncovered by both the exhaustive investigations of Senate Select Committee and other entities stood up to consider the range and extent of programs underway.[48] Both statutory violations and constitutional concerns accompanied these inquiries.

In 1970, for instance, Senator Sam Ervin (D-NC), began investigating the public allegations. After a year of making minimal progress in the face of misleading statements from the Nixon Administration, claims of inherent Executive power, and the refusal to disclose information that might damage national security, in 1971 Senator Ervin called for public hearings to consider "the dangers the Army's program presents to the principles of the Constitution."[49]

In 1975 President Ford issued an executive order establishing the President's Commission on CIA Activities Within the United States ("Rockefeller Commission").[50] Ford appointed Vice President Nelson Rockefeller as Chair.[51] The public charges to which the Rockefeller Commission responded included large-scale domestic surveillance of U.S. citizens; retaining dossiers on U.S. citizens; and aiming such collection efforts at individuals who disagreed with government policies.[52] The Commission's aim was further supplemented by allegations that for the past twenty years the CIA had (a) intercepted and opened personal mail in the United States; (b) infiltrated domestic dissident groups and intervened in domestic politics; (c) engaged in illegal wiretaps and break-ins; and (d) improperly assisted other government agencies.[53]

Like the Senate Select Committee, a key question confronting the Rockefeller Commission was how to define the term "foreign intelligence"—a crucial step in protecting Americans' right to privacy. Accordingly, in its first recommendation, the

---

[44] *Id.* at 71.
[45] *Id.* at 71-72.
[46] *Id.* at 72.
[47] *See, e.g., id.* at 64-65, 84, 125.
[48] *See, e.g., Church Committee Report, Vol. 5, supra,* at 6.
[49] 91 CONG. REC. 26,329.
[50] Exec. Order No. 11,828, 3 C.F.R. 933 (1975).
[51] *Commission on CIA Activities Within the United States: Announcement of Appointment of Chairman and Members*, 11 WEEKLY COMP. PRES. DOC. 25 (Jan. 5, 1975).
[52] REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES 9 (June 1975).
[53] *Id.*

Rockefeller Commission advised that Section 403 of the 1947 National Security Act be amended to make it explicit that the CIA's activities solely related to "foreign intelligence."[54] Any involvement of U.S. citizens could only be incidental to foreign intelligence collection.[55]

The Commission reinforced the strict separation between foreign targets and U.S. persons through its second recommendation: that the President, via Executive Order, "prohibit the CIA from the collection of information about the domestic activities of United States citizens (whether by overt or covert means), the evaluation, correlation, and dissemination of analyses or reports about such activities, and the storage of such information." [56]

The House Select Intelligence Committee, in turn, created on February 19, 1975 (known as the Nedzi Committee, after its chair, Lucien Nedzi, Chairman of the Armed Services Committee at the time), was replaced five months later by a committee headed by Representative Otis Pike (D-NY).[57] The Pike Committee focused on a range of intelligence agency intelligence gathering programs—including those of the National Security Agency.[58] Public hearings on the agency's operations were held in October 1975 and February and March 1976.[59] Its draft report complained of the tension between Congress and the Executive branch, noting the "intense Executive branch efforts" to have the NSA hearings curtailed or postponed—both in the Senate and the House.[60]

Like the Church Committee, the Pike Committee expressed concern about SHAMROCK and MINARET, noting that the former resulted in the NSA maintaining files on approximately 75,000 American Citizens between 1952 and 1974:

> Persons included in these files included civil rights leaders, antiwar activists, and Members of Congress. For at least 13 years, CIA employees were given unrestricted access to these files, and one or more worked full time retrieving information that presumably was contributed to the CIA's domestic intelligence program – Operation CHAOS – which existed from 1967 to 1974.[61]

For the Pike Committee, these programs violated both Section 605 of the Communications Act and the Fourth Amendment.[62]

The committee expressed particular concern about the NSA's "vacuum cleaner" approach to foreign intelligence gathering.[63] The committee noted that some 24 million telegrams and 50 million telex (teletype) messages entered, left, and transited the United States each year; millions of additional messages traveled over leased lines, "Including millions of computer data transmissions electronically entering and leaving the

---

[54] *Id.* at 12.
[55] *Id.*
[56] *Id.* at 15.
[57] H.R. Res. 138, 94th Cong. (Feb. 19, 1975) (introduced Jan. 16, 1975 and passed Feb. 19, 1975 by a vote of 286-120).
[58] *See, e.g., U.S. Intelligence Agencies and Activities; Intelligence Costs and Fiscal Procedures: Hearings Before the Select Comm. on Intelligence*, 94th Cong. Pt. 1 (1975), printed for the Select Comm. on Intelligence, 58-920 (1975); *U.S. Intelligence Agencies and Activities: Domestic Intelligence Programs: Hearings Before the Select Comm. on Intelligence*, 94th Cong., Pt. 3 (1975), printed for the Select Committee on Intelligence, 53-165 (1976); *U.S. Intelligence Agencies and Activities: Committee Proceedings-Proceedings of the Select Committee on Intelligence*, 94th Cong. Pt. 4 (1975), printed for the Select Comm. on Intelligence, 63-746 (1976).
[59] HOUSE COMM. ON GOV'T OPERATIONS, INTERCEPTION OF INTERNATIONAL TELECOMMUNICATIONS BY THE NATIONAL SECURITY AGENCY (DRAFT REPORT) 2, *available at* http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=4.
[60] *Id.*
[61] *Id.* at 14.
[62] *Id.* at 15-17.
[63] *Id.* at 18.

country"—and international telephone calls presented yet further potential sources of intelligence.[64]

Coming on the heels of the Pentagon Papers (demonstrating that the Johnson Administration had systematically lied to the public and to Congress), the Watergate scandal (in which the Nixon Administration orchestrated a June 1972 break-in at the Democratic National Committee Headquarters), and President Nixon's resignation on August 9, 1974, the existence of programs investigated by the Church Committee, the Rockefeller Commission, the Pike Committee, and others fed into and deepened the erosion of public confidence in the executive branch. More specifically, their findings undermined citizens' confidence in the intelligence agencies.[65] A critical question facing Congress was how to rebuild confidence in the system, how to incorporate new technologies into the existing infrastructure, and how to empower the intelligence agencies to conduct electronic surveillance, while protecting the privacy rights of U.S. citizens.

A timely judicial decision helped to lay the groundwork for Congressional action. In 1972 the Supreme Court had held that the electronic surveillance of domestic groups, even where security issues might be involved, required that the government first obtain a warrant. The "inherent vagueness of the domestic security concept", and the significant possibility that it could be abused to quash political dissent, underscored the importance of the Fourth Amendment—particularly when the government was engaged in spying on its own citizens.[66]

Justice Powell, writing for the Court, emphasized the limits on the scope of the decision: "[T]his case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."[67] Different standards and procedures might apply to domestic security surveillance than those required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[68] The Court issued an invitation to Congress to pass new laws covering such cases.[69]

Four critical changes followed. First, consistent with the Church Committee's recommendations, Congress created a permanent Senate Intelligence Committee. Indeed, within a month of the final report, a resolution to this effect was introduced, and on May 19, 1976 it passed by overwhelming majority, 72-22.[70] The new Senate Select Committee on Intelligence ("SSCI") was provided exclusive oversight of the CIA and concurrent jurisdiction over the NSA and other elements of the Intelligence Community ("IC"). The resolution directed that the IC keep the new entity "fully and currently informed" of their activities, including all "significant anticipated activities." It was to be a "select", rather than a "standing" committee, precisely to allow the Senate majority and minority leaders to decide its composition – and to avoid the same in the party caucuses preceding each new Congress. The Chair and Vice Chair would not be allowed to serve concurrently as Chair or ranking minority member of any major standing committee.

Of the 15 members selected, no more than 8 would be drawn from the majority party, ensuring balance between the parties. In addition, composition would be built to ensure cross-representation in related committees: two members had to sit each on Appropriations, Armed Services, Foreign Relations, and Judiciary. A limit of eight years

---

[64] *Id.*
[65] 124 CONG. REC. 36,415 (1978).
[66] *United States v. U.S. District Court*, 407 U.S. 297 (1972).
[67] *Id.* at 321-322.
[68] *Id.* at 322.
[69] *Id.* at 323.
[70] S. Res. 400, 94th Cong. (1976).

was placed on committee membership, to avoid intelligence agency capture. Notably, five of the first 15 members (Walter Huddleston (D-KY), Gary Hart (D-CO), Robert Morgan (D-NC), Barry Goldwater (R-AZ), and Howard Baker (R-TN), had served as members of the Church Committee—while 14 members of SSCI's staff had served as staff members to the same, including William Miller, the staff director for both the Church Committee and the newly-minted SSCI.[71]

Second, the President issued an Executive Order, "to improve the quality of intelligence needed for national security, to clarify the authority and responsibilities of the intelligence departments and agencies, and to establish effective oversight to assure compliance with law in the management and direction of intelligence agencies and departments of the national government."[72]

Executive Order 11905 prohibited the Central Intelligence Agency from engaging in electronic surveillance in the United States and banned intelligence agencies from engaging in physical surveillance, electronic surveillance, unconsented physical searches, mail opening, or examining federal tax returns except as consistent with procedures approved by the Attorney General or in accordance with applicable statutes and regulations.[73] It prohibited the infiltration of organizations for the purpose of reporting on their activities, unless the organization was primarily composed of Non-US persons and reasonably believed to be acting on behalf of a foreign power.[74] Importantly, the order prevented any *collection* of information about U.S. persons' domestic activities absent situations with clear foreign intelligence or counterintelligence component.[75]

Despite the provisions contained in the Executive Order, Congress considered legislative action to be crucial to reigning in the intelligence agencies. Resultantly, as a third outcome, Congress re-wrote the National Security Act to require a finding and notification for covert action.

Fourth, and most germane to the Judiciary Committee hearing today, Congress passed the Foreign Intelligence Surveillance Act. The aim was to empower the intelligence agencies to collect information necessary to protect U.S. national security, while simultaneously preventing agencies from using foreign intelligence gathering as an

---

[71] Discussion with William Miller, Washington, D.C. (Sept. 24, 2013). For discussion of the history of the founding of this committee and its subsequent development, *see* LEGISLATIVE OVERSIGHT OF INTELLIGENCE ACTIVITIES: THE U.S. EXPERIENCE, Report, Prepared by the Select Comm. on Intelligence of the United States Senate, 103rd Cong. (1994). *See also* FRANK J. SMIST, CONGRESS OVERSEES THE UNITED STATES INTELLIGENCE COMMUNITY, 1947-1989 (1990); L. BRITT SNIDER, THE AGENCY & THE HILL: CIA'S RELATIONSHIP WITH CONGRESS, 1946-2004, at 51-91(2008). Following the rather dismal mood that marked the Pike Committee's operations, the House Permanent Select committee on Intelligence was not founded until July 17, 1977. At that point, House Resolution 658 passed 227-171, creating the Permanent Select Committee on Intelligence (HPSCI). The structure of both committees remained relatively constant until 2004. The National Commission on Terrorist Attacks upon the United States issued its report in July 2004, criticizing the system of congressional oversight of intelligence agencies as "dysfunctional" and recommending either a joint committee on intelligence (similar to the Joint Atomic Energy Committee), with authority both the authorize and appropriate, smaller committees, and the elimination of term limits. U.S. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT 420-21 (2004). (NB: the first proposal to create a joint committee on intelligence was actually made in 1948. *See* H. Con. Res. 186, 80th Cong. (1948) (introduced by Rep. Devitt). In 2004, the Senate eliminated the eight-year term limits, elevated the committee to category A (Senators are generally only able to serve on up to two "A" Committees), created an Oversight Subcommittee, and created an Intelligence Subcommittee in the Appropriations Committee. S. Res. 445, 108th Cong. (2004).

[72] Exec. Order No. 11905, 41 Fed. Reg. 7703 (Feb. 18, 1976). This order was subsequently altered/strengthened by Exec. Order No. 12036, 43 Fed. Reg. 3674 (Jan. 24, 1978) and replaced in part by Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

[73] Exec. Order No. 11905, § 5(b)(1)-(5), 41 Fed. Reg. 7703 (Feb. 18, 1976).

[74] *Id.* § 5(b)(6).

[75] *Id.* § 5(b)(7).

excuse for engaging in domestic surveillance of U.S. citizens. The process began with the Foreign Intelligence Surveillance Act of 1976, the first bill introduced into Congress, and supported by the President and Attorney General, that would require judicial warrants in foreign intelligence cases.[76] Its successor bill, S.1566, became the Foreign Intelligence Surveillance Act of 1978.[77]

III. CONTOURS OF FISA

From the beginning, Congressional members made it clear that the legislation was designed to prevent precisely the types of broad surveillance programs and incursions into privacy represented by Project MINARET, Operation SHAMROCK, COINTELPRO, Operation CHAOS, and other intelligence-gathering initiatives that had come to light.

During consideration of the Conference Report on S. 1566, for instance, Senator Ted Kennedy (D-MA) noted, "The abuses of recent history sanctioned in the name of national security highlighted the need for this legislation."[78] The debate represented the "final chapter in the ongoing 10-year debate to regulate foreign intelligence electronic surveillance."[79] With the passage of FISA, the Senate would "at long last place foreign intelligence electronic surveillance under the rule of law."[80] Senator Birch Bayh, Jr. (D-IN) echoed Kennedy's sentiments, "This bill, for the first time in history, protects the rights of individuals from government activities in the foreign intelligence area."[81] Senator Charles Mathais (R-MD) noted that enactment of the legislation would be a milestone, ensuring "that electronic surveillance in foreign intelligence cases will be conducted in conformity with the principles set forth in the fourth amendment."[82]

Congress purposefully circumscribed the NSA's authorities in the Foreign Intelligence Surveillance Act by adopting four key protections. First, any information obtained from an electronic intercept had to be tied to a specific person or entity, identified as a foreign power or an agent thereof, *prior to the collection* of the information. Second, the government had to demonstrate probable cause that the target, about whom information was to be collected, was a foreign power or an agent thereof. For U.S. persons, such probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing American citizens with a higher level of protection. Third, Congress adopted minimization procedures to restrict the type of information that could be obtained and retained. Fourth, FISA made provision for a Foreign Intelligence Surveillance Court ("FISC") to oversee the process. Designed to introduce a neutral, disinterested magistrate into the equation, FISC's role was, narrowly, to ascertain whether the government had met the appropriate requirements for targeting *prior* to the acquisition of information. All of these limits dealt, specifically, with electronic communications. Over time, the statute expanded to apply a similar approach to physical searches, the placement of pen registers and trap and trace, and business records—as well as tangible goods.

---

[76] 124 CONG. REC. 35,389 (1978); *see also* Foreign Intelligence Surveillance Act of 1976, S. 3197, 94th Cong (1976).
[77] 124 CONG. REC. 35,389 (1978); *see also* Foreign Intelligence Surveillance Act of 1978, S. 1566, 95th Cong (1978).
[78] 124 CONG. REC. 34,845 (1978).
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] 124 CONG. REC. 35,389 (1978) (statement of Senator Mathais).

A. Acquisition of Information Tied to Entity Targeted Prior to Collection

From the outset, Congress sought to limit the amount of information acquired by the NSC and others by requiring that the target of surveillance be a foreign power or an agent of a foreign power *prior* to orders being issued to intercept communications. FISA defined a "foreign power" as:

(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowlwedged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organizations, not substantially composed of United States persons; or
(6) an entity that is directed and controlled by a foreign government or governments.[83]

Prior to passage of the bill, the Senate defined "foreign power", with regard to terrorist groups, to mean a foreign-based entity. The House amendments, in contrast, understood "foreign power" to include groups engaged in international terrorism or activities in preparation therefor. In the end, the Conference adopted the House definition, with the idea that limiting such surveillance solely to foreign-based groups would be unnecessarily burdensome.[84]

Regardless, however, of whether the target was a foreign power (in the strict sense), or a group engaged in international terrorism, in both Houses, throughout the nuanced discussion, underlying the definition of "foreign power" was the understanding that *prior* to collection of information, the government would have to establish that the target—in relation to whom such information would be obtained—qualified as a foreign power or an agent thereof.[85]

In focusing thus on the targets of the communications, Congress rejected the NSA's previous (and now current) reading of what constituted a "target" in relation to data collection.[86] That is, the information to be obtained, *at the moment of acquisition* (not in the context of subsequent analysis—the position advocated by General Allen during the Church Committee hearings and recently resurrected by the NSA), had to relate directly to the individual or entity believed to be a foreign power or an agent thereof.

B. Probable Cause and Satisfaction of Criminal Standards Prior to Collection

A second protection stemmed from concerns evinced in the Senate about how to determine whether the (specific) target was a "foreign power" or "an agent thereof". Uppermost in legislators' minds was the need to provide heightened protections for targets of surveillance generally and U.S. citizens in particular. The final bill accomplished this in two ways: adoption of a standard of probable cause and, under certain circumstances, the requirement of a showing of criminal wrongdoing, in order to

[83] 50 U.S.C. §1801(a) (2006 & Supp. V 2011).
[84] 124 CONG. REC. 33,782 (1978); *see also* 50 U.S.C. § 1801 (2006 & Supp. V 2011).
[85] 124 CONG. REC. 33,782 (1978).
[86] Testimony of General Lew Allen, Jr., *Church Committee Hearings, Vol. 5, supra,* at 16; Statement of NSA Director Bobby R. Inman, before Senate Subcommittee on Intelligence and Human Rights, as reported in the Washington Post, July 22, 1977, stating "Let there be no doubt, no U.S. citizen is now targeted by the NSA in the United States or abroad."

acquire information. These elements underscore the particularity that Congress insisted upon prior to foreign intelligence gathering.

FISA incorporated a standard of probable cause.[87] Unlike criminal law, however, in which the courts required that probable cause be established that a target had committed, was committing, or was about to commit a particular offense, under FISA, the agency requesting surveillance would have to demonstrate probable cause that the entity to be placed under surveillance was a "foreign power" or "an agent thereof", and that the target was likely to use the facilities to be monitored.[88]

Under certain circumstances, FISA also required a criminal showing for an entity to be considered a "foreign power". Excluded from this consideration were foreign governments. When they are directly involved, no showing of criminal activity is required. A foreign government, regardless of whether it is an ally or an enemy of the United States, qualifies as a "foreign power."[89]

For groups that qualify as foreign powers because they are engaged in international terrorism, a criminal activity must be involved. The statute defines "international terrorism" to include, inter alia, "activities that...involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State."[90] Acts in which individuals engage that would qualify them for inclusion in this category must be acts that would be criminal if committed within the United States.

A group may be a "foreign power" not just when it engages in international terrorism, but when engaged in "activities in preparation therefor." This may or may not exceed the criminal "attempt" standard, which is broadly understood as requiring a "substantial step" towards the completion of an offense.[91] Nevertheless, a "group" engaged in preparatory activities for international terrorism would satisfy criminal conspiracy standards.[92]

For agents of a foreign power, Congress inserted heightened protections for U.S. persons.[93] Specifically, FISA defines "agent of a foreign power" as:

---

[87] 50 U.S.C. § 1805(a)(2) (2006 & Supp. V 2011).

[88] *Compare* 18 U.S.C. §2518(3)(a) (2006) (requiring, under Title III, that the court must find "on the basis of the facts submitted by the applicant that ...there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter.") and 50 U.S.C. §1805(a)(3) (2006) (requiring, in contrast, that FISC find "on the basis of the facts submitted by the applicant," that "there is probable cause to believe that...the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.") Note that for ordinary criminal law, for wire and oral communications (e.g., telephone and microphone interceptions), §2516 enumerates predicate offenses that qualify, such as bank fraud (18 U.S.C §1344 (2006)), unlawful possession of a firearm (18 U.S.C. §922(g) (2006)), espionage (e.g., 18 U.S.C. §794 (2006)), assassination (e.g., 18 U.S.C §§351, 1751 (2006 & Supp. V 2011)), sabotage (e.g., 18 U.S.C. §2155 (2006)), and terrorism (e.g., 18 U.S.C. §2332 (2006)). For electronic communications (e.g., e-mail), any federal felony may serve as a predicate. 18 U.S.C. §2516(3) (2006).

[89] 50 U.S.C. §1801(a)(1) (2006 & Supp. V 2011).

[90] 50 U.S.C. §1801(c) (2006 & Supp. V 2011).

[91] *Braxton v. United States*, 500 U.S. 344, 351 (1991). This is not broader, however, than the "overt act" requirement contained in some criminal conspiracy statutes. *See, e.g.*, 18 U.S.C. §371 (2006). *See also* discussion in *In re [deleted]*, Appendix: Comparison of FISA and Title III.

[92] 18 U.S.C. §371 (2006).

[93] A "United States person" is understood under the statute as "a citizen of the United States, an alien lawfully admitted for permanent resident (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power as defined in subsection (a)(1), (2), or (3) of this section." 50 U.S.C. §1801(i) (2006 & Supp. V 2011).

(1) any person other than a United States person, who –
   (a) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
   (b) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who –
   (a) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
   (b) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
   (c) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
   (d) knowingly enters the United States under a false or frauduluent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreing power; or
   (e) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or C).[94]

What these definitions mean is that U.S. persons may only be considered agents of a foreign power consistent with the five provisions in the second sections. Taken together, three categories emerge for a U.S. person to be considered "an agent of a foreign power": either the person (1) engages in espionage and clandestine intelligence activities; (2) engages in sabotage and international terrorism (or aids, abets, or conspires to do the same); or (3) enters the United States under a false identity. This means that for U.S. persons, for the most part, evidence of criminality on a par with criminal law must be established prior to the collection of information.

Looking more closely, the first category requires that the individual knowingly engage in espionage and clandestine intelligence activities. Unlike the other two categories, there is some variation here with criminal law, specifically with regard to the "may involve" standard of category (a). Something less than the showing of probable cause required in ordinary criminal cases would satisfy this provision. Thus, for counterintelligence operations, something less than probable cause is required for evidence of criminality. But for a U.S. person to fall into this category, some evidence of criminality is involved.

For the second category, sabotage and international terrorism, the term "sabotage" is defined to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."[95] "International terrorism," in turn, as noted above, is also defined in terms of activities that are criminal or would be criminal if the United States were directly involved. To be considered "an agent of a foreign power" (and thus subject to surveillance under FISA), a U.S. person

[94] 50 USC §1801(b) (2006 & Supp. V 2011).
[95] 50 U.S.C. §1801(d) (2006 & Supp. V 2011).

must actually be engaged in such activities, or activities in preparation for sabotage or international terrorism—or knowingly aiding, abetting, or conspiring with others engaged in similar activities.[96]

These provisions reflect criminal law standards.[97] As the House of Representatives explained at the introduction of FISA,

> This standard requires the Government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding and abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision."[98]

The third category, which allows a U.S. person to be considered "an agent of a foreign power" for knowingly entering the country under false or fraudulent identity, almost always involves a showing of criminality, for the simple fact that it is not possible to legally enter the United States without providing proof of one's identity to a government official.[99] It is similarly illegal to knowingly assume a false identity on behalf of a foreign power under anti-fraud provisions of the U.S. code.

FISA's deliberate engagement of criminal law provisions and standards has been acknowledged by the government in defense of bringing down the wall between prosecution and investigation.

> [A] U.S. person may not be an "agent of a foreign power" unless he engages in activity that either is, may be, or would be a crime if committed against the United States or within U.S. jurisdiction. Although FISA does not always require a showing of an imminent crime or "that the elements of a specific offense exist," Senate Intelligence Report at 13, it does require the government to establish probable cause to believe that an identifiable target is knowingly engaged in terrorism, espionage, or clandestine intelligence activities or is knowingly entering the country with a false identity or assuming one once inside the country on behalf of a foreign power. Thus, while FISA imposes a more relaxed criminal probable cause standard than Title III, those differences are not extensive as applied to U.S. persons.[100]

The government cannot have it both ways: either U.S. persons have heightened protections under FISA—indeed, protections that rise to the level of those provided under Title III—or they do not.

Congress provided yet further protections for U.S. persons. The statute limited the breadth of surveillance operations by requiring that probable cause could not be established solely on the basis of otherwise protected first amendment activity.[101] This was meant to ensure that the executive branch could not place Americans under surveillance simply for exercising their First Amendment rights.

---

[96] 50 U.S.C. §1801(b)(2)(E) (2006 & Supp. V. 2011).

[97] *Compare* 18 U.S.C. §§ 2, 371 (2006) *See also In re [deleted]*, on Appeal from the United States Foreign Intelligence Surveillance Court, Supplemental Brief for the United States, No. 02-001, Appendix: comparison of FISA and Title III, *available at* https://www.fas.org/irp/agency/doj/fisa/092502sup.html.

[98] H.R. Rep. No. 95-1283, Part I, 95th Cong., 2d Sess. 44 (1978).

[99] 18 U.S.C. §1001 (2006).

[100] *In re [deleted]*, on Appeal from the United States Foreign Intelligence Surveillance Court, Supplemental Brief for the United States, No. 02-001, Appendix: comparison of FISA and Title III, *available at* https://www.fas.org/irp/agency/doj/fisa/092502sup.html.

[101] 50 U.S.C. §1805(a)(2) (2006).

C. Minimization Procedures for Acquisition and Retention

A third protection inserted by Congress centered on the introduction of minimization procedures, in order to protect activity not related to foreign intelligence from government scrutiny.[102] The legislature insisted here on minimizing not just the analysis of the information, but its "*acquisition* and *retention*."[103] Specifically, according to the statute:

> "Minimization procedures", with respect to electronic surveillance, means—
> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons. . .[104]

Under FISA, only U.S. persons' information must be subject to minimization procedures.[105]

D. Introduction of the Foreign Intelligence Surveillance Court

As a further precaution against executive overreach, Congress provided in FISA for two courts: the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review. A key principle throughout the debates was the importance of heightened protections where U.S. persons' information may be involved. The conference was deadlocked on this point until the Senate receded and accepted the House language exempting certain particularly sensitive surveillance (i.e., relating solely to foreign powers) from judicial review, on the grounds that (1) such surveillance did not involve U.S. persons; and (2) having removed the most sensitive information from external review, the Foreign Intelligence Surveillance Court could be given a greater role in protecting the rights of each U.S. person targeted by the government.[106] The use of a judicial element went some way towards providing for an independent, neutral, disinterested magistrate, to review the strength of the government's case supporting the initiation of surveillance.[107]

Initially, the statute provided for seven judges to sit on FISC; that number has since expanded to include eleven judges drawn from at least seven of the federal circuits, three of whom must reside in the Washington, D.C. area.[108] Both the FISC judges and the judges on the court of appeal are selected by the Chief Justice of the U.S. Supreme Court.[109] To avoid agency capture, judges may only serve for up to seven years, at the conclusion of which they are not eligible to again serve as FISC judges.[110]

From the beginning, FISC's role was significantly limited: it was merely to grant or to deny applications for orders.[111] The statute thus included extensive details about what would have to be included in such applications: the identity of the Federal officer making the application, the identity, if known, of the target, a statement of the facts and circumstances relied upon to justify the applicant's belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which

---

[102] 50 U.S.C. § 1804(a)(4) (2006 & Supp. V 2011).
[103] 50 U.S.C. § 1801(h) (2006 & Supp. V 2011) (emphasis added).
[104] *Id.*
[105] *Id.*
[106] 124 CONG. REC. 36,409 (1978).
[107] Discussion with former members of the Church Committee, Washington, D.C. (Sept. 23, 2013).
[108] 50 U.S.C. §1803(a)(1) (2006 & Supp. V 2011).
[109] 50 U.S.C. §1803(a)(1) (2006 & Supp. V 2011) and 50 U.S.C. §1803(b) (2006 & Supp. V 2011).
[110] 50 U.S.C. §1803(d) (2006 & Supp. V 2011).
[111] *Id.*

electronic surveillance is directed is being (or about to be) used by a foreign power or an agent thereof, a statement of the proposed minimization procedures, a description of the nature of the information sought, a certification from an executive branch official, a summary statement of the means by which the surveillance will be effected, a statement of the facts concerning all previous applications, and a statement of the period of time for which the surveillance is required to be maintained.[112]

Where the government has met the necessary criteria, the judge's role is to enter an ex parte order as requested, or to modify it accordingly. Initially, such orders could only be issued in relation to electronic surveillance. Subsequent amendments expanded FISC's jurisdiction to physical searches, pen registers and trap and trace devices and business records or tangible things.[113] These alterations, however, were merely in substance and not in form. The function being performed by FISC throughout was the same: it was merely to grant or to deny orders prior to the acquisition of information on particular targets.

E. Broad Congressional Support

The Foreign Intelligence Act of 1978 represented the culmination of a multi-branch, multi-year, cross-party initiative directed at bringing the collection of foreign intelligence within a narrowly circumscribed, legal framework. In 1972 the Senate Committee on the Judiciary's Subcommittee on Administrative Practice and Procedure held extensive hearings on the subject of warrantless wiretapping.[114] In 1975 the subcommittee issued a report jointly with a special subcommittee of the Foreign Relations Committee, calling for Congress to introduce legislation governing foreign intelligence collection.[115] In 1976 President Ford and Attorney General Levi introduced the first foreign intelligence bill.[116] President Carter and Attorney General Bell subsequently supported S. 1566, which became FISA.[117] Congress consulted the NSA, FBI, CIA, and representatives of interested citizen groups, gaining broad support for the measure.[118]

Because of the bipartisan, multi-branch approach taken to its construction, FISA passed by significant majorities. S. 1566 passed the Senate 95 to 1.[119] H.R. 7308 passed the House 246 to 128.[120] In October 1978 the Senate adopted the Conference Report "by an overwhelming voice vote, with no dissenting voice vote."[121] The House of Representatives, in turn, adopted the Conference Report by a vote of 226 to 176.[122]

F. Subsequent Amendment: Traditional and Non-Traditional FISA

Since FISA's introduction, Congress has amended the statute to cover physical searches,[123] pen register and trap and trace devices,[124] business records,[125] and tangible

---

[112] 50 U.S.C. §1804 (2006 & Supp. V 2011).
[113] 50 U.S.C. §§1821-1824 (2006 & Supp. V 2011) (orders for physical search); 50 U.S.C. §1842 (pen register and trap and trace devices); 50 U.S.C. §1861 (2006) (business records and tangible goods).
[114] 122 CONG. REC. 7543 (1976).
[115] *Id.*
[116] Foreign Intelligence Surveillance Act of 1976, H.R. 12750, 94th Cong. (introduced in the House, Mar. 23, 1976).
[117] 124 CONG. REC. 36,409 (1978).
[118] 124 CONG. REC. 37,738 (1978); 124 CONG. REC. 36,414 (1978).
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] 124 CONG. REC. 36,417-18 (1978).
[123] Pub L. No. 103-359, §101-909, 108 Stat. 3423, 3443 (1994); 50 U.S.C. §§1821-1829 (2006 & Supp. V 2011).
[124] Pub. L. No. 105-272, §§601-02, 112 Stat. 2396, 2404 (1998); 50 U.S.C. §§1841-1846 (2006 & Supp. V 2011).

goods.[126] Because of their consistent structure and approach, these provisions have come to be referred to collectively as "traditional FISA".[127] In 2008 Congress further amended the statute under Section 702 of the FISA Amendments Act, creating a new, non-traditional surveillance authority. Recent information made public suggests that the NSA is making extensive use of both traditional and modern authorities to conduct broad surveillance programs, in the process obtaining significant amounts of data on U.S. persons. A brief discussion of the provisions helps to underscore Congress' general approach in FISA and to elucidate ways in which these programs violate both the orientation of the statute and the existing statutory language.

1. Traditional FISA: Physical Search, Pen/Trap

Similar to the electronic surveillance provisions, physical search orders under FISA are limited by the government establishing the target of the search prior to acquisition of information. Specifically, physical search orders may only be used to target "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers."[128] The sub-section adopts the same definitions of "foreign power", "agent of a foreign power", "international terrorism", "sabotage", "foreign intelligence information", and "United States person" as used elsewhere in the statute.[129] It provides for FISC to grant or to deny orders consistent with FISC's role in electronic surveillance.[130] The government must make the same showings, particularly describing the target prior to FISC granting the order.[131] And heightened protections are afforded to U.S. persons.[132]

In 1998 Congress amended FISA to allow for the installation and use of pen register (recording numbers dialed from a particular phone) and trap and trace devices (acting as a caller ID record).[133] The Attorney General, or a designated attorney, must submit an application in writing and under oath either to FISC or to a magistrate specifically appointed by the Chief Justice to hear pen register or trap and trace applications on behalf

---

[125] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, §602, 112 Stat. 2396, 2410 (1998).

[126] Various further amendments of these sections have occurred. The USA PATRIOT Act, for instance, changed the duration of certain FISA authorization orders (§207), increased the number of FISC judges to 11 (§208); amended FISA pen/trap provisions (§214), changed the purpose of electronic & physical searches (§218), and authorized coordination between intelligence and law enforcement (§504). ITRPA subsequently added a "lone wolf" provision via §60001(a).

[127] *See, e.g.,* DAVID S. KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, Chapter 12 (2d ed. 2012). In addition to the aforementioned amendments, in 2001 Congress amended FISA to take account of roving wiretaps. USA PATRIOT Act, §206 (amending §105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978, codified as amended at 50 U.S.C. §1805(c)(2)(B) (2006)). This alteration reflected a change that had been integrated into criminal law measures in 1998. At that time, the House Conference Report explained: "Under current law, judges issue wiretap orders authorizing law enforcement officials to place a wiretap on a specific telephone number. Criminals, including terrorists and spies, know this and often try to avoid wiretaps by using pay telephones on the street at random, or by using stolen or cloned cell telephones. As law enforcement officials cannot know the numbers of these telephones in advance, they are unable to obtain a wiretap order on these numbers from a judge in time to intercept the conversation, and the criminal is able to evade interception of his communication."

[128] 50 U.S.C. § 1822(a)(1)(A)(i) (2006).

[129] 50 U.S.C. § 1821(1) (2006 & Supp. V 2011).

[130] 50 U.S.C. §§ 1822-1824 (2006).

[131] 50 U.S.C. § 1823 (2006 & Supp. V 2011).

[132] *See, e.g.,* 50 U.S.C. § 1821(1)(A)(ii) (2006 & Supp. V 2011) (requiring the Attorney General to certify in writing and under oath that "there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States Person.") and 50 U.S.C. § 1821(1)(A)(iii) (2006 & Supp. V 2011) (requiring minimization procedures for U.S. persons information).

[133] Pub. L. No. 105-272, §§601-02, 112 Stat. 2396, 2404 (1998); 50 U.S.C. §§1841-1846 (2006) (pen/trap); 50 U.S.C. §§1861-1862 (2006) (tangible things).

of the FISA court.[134] Similar to the provisions related to electronic communications and physical search, the application must include information to show that the device has been, or will in the future be, used by someone who is engaging (or has engaged) in international terrorism or is a foreign power or agent thereof.[135] In the event of an emergency, the Attorney General can authorize the installation and use of a pen register or trap and trace device without judicial approval.[136] Nevertheless, a proper application must be made to the appropriate judicial authority within forty-eight hours.[137]

Following the 9/11 attacks, Congress relaxed the requirement for factual proof for placement of a pen/trap: the applicant no longer must demonstrate why he or she believes that a telephone line will be used by an individual engaged in international terrorism. Instead, the applicant must demonstrate only that the information likely to be gained does not directly concern a U.S. person and will be relevant to protect against international terrorism. This provision, hotly contested by civil libertarians, was scheduled to sunset on December 31, 2005.[138] But in 2006, Congress made it permanent.[139] Critically, while it relaxes the standard for obtaining information from particular telephone lines, it still draws a higher bar for obtaining U.S. persons' information.

The statute understands the terms "pen register" and "trap and trace device" consistent with the criminal law standard—namely: a pen register is:

> [A] device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facilitiy from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication.[140]

A "trap and trace device", in turn, is defined as:

> [A] device or process which captures the incoming electronic or other impulses which identify the originating number of other dialing, routing, addressing, and signalling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.[141]

In addition to all dialing, routing, addressing and signalling information sent from or received by a target, orders may require electornic communication service providers to disclose further information, including:

(1) the name of the customer or subscriber;
(2) the address of the customer or subscriber
(3) the telephone or instrument number, or other subscriber number of identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission ifnormation;

---

[134] 50 U.S.C. § 1842(a)-(b) (. As with the application for electronic surveillance, the applicant must include the name of the official seeking surveillance, as well as certification that "the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation." 50 U.S.C. § 1842(c)(1)-(2) (2006).

[135] 50 U.S.C. § 1842(c)(A) (2006 & Supp. V 2011).

[136] 50 U.S.C. § 1843(a) (2006 & Supp. V 2011).

[137] 50 U.S.C. § 1843(a)(2) (2006 & Supp. V 2011).

[138] Uniting and Strengthening America by Proving Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 215, 115 Stat. 272 (2001) (codified as amended at 50 U.S.C. §1861 (2000 & Supp. V 2001)); 18 U.S.C. § 214 (2000).

[139] USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 102, 120 Stat. 192 (2006).

[140] 18 U.S.C. §3127(3) (2006 & Supp. V 2011).

[141] 18 U.S.C. §3127(4) (2006 & Supp. V 2011).

(4) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;
(5) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;
(6) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and
(7) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service.[142]

Notably, what these passages demonstrate is that the collection of all of the information encapsulated in the NSA's telephony metadata program is already provided for under FISA subchapter three.

Unlike the NSA's current practice, however, *each order* under the pen/trap provisions must be approved by either FISC or a magistrate judge appointed for the purpose of approving pen/trap orders under FISA.[143] Orders must specify the precise identity (if known) of the person who is the subject of the investigation, and the person to whom is leased or in whose name the telephone line is listed.[144] And heightened protections are provided for U.S. persons.[145]

These provisions are entirely consistent with Congress' approach in FISA: namely, particularized showing in relation to the target, a decision prior to the collection of information, issuance of an individualized order by the court, and heightened protections for U.S. persons. By inappropriately introducing the telephony metadata under subchapter four, the NSA is simply doing an end-run around the carefully thought-out protections of subchapter three. I will return to this point, below.

2. Traditional FISA: Business Records, Tangible Goods, and Section 215

Following the Oklahoma city bombing, in 1998 Congress amended FISA to authorize the production of certain kinds of business records of those suspected of being foreign powers or agents of a foreign power: namely, documents maintained by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[146] Any records obtained under this provision had to be for "an investigation to gather foreign intelligence information or an investigation concerning international terrorism."[147] The application had to include "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[148]

As with the other provisions of traditional FISA, Congress assigned the terms "foreign power", "agent of a foreign power, "foreign intelligence information", and "international terrorism" the same meaning as employed in relation to electronic surveillance.[149] Congress also required intelligence agencies to follow the same steps as

---

[142] 50 U.S.C. §1842(d)(2)(c)(i) (2006 & Supp. V 2011).
[143] 50 U.S.C. §1842(b)(2) (2006 & Supp. V 2011).
[144] 50 U.S.C. §§1842 (d)(2)(A)(i)-(ii) (2006 & Supp. V 2011).
[145] 50 U.S.C. §§1842 (c)(2) (2006 & Supp. V 2011) (requiring "certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.")
[146] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, §602, 112 Stat. 2396, 2410 (1998).
[147] *Id.*
[148] *Id.*
[149] *Id.*

those taken with regard to electronic surveillance: i.e., to submit an application to FISC to obtain an order, which then compels the companies to hand over the records.[150]

Initially, the FBI did not heavily rely on the business records provision: between 1998 and 2001, the Bureau only used it once. Nevertheless, in 2001 Congress expanded the types of records that could be obtained, authorizing intelligence agencies to apply for an order from FISC "requiring the production of any tangible things (including books, records, papers, documents, and other items)".[151] Congress eliminated restrictions on the types of businesses or entities on which such an order could be served.[152] It retained, however, the general contours of FISA, specifying that such items be obtained in the course of "an investigation to protect against international terrorism or clandestine intelligence activities."[153] Congress again added heightened protections for U.S. persons, requiring that such investigation, where directed towards a U.S. person, not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[154]

In the new statute, Congress lowered the standard for obtaining Section 215 orders, eliminating the requirement that the application include "specific and articulable facts" indicating that the individual to whom the records pertain is a foreign power or an agent thereof.[155]

Nevertheless, from the beginning, the Department of Justice rightly understood that the information to be obtained under the tangible goods provision was still narrow, in that it must pertain directly to the person targeted in the authorized investigation. A memorandum sent in October 2003 to all Field Offices explained:

> The business records request is not limited to the records of the target of a full investigation. The request must simply be sought for a full investigation. Thus, if the business records relating to one person are relevant to the full investigation of another person, those records can be obtained by a FISC order despite the fact that there is no open investigation of the person to whom the subject of the business records pertain.[156]

The relevance standard adopted was thus specific with regard to the connection between the records sought and the target of the investigation, as well as limited, with regard to the actual establishment of a particular investigation.

---

[150] *Id.*

[151] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861 (2006 & Supp. V 2011). Congress also amended FISA to require that applicants to FISC certify that "a significant purpose" of the surveillance be to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7)(B) (2006 & Supp. V 2011). This shift, from the prior language that "the" purpose be to obtain foreign intelligence, had the effect of removing a wall that had built up within the Department of Justice between intelligence officers and criminal prosecutors. The government argued that the latter should be allowed to advise the former concerning the initiation, operation, continuation, or expansion of FISA searches or surveillance. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 623 (FISA Ct. 2002). The Foreign Intelligence Surveillance Court of Review upheld the change. *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). This alteration, however, simply recognizes parallels between criminal violations and national security threats. It does not suddenly shift the focus of the statute to allow intelligence agencies to collect information on millions of Americans not suspected of any wrongdoing.

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] USA PATRIOT Act § 215, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861 (2006 & Supp. V 2011).

[156] FBI Memorandum from General Counsel, National Security Law Unit, to All Field Offices, Business Records Orders Under 50 U.S.C. § 1861 (Oct. 29, 2003), *available at* http://epic.org/privacy/terrorism/usapatriot/foia/field_memo.pdf.

For the first two years, attorney general guidelines only allowed business record requests as part of full field investigations. In the same memo specifying that the records must be directly related to the person under investigation, the general counsel of the national security law unit indicated that the type of investigation that must already be established, and in relation to which the records being sought must pertain, "may be revised in the near future to allow the use of a FISC business records order in a preliminary investigation."[157] Near future indeed—two days later, on October 31, 2003, Attorney General issued a 38-page document, establishing new guidelines for national security investigations—and allowing agents to obtain business records during preliminary investigations.[158]

Despite the expansion to preliminary investigations, the specificity embedded in the relevance principle remained. In order to open a preliminary investigation, the Attorney General required in his 2003 guidelines that, inter alia, the individual targeted in the investigation be an international terrorist or an agent of a foreign power, or any individual, group, or organization engaged in activities constituting a threat to national security for or on behalf of a foreign power, or who may be the target of a recruitment or infiltration effort by an international terrorist, foreign power, or an agent of a foreign power.[159]

There are two points to make about this construction. First, the Attorney General emphasized particular "individuals," "groups," or "organizations" as the target of preliminary investigations. This was consistent with FISA's traditional approach. Second, only once a preliminary investigation was established could agents then make use of "authorized techniques" to obtain information (e.g., mail opening, physical search, or electronic surveillance requiring judicial order or warrant).[160] This meant that the target had to be determined (in the course of which the FBI would open a preliminary investigation) prior to orders allowing for the acquisition of tangible goods could issue.

Section 215 of the USA PATRIOT Act was set to expire December 31, 2005.[161] Congress has since renewed it seven times.[162] It is now set to expire June 1, 2015.[163] In

---

[157] *Id.*

[158] The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003), *available at* http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf.

[159] *Id.* at 14.

[160] *Id.* at 15.

[161] *Id. See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, 50 U.S.C. §§ 1861-63 (amending Title V, Section 501 of the Foreign Intelligence Surveillance Act, "Access to Certain Business Records for Foreign and International Terrorism Investigations, 50 U.S.C. § 1861).

[162] An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Prevention Act of 2004 to July 1, 2006, Pub. L. No. 109-160, 119 Stat. 2957 (2005) (extension until Feb. 3, 2006); An Act To Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109-170, 120 Stat. 3 (2006) (extension until Mar. 10, 2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (extension until Dec. 31, 2009); Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009) (allowing for a short-term, 60-day extension of 50 U.S.C. 1861 until February 28, 2010); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010) (extension until Feb. 28, 2011); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (2011) (extension until May 27, 2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011) (extension until June 1, 2015).

[163] PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011). Note that in a race against the clock, President Obama signed the most recent, four-year extension of Section 215 just minutes before the midnight deadline May 26, 2011. Patriot Act Extension Signed Into Law Despite Bipartisan Resistance in Congress, WASH POST, May 27, 2011, *available at* http://www.washingtonpost.com/politics/patriot-act-extension-signed-into-law-despite-bipartisan-resistance-in-congress/2011/05/27/AGbVlsCH_story.html. A bipartisan group of lawmakers had rallied against the

2005, in the course of extending the tangible goods provision, Congress added language tying the section more closely to FISA's overarching structure. It required applicants to submit a statement of facts, establishing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)."[164] The investigation to which the order is tied must be conducted under guidelines approved by the Attorney General.[165] The purpose of the investigation must be "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[166] The underlying investigation may not be directed at a U.S. person based solely on otherwise protected First Amendment activity.[167]

Tangible things are presumptively relevant to an investigation where 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, themselves the subject of an authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation.[168]

For certain materials—namely, library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records with information identifying an individual, only the Director of the FBI, the Deputy Director of the FBI, or the Executive Assistant Director for National Security may make the application; none of these individuals may further delegate their authorities in this respect.[169]

In the 2005 amendments, Congress required "an enumeration of the minimization procedures" related to the retention and dissemination of any tangible things obtained.[170] Any orders issued "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."[171] As discussed, below, the telephony metadata program, by FISC's own admission, fails to satisfy this statutory requirement. Any individual served with an order is gagged from telling anyone other than individuals to whom disclosure is necessary to comply with the order or an attorney to obtain legal advice or help with regard to producing the items sought.[172] Under the

---

measure, with the result that the USA PATRIOT Sunsets Extension Act of 2011 passed the Senate 72 to 23 and the House 250 to 153. With President Obama at a summit in France, the White House took the unusual step of having him sign the bill with an autopen—prompting commentators to question whether it was legal under Art. 1(7) of the U.S. Constitution. See, e.g., *PATRIOT Sunset Extension Act of 2011 "Signed" into Law*, Law Librarian Blog, *available at* http://lawprofessors.typepad.com/law_librarian_blog/2011/05/patriot-sunset-extension-act-of-2011-signed-into-law-.html; Originalism and the Autopen: Obama's "Signing" of Patriot Act Extension Constitutional, Constitutional Law Prof Blog, May 30, 2011, http://lawprofessors.typepad.com/conlaw/2011/05/originalism-and-the-auto-pen.html. The White House apparently relied on a memorandum opinion issued by the Office of Legal Counsel in 2005. See Whether the President May Sign a Bill by Directing that His Signature be Affixed to It, Memorandum Opinion for the counsel to the President, July 7, 2005, *available at* http://lawprofessors.typepad.com/files/opinion_07072005.pdf.

[164] USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. 196 (codified as amended at 50 U.S.C. §1861 (2006).

[165] 50 U.S.C. §1861(a)(2)(A) (2006). Such guidelines are issued consistent with Executive Order 12333.

[166] USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. 196 (codified as amended at 50 U.S.C. §1861(2006)).

[167] 50 U.S.C. §1861(a)(2)(B) (2006).

[168] 50 U.S.C. §1861(b)(2)(A) (2006) and 50 U.S.C. §1861(c)(1) (2006).

[169] 50 U.S.C. §1861(a)(3) (2006).

[170] *Id.*

[171] 50 U.S.C. §1861(c)(2) (2006).

[172] 50 U.S.C. §1861(c)(2)(E) (2006).

statute, an individual on whom an order has been served may challenge the legality of the order by filing a petition with the court within a year, requesting that the order be modified or set aside.[173]

3. Modern FISA and Section 702

Until recently, FISA did not regulate any of the four activities (electronic surveillance, physical searches, pen/trap, or tangible things) when conducted abroad. If a U.S. person went overseas, their telephone calls could be monitored and their hotel room searched without regard to FISA. Authority stemmed from the President's inherent constitutional authority, as channeled through Executive Orders, Department of Defense directives, and policy documents.[174] Nevertheless, in recognition of the higher level of protection afforded to U.S. persons, SIGINT practice, prior to the attacks of September 11, 2001, was not to listen in on, or to collect information on, Americans overseas.[175] U.S. citizens within domestic bounds fell within traditional FISA.

It thus came as a surprise when, in late 2005, the *New York Times* reported that the NSA had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[176]

White House Press Secretary, Scott McClellan, initially refused to comment.[177] But the next morning, President Bush went on national television to defend the surveillance operation.[178] He grounded his power in the 2001Authorization for the Use of Military Force (passed by Congress one week after the September 11, 2001 attacks), and his

---

[173] 50 U.S.C. §1861(f)(1)(B) (2006).

[174] Exec. Order 12333, § 2.5, 46 Fed. Reg. 59941 (Dec. 4, 1981) "The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this order.") *See also* DoD Directive 5240.1, Activities of DoD Intelligence Components that Affect US Persons, Apr. 5, 1988; NSA/CSS Directive No. 10-30, Procedures Governing Activities of NSA/CSS that Affect US Persons, Sept. 20, 1990.

[175] [NSA/Central Security Services] U.S. Signals Intelligence Directive 18 [July 27 1993] at §3.1 ("The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.* The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID."). *See also id.* at §4.1.

[176] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N. Y. TIMES, Dec. 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0 (also writing "Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying. . .")

[177] Press Briefing by Scott McClellan, James S. Brady Briefing Room, 12:33 pm, Dec. 16, 2005, available at http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051216-1.html ("there's a reason why we don't get into discussing ongoing intelligence activities, because it could compromise our efforts to prevent attacks from happening. And it could telegraph to the enemy what we are doing. . . And we don't want to do anything to compromise sources and methods. As for talking about the NSA, "that would be getting into talking about ongoing intelligence activities. And they're classified for a reason, because they do to the issue of sources and methods and protecting the American people. And because they're classified, I'm not able to get into discussing those issues from this podium.")

[178] President's Radio Address, Roosevelt Room, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html. ("I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.")

constitutional authorities as Commander-in-Chief.[179] Bush revealed that he had re-authorized the program more than 30 times since 9/11.[180] Each review, he said, had included the Attorney General and the Counsel to the President, with NSA's activities further overseen by legal counsel at DOJ and NSA.[181] Leaders in Congress also had been briefed on the program.[182] Bush added, "This authorization is a vital tool in our war against the terrorists. It is critical to saving American lives."[183] He stated that the release of the *New York Times* story had been illegal.[184] The FBI immediately began an investigation into the leak, with 25 agents and 5 prosecutors assigned to the case.[185]

The Administration soon offered a more detailed legal defense of the Terrorism Surveillance Program ("TSP"), largely consistent with the President's initial statements.[186] The Department of Justice explained that the purpose of the program was to "intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations".[187] The Department cited "the President's well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes."[188] It referenced the President's authority under Article II of the Constitution to repel acts of aggression.[189] And it argued that the language in the AUMF, giving the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided

---

[179] *Id.* ("I am using authority vested in me by Congress, including the Joint Authorization for Use of Military Force, which passed overwhelmingly in the first week after September the 11th. I'm also using constitutional authority vested in me as Commander-in-Chief.") *See also* Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat 224 (2001).

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] Scott Shane, Obama Takes a Hard Line Against Leads to Press, N. Y. TIMES, June 11, 2010, *available at* http://www.nytimes.com/2010/06/12/us/politics/12leak.html.

[186] See U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President* (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; Letter from William E. Moschella, Assistant Attorney General to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockiefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives, Washington, DC, (Dec. 22, 2005) (available at https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf)

[187] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 5, (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf)

[188] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 1 (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf).

[189] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 1 (Jan. 19, 2006) http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; and Letter from William E. Moschella, Assistant Attorney General, to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives, Washington, DC (Dec. 22, 2005) (available at https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf) ("This constitutional authority," the Assistant Attorney General continued, "includes the authority to order warrantless foreign intelligence surveillance within the United States, as all federal appellate courts, including at least four circuits, to have addressed the issue have concluded.")

the terrorist attacks" of September 11 to prevent "any future acts of international terrorism against the United States" included traditional military activity—into which category warrantless communications intelligence fell.[190] According to DOJ, this moved the decision into the first category of the tripartite framework established by Justice Jackson's concurrence in Youngstown Sheet & Tube Co. v. Sawyer.[191] The government also relied on the War Powers Resolution, enacted less than five years before FISA, as allowing the President to introduce United States Armed Forces into hostilities.[192]

Congress and others strongly objected to the legal analysis. The Authorization of the Use of Military Force nowhere made reference to electronic surveillance; nor did the legislative history associated with the authorization.[193] FISA, moreover, contemplated the advent of war, allowing for special procedures to be followed with respect to electronic surveillance, physical searches and pen/trap surveillance.[194] It provided for a 15 day grace period, to "allow time for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency."[195] At the expiry of the 15 days, absent any amendment, ordinary FISA provisions would have to be followed. This was a carefully-constructed compromise position: during the debates on FISA, the House of Representatives had sought a complete abatement of FISA during periods of declared war. The Senate objected, and the House of Representatives changed its position.

Congress (and the Courts) also had considered and declined to recognize claims to Presidential Article II authority to conduct foreign intelligence gathering within domestic bounds. During passage of FISA, the House wanted the statute to read that it was the "exclusive statutory" means for the Executive to conduct electronic surveillance, implying in the process that the President had inherent surveillance powers outside the statute. The Senate completely rejected this notion, suggesting that if the President were to engage in electronic surveillance outside the parameters of FISA, on judicial review, they wanted the Supreme Court to treat the President's actions as under Justice Jackson's third category in Youngstown: against the expressed intent of Congress. The Senate view carried.

The TSP turned out to be more far-reaching than initially acknowledged. Five months after the initial revelations, on May 11, 2006, a *USA Today* article detailed how, since 9/11, the country's largest telecommunications companies had been secretly providing customers' domestic calling records to the NSA for analysis. AT&T, Verizon, and BellSouth were implicated in the report.[196] Once again, the White House defended the program, stating that no domestic surveillance is conducted without court approval.

---

[190] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 2 (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf).

[191] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 2 (Jan. 19, 2006) (available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf). *See also Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-638 (1952) (Jackson, J., concurring).

[192] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the national Security Agency Described by the President*, at 27 (Jan. 19, 2006) http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

[193] Authorization for the Use of Military Force (AUMF), Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001).

[194] 50 U.S.C. §1811 (2006) (electronic surveillance); 50 U.S.C. §1829 (2006) (physical search), 50 U.S.C. §1844 (2006) (pen/trap) ("Notwithstanding any other law, the President, through the Attorney General, may authorize [electronic surveillance, physical search, or pen/trap] to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by Congress.")

[195] Foreign Intelligence Surveillance Act of 1978, H.R. Rep. No. 1720, 95th Cong., 2d Sess. at 45 (1978) (Conf. Rep.).

[196] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm?csp=34.

According to Dana Perino, deputy White House Secretary, the appropriate members of Congress had been briefed.[197] Nevertheless, the news seemed to take the then-Chairman of the Senate Judiciary Committee, Senator Arlen Specter (R-PA) by surprise.[198] Senator Patrick Leahy (D-VT) sounded similarly incredulous, railing against the lack of congressional oversight and suggesting that the media was doing rather a better job of it than the legislature. "Are you telling me that tens of millions of Americans are involved with al Qaeda?" Leahy asked.[199] "These are tens of millions of Americans who are not suspected of anything. . . Where does it stop?"[200] He held up a copy of the newspaper and added, "Shame on us for being so far behind and being so willing to rubber stamp anything this administration does. We ought to fold our tents."[201]

General Michael V. Hayden, NSA director 1999-2005, defended the program to Congress and to the public by saying that the NSA was only targeting international communications – and only those U.S persons suspected of ties to terrorism.[202] According to Hayden, attorneys inside and outside the agency considered that the program was constitutional—and vital to U.S. national security.[203] Hayden's language was strikingly similar to Church Committee hearings and Lt. Gen. Lew Allen Jr.: "This activity was reviewed by proper authority within NSA and by competent external authority. . ."[204] A major difference, of course, was that in the interim Congress had passed FISA, precisely to prevent this type of large-scale collection of information.

In light of growing tension about the program, in 2007 the NSA discontinued it.[205] In April of that year, the Director of National Intelligence J.M. McConnell submitted a proposal to Congress to amend FISA to make it easier for the executive branch to target U.S. interests abroad. Four months later, Congress passed the Protect America Act ("PAA"), easing restrictions on the surveillance of foreigners where one (or both) parties were located overseas.[206] The statute removed FISC from supervising the interception of communications that began or ended in a foreign country. In its place, the Attorney General and the Director of National Intelligence could authorize, up to one year, the acquisition of communications concerning "persons reasonably believed to be outside the United States", where five criteria were met:

1. there were reasonable procedures in place for determining that the acquisition concerns persons reasonably believed to be located outside the United States;
2. the acquisition did not constitute electronic surveillance (meaning it did not

---

[197] *Id.*

[198] *Id.*(reporting Specter as saying that "he would call the phone companies to appear before the panel 'to find out exactly what is going on.'")

[199] *Id.*

[200] *Id.*

[201] *Id.*

[202] *See, e.g.,* Jim Sensenbrenner, Directing the Attorney General to Submit to the House of Representatives all Documents in the Possession of the Attorney General Relating to Warrantless Electronic Surveillance of Telephone Conversations and Electronic Communications of Persons in the United States Conducted by the National Security Agency, H.R. REP. No. 109-382 (2006) (citing, inter alia, Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, Press Briefing (Dec. 19, 2005); NSA Director General Hayden Press Conference (Jan. 23, 2006).

[203] *Id.*

[204] *The National Security Agency and Fourth Amendment Rights: Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Cong. 22 (1976).

[205] S. REP. NO. 110-209, at 4 (2007); and Letter from Attorney General Alberto Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (Jan. 17, 2007). Note that these documents suggest that the program ran from just after the attacks of 9/11 until January 2007).

[206] Protect America Act, 2007, Pub. L. 110-55, § 2, 121 Stat. 553. (Aug. 5, 2007) (amending FISA, §105B(a)(1)-(5)), codified at 50 U.S.C. §1805b (2006)).

involve solely domestic communications);

3. the acquisition involved obtaining the communications data from or with the assistance of a communications service provider who had access to communications;
4. a significant purpose of the acquisition was to obtain foreign intelligence information; and
5. minimization procedures outlined in the FISA would be used.[207]

The PAA required the Attorney general to submit the targeting procedures to FISC and to certify that the communications to be intercepted were not purely domestic in nature.[208] Once certified, however, FISC was given no option as to whether or not to grant the order. Twice a year the Attorney General would be required to inform the Intelligence and Judiciary Committees of the House and Senate of incidents or noncompliance with the directive issued by the Attorney General or Director of National Intelligence, incidents of noncompliance with FISC-approved procedures, and the numbers of certifications or directives issued during the reporting period.[209] In addition, the PAA gave retroactive immunity to service providers to insulate them from civil liability. The PAA initially was to operate for six months.[210] Congress then continued it until February 17, 2008.[211] Congress eventually replaced the legislation with a more permanent measure: the FISA Amendments Act ("FAA").[212]

The FAA empowers the Attorney General and the Director of National Intelligence to jointly authorize, for up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[213] FISC annually reviews this certification but has no substantive role in the decision either to engage in the surveillance or to cease doing the same. Five limitations apply to the order issued by the AG and DNI: first, it "may not intentionally target any person known at the time of acquisition to be located in the United States."[214] Second, it "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States."[215] Third, it "may not intentionally target a United States person reasonably believed to be located outside the United States."[216] Fourth, it "may not intentionally acquire 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."[217] And fifth, the collection of such information "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."[218]

---

[207] *Id.*

[208] Protect America Act, 2007, Pub. L. 110-55, § 3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA §105B(c), codified at 50 U.S.C. §1805c (2006).

[209] Protect America Act, 2007, Pub. L. 110-55, §3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA §105C).

[210] Protect America Act, 2007, Pub. L. 110-55, §6 , 121 Stat. 552 (Aug. 5, 2007).

[211] Various bills were proposed in the interim. See, e.g., S. 2248 (2007).

[212] FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (July 10, 2008).

[213] Foreign Intelligence Surveillance Act, "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons, Title VII, Section 702, codified at 50 U.S.C. § 1881(a) (2006). Except as otherwise noted, section 702 mirrors the definitions adopted in FISA for the terms "agent of a foreign power", "foreign intelligence information" , "foreign power", and "person".

[214] §1881b(1).

[215] §1881b(2).

[216] §1881b(3).

[217] §1881b(4).

[218] §1881b(5).

The upshot is that Section 702 gives the NSA the authority to target non-U.S. persons located outside the United States at the time of the collection of data.[219] FAA brought the targeting of U.S. persons overseas, previously addressed via Section 2.3 of Executive Order 12333, within traditional FISA. Consistent with the overall approach of FISA, this shift provided a higher protections for U.S. persons. The FAA required, in addition, that the government adopt targeting and minimization procedures for review by FISC. The minimization procedures, in particular, restrict handling information concerning U.S. persons incidentally acquired under Section 702—including the retention and dissemination of such information. In December 2012, Congress passed, and the President signed, the FISA Amendments Act Reauthorization Act, extending Title VII of FISA through December 31, 2017.[220] Absent intervening action by Congress, Title VII will automatically be repealed on that date.[221] Any orders in place as of that date will continue until their ordinary expiration.

IV. NSA TELEPHONY METADATA COLLECTION UNDER §215

On May 24, 2006, the Foreign Intelligence Surveillance Court approved an FBI application for an order, pursuant to 50 U.S.C. §1861, requiring telecommunications providers to turn over all telephony metadata to the National Security Agency.[222] Over the next seven years, FISC issued orders renewing the program thirty-four times.[223] As FISC acknowledged in classified rulings:

> [N]early all of the call detail records collected pertain to communications of non-U.S. persons who are *not* the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are *not* the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities, and are data that otherwise could not be legally captured in bulk by the government.[224]

This program remained secret until a combination of the Snowden documents and FOIA litigation launched by the Electronic Frontier Foundation forced key documents into the

---

[219] In exigent circumstances, the Attorney General and the DNI may authorize an immediate acquisition under Section 702; however, they must then submit a certification to the FISC as soon as practicable, but in no event later than seven days after they determined the existence of such exigent circumstances.

[220] Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

[221] 50 U.S.C.S. §1881 note (LexisNexis Supp. Apr. 2013).

[222] In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR-05 (FISA Ct. May 24, 2006), *available at* https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf (released by court order as part of the Electronic Frontier Foundation's FOIA litigation). Note that the specific telecommunications company from which such records were sought were redacted, as well as the remaining title; however, the government also released an NSA report that provided more detail on the title of the Order. OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 94 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf. For purposes of a more precise citation, I draw from both sources.

[223] Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act 2 (Aug. 9, 2013), *available at* https://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html [hereinafter "Section 215 White Paper"].

[224] In re Production of Tangible Things *From* [REDACTED], Order, No. BR 08-13, at 12 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf (emphasis in original).

public domain.[225] In response, the Obama Administration issued statements, fact sheets, redacted FISC opinions, and even a White Paper, acknowledging the existence of the program and arguing that it is both legal and Constitutional.

According to these document, the purpose of the telephony metadata program is to collect information related to counterterrorism and foreign intelligence.[226] The information includes all communications routing information, including (but not limited to) session identifying information (e.g., originating and terminating telephone number, identity of the communications device, etc.), trunk identifier, and time and duration of the call.[227] The metadata collected as part of this program does not include the substantive content of communications [as defined by 18 U.S.C. §2510(8)], nor does it include subscribers' names, addresses, or financial information.[228]

Although many of the details about the telephony metadata program remain cloaked from view, from what has been made public by the government, it appears that the Government takes all information obtained and feeds it into a bulk data set, which is then queried with an "identifier", referred to as a "seed"[229] The NSA uses both international and domestic identifiers.[230]

FISC requires that the NSA establish a "reasonable, articulable suspicion" that a seed identifier used to query the data be linked to a foreign terrorist organization before running it against the bulk data. Once obtained, information responsive to the query can be further mined for information. The NSA can analyze the data to ascertain second- and third-tier contacts, in steps known as "hops":

> The first "hop" refers to the set of numbers directly in contact with the seed identifier. The second "hop" refers to the set of numbers found to be in direct

---

[225] Electronic Frontier Foundation v. U.S. Dep't of Justice, No. 4:11-cv-05221-YGR, at 2, ¶1(b) (N.D. Cal. Jul. 19, 2013) (order responding to the request for records related to Section 215 as narrowed by negotiation between the parties in the litigation, i.e., orders and opinions of the FISC issued from January 1, 2004 to June 6, 2011, containing a significant legal interpretation of the government's authority or use of its authority under Section 215; and responsive "significant documents, procedures, or legal analyses incorporated into FISC opinions or orders and treated as binding by the Department of Justice or the National Security Agency.").

[226] *See, e.g.*, Section 215 White Paper, *supra* note 223, at 3 ("The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism."); *id.* at 4, "Query results can be further analyzed only for valid foreign intelligence purposes.")

[227] *Id.* at 2.

[228] But note that the same arguments brought by the government in support of the telephony metadata program would support building similar databases of subscribers' and customers' financial records. *See* Section 215 White Paper, *supra* note 223, at 3. In addition, the Aug. 9, 2013 White Paper is careful to note that the government does not collect cell phone locational information "pursuant to these orders." *Id.* However, the same arguments that support the telephony metadata program would support the collection of precisely this information under other FISC orders.

[229] Section 215 White Paper, *supra* note 223 at 3. Note that although the White Paper uses telephone numbers as an example of an identifier, it is conceivable that various other identifiers may be used. In a recently-released memorandum, for instance, the government refers to "bins" or "zip codes", suggesting that the types of queries can be significantly broad. *See* Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 9, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf. The Guardian, in turn, reports that the term "identifiers" includes information such as names, telephone numbers, email addresses, IP addresses, and usernames. *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. citizens' emails and phone calls*, THE GUARDIAN (Aug. 9, 2013, 12:08 PM), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (containing screen shot of classified document).

[230] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 8, 10, In re Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

> contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers.[231]

It appears that, initially, neither FISC nor the NSA limited the number of "hops" that could be undertaken. It was not until March 2009 that the Government implemented software changes to its system to limit the number of hops permitted to three.[232]

As a practical matter, what this means is that the NSA currently understands the primary order as authorizing the agency to retrieve information as many as three tiers away from the initial identifier.[233] The government refers to this process as "automated chaining."[234] These results can then be further queried "for foreign intelligence purposes."[235] In some cases, this information can then be forwarded to the FBI for further investigation, including using the information thus obtained for applications for an electronic intercept order under Title I of the Foreign Intelligence Surveillance Act.[236]

Like the programs that existed prior to the Church Committee hearings, the range of targets has gradually expanded. Following the initial order, on at least three occasions, the government obtained authorization to expand the telephone identifiers that the NSA could query.[237] And like the programs that led to the creation of FISA in the first place, a significant focus has been on domestic communications.

Since the advent of the program, FISC has understood "that the vast majority of the call-detail records provided are expected to concern communications that are (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[238] The government laid out its rationale:

> International terrorist organizations and their agents use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, terrorist operatives make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the homeland.[239]

The program is thus designed to obtain foreign intelligence or to protect against international terrorist threats in the United States and overseas. Under the statute, the

---

[231] Section 215 White Paper, *supra* note 223, at 3-4.

[232] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 20, In re Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

[233] Section 215 White Paper, *supra* note 223, at 4.

[234] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 10, In re Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

[235] Section 215 White Paper, *supra* note 223, at 4.

[236] *Id.*

[237] *See generally* Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 4 n. 3, In re Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("Authorizations after this matter was initiated in May 2006 expanded the telephone identifiers that NSA could query to those identifiers associated with [REDACTED] *see generally* docket number BR 06-05 (motion to amend in August 2006)...docket number BR 07-10 (motion to amend granted in June 2007). The Court's authorization in docket number BR 08-13 approved querying related to [REDACTED] Primary Order, docket number BR 08-13, at 8.").

[238] *Id.* at 2 n. 1.

[239] Section 215 White Paper, *supra* note 223, at 3.

data obtained is understood as "presumptively relevant to an authorized investigation" where the Government can establish that the information pertains to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation.[240]

Statutory requirements are designed to protect against the collection of information on U.S. persons. Indeed, the statute limits the scope to obtaining foreign intelligence information "not concerning a United States person".[241] Where a U.S. person is involved, it must specifically be "to protect against international terrorism or clandestine intelligence activities."[242]

Despite special protections, the collection of information relating to U.S. persons, who are not themselves the target of any investigation, is central to the program. Indeed, from the beginning, both the government and the Court were fully aware that, as a result of the broad approach—namely, the collection of all information, including that of a purely local nature—such information would be obtained.[243] "Ordinarily," Judge Reggie Walton later wrote, "this alone would provide sufficient grounds for a FISC judge to deny the application."[244] But in the face of Executive Branch claim, under oath, that the program was vital for U.S. national security, the Court acquiesced, requiring only that the Executive follow certain procedural protections.[245] These protections failed to prevent abuses.

The NSA's telephony metadata program contradicts FISA's language, design, and purpose. To understand it otherwise would be to vitiate the statute in terms of Congress' intent in introducing FISA and the general orientation of the statute, as well as the specific statutory restrictions placed on the intelligence agencies and duties assigned to the Foreign Intelligence Surveillance Court. The program also raises constitutional concerns with regard to search and seizure.

V. BULK COLLECTION RUNS CONTRARY TO FISA'S GENERAL APPROACH

The telephony metadata program violates the general intent of Congress in enacting FISA—and the approach adopted in the statute itself—in two important ways: first, in its

---

[240] 50 U.S.C. § 1861(b)(2)(A)(i)-(iii) (2006).

[241] § 1861(b)(2)(A).

[242] § 1861(b)(2)(A) (2006 & Supp. V. 2012).

[243] *Id. See* In re Prod. of Tangible Things From [REDACTED], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13, at 2 n. 1 (FISA Ct. Jan 28, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf ("As the government noted in its application, '[i]f authorized, the requested order will result in the production of call detail records pertaining to [REDACTED] telephone communications, including call detail records pertaining to communications of U.S. persons located within the United States who are not the subject of any FBI investigation.").

[244] In re Prod. of Tangible Things from [REDACTED], Order, No. BR 08-13 at 12 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[245] *Id.* (stating that the Court had authorized the bulk collection of call detail records based upon: "(1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and include specific oversight requirements. Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program. . .").

rejection of particularization at the point of acquisition of information; and, second, with regard to the role played by the Foreign Intelligence Surveillance Court.

A. Particularization in Place of Broad Surveillance

The telephony metadata program lacks the particularization that marks Congress' entire approach to domestic foreign intelligence gathering as articulated in the Foreign Intelligence Surveillance Act. Specifically, FISA rejects the wholesale collection of domestic information, insisting instead on minimization; relies on the *prior* targeting of foreign intelligence targets to justify surveillance; provides U.S. persons a heightened level of protection; and seeks to minimize the acquisition (not just the retention and dissemination) of information.

1. Wholesale Collection of Information

Project MINARET, which represented precisely the type of surveillance program that FISA was designed to forestall, was not nearly as extensive as the telephony metadata program at issue in this case. Over the course of Project MINARET, for instance, the watch list expanded to include approximately 1,650 U.S. citizens in total.[246] At no time were there more than 800 U.S. citizens' names on the list, out of a population of about 200 million Americans.[247]

Today, in contrast, there are approximately 316 million Americans, United States Census Bureau, U.S. and World Population Clock (Aug. 28, 2013), http://www.census.gov/popclock/, most of whom would have been subject to the Verizon (and similar) orders issued by the Foreign Intelligence Surveillance Court ("FISC"). This number eclipses the total number of U.S. citizens subject to one of the most egregious programs previously operated by the NSA, which gave rise to FISA in the first place.

The telephony program also goes substantially beyond the previous surveillance operation in its focus on calls of a purely local nature. According to the Director the National Security Agency, Project MINARET did not monitor entirely domestic conversations.[248]

In contrast, the Order issued in April 2013 by FISC specifically *requires* the collection of information "wholly within the United States, including local telephone calls."[249] Set to expire July 19, 2013, the Office of the Director of National Intelligence has confirmed that FISC has again renewed the order.[250]

As discussed above, Congress designed the statute to be used in *specific cases* of foreign intelligence gathering. By limiting the targets of electronic surveillance, requiring probable cause, disallowing investigations solely on the basis of otherwise protected first amendment activities, and insisting on minimization procedures, Congress sought to restrict agencies' ability to violate U.S. citizens' privacy. The business records provision built on this approach, adopting the *same definitions* that prevailed in other portions of the statute, and requiring that agencies obtain orders to collect information on individuals believed to be foreign powers or agents of a foreign power. Congress later deliberately

---

[246] *Id.*

[247] *Id.* at 30, 33-34.

[248] *Church Committee Report, Vol. 5, supra*, at 36 (testimony of General Lew Allen, Director, National Security Agency).

[249] In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., Secondary Order, No. BR 13-80 (FISA Ct. Apr. 25, 2013).

[250] Press Release, Office of the Dir. of Nat'l Intelligence, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/898-foreign-intelligence-surveillance-court-renews-authority-to-collect-telephony-metadata.

inserted "relevant" into the statute to ensure the continued specificity of targeted investigations.

In addition, Congress empowered the FISC to consider each instance of placing an electronic wiretap. The NSA's program, in contrast, delegates such oversight to the executive, leaving all further inquiries of the databases to the agency involved. Once the NSA collects the telephony metadata, it is the NSA (and not the FISC) that decides which queries to use, and which individuals to target within the database.

This change means that the FISC is not performing its most basic function: protecting U.S. persons from undue incursions into their privacy. Instead, it leaves the determination of whom to target to the agency's discretion. Traditional FISA, as well as authorities under §702, depend upon the criteria in the statute being met *prior to collection of information*. That is, the authorities apply at the moment data is acquired—not when it is subsequently analyzed for more information.

Although the government argues that intelligence is not acquired until it is mined for more information, or until a human operator is involved in the analysis, this is neither the statutory language nor the government's own internal position. The NSA's own minimization procedures with regard to §702 state:

> In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:
> (a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party...[251]

2. Prior Targeting to Justify Collection of Data

The government has indicated that the information obtained from this program is important because, "by analyzing it, the Government can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States."[252] The government sees the enormous number of records as central to the success of the program.[253] Once the records are obtained—i.e., once the "haystack" is created—the government can then go about finding out who the threats are—i.e., the proverbial needles in the haystack.[254]

This process is exactly backwards. The whole point of FISA is for the government to first identify the target, and then to use this to obtain information. In contrast, the government is now arguing that it can obtain information, as a way of figuring out who the targets should be. This runs directly contrary to FISA's design.

3. Heightened Protections for U.S. Persons

In addition, as detailed above, there are myriad ways in which FISA creates extra protections for U.S. persons. The statute itself came from revelations about the rather cavalier manner in which the intelligence agencies were treating Americans' right to

---

[251] Eric H. Holder, Jr., Att'y General of the United States, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (Jan. 8, 2007), *available at* http://epic.org/2013/06/nsa-targeting-and-minimization.html.

[252] Section 215 White Paper, *supra* note 223, at 2.

[253] *Id.* at 4 ("It would be impossible to conduct these queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries.").

[254] *See, e.g.*, How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence, 113th Cong. (2013) (testimony of Deputy Att'y Gen. James Cole), *available at* http://intelligence.house.gov/video/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries.

privacy. These protections related to the targeting of U.S. persons—not just the later analysis and dissemination of information.

Outside of minimization procedures relating to the downstream manipulation and dissemination of information, the telephony metadata program does not recognize any protection for U.S. persons at the moment of data acquisition. This, too, contradicts the way the statute was structured.

B. Role of the Foreign Intelligence Court

In at least three important ways, the Foreign Intelligence Surveillance Court no longer serves the purpose for which it was designed. First, it was created to determine whether sufficient evidence existed to target individuals within the United States, prior to the collection of such information. But the Court has abdicated this responsibility to the executive branch generally, and to the NSA in particular. Continued noncompliance underscores concern about relying on the intelligence community to protect the Fourth Amendment rights of U.S. persons. Second, Congress did not envision a law-making role for the Court. Its decisions were not to serve as precedent, nor was the Court to offer lengthy legal analyses, crafting in the process, for instance, exceptions to the Fourth Amendment warrant requirement or defenses of wholesale surveillance programs. Third, instead of being a neutral, disinterested magistrate, the court appears to have become representative of one political approach. Question exists about the extent to which it acts as an effective check on the exercise of surveillance authorities. The manner of appointment of judges, lack of technical expertise, and absence of an effective adversarial process has here impacted perceptions—and potentially the workings—of the Court.

1. Reliance on NSA to Ascertain Reasonable, Articulable Suspicion

FISC's primary order authorizing the collection of telephony metadata required that designated NSA officials make a finding that there is "reasonable, articulable suspicion" ("RAS") that a seed identifier proposed for query is associated with a particular foreign terrorist organization prior to its use. Documents recently released as a result of court orders in a related FOIA case establish that for nearly three years, the NSA did not follow these procedures[255]—despite the fact that numerous officials at the agency were aware of the violation.[256] Noncompliance incidents have continued. Collectively, these incidents raise serious question as to whether FISC is performing the functions it was designed to address.

a. Failure to Report Initial Noncompliance

---

[255] In re Prod. of Tangible Things From [Redacted], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13 (FISA Ct. Jan. 28, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf; *see also* DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA), Sept. 10, 2013, *available at* http://icontherecord.tumblr.com/.

[256] Declaration of Lieutenant General Keith B. Alexander at 25, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (listing seven people in the Signals Intelligence Directive, two from the Office of the General Counsel, and one additional person [REDACTED] who knew, or may have known of the problem since May 2006). Three additional people from the General Counsel's office and from SID became aware of the use of non-RAS-approved identifiers via email on May 25, 2006. *Id.* at 26. The DNI noted an additional "indeterminate number of other NSA personnel who knew or may have known the alert list contained both RAS and non-RAS selectors. *Id.* at 26-27.

Although the NSA had been acting in contravention of the order since May 2006, it was not until early 2009, when representatives of the Department of Justice met with NSA representatives to be briefed on the NSA's handling of the telephony metadata, that the illegal behavior was brought to FISC's attention.[257] During the briefing and in subsequent discussions, DOJ representatives inquired about the alert process. Learning of the process being used, DOJ personnel expressed concern that the program had been misrepresented to FISC.[258] The NSA had been using identifiers employed to collect information pursuant to Executive Order 12333—not FISA—to search the telephony database.[259]

DOJ informed FISC within a week of the meeting that the government had been querying the business records in a manner that contravened both the original order and sworn statements of several Executive Branch officials.[260] The Court was not amused.

---

[257] *Id.* at 27

[258] *Id.*

[259] NSA's general SIGINT authorities derive from (1) Exec. Order No. 12333, §1.7, 46 Fed. Reg. 59941 (Dec. 4, 1981) (authorizing the NSA to "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions"); (2) Foreign Wireless and Radio Monitoring, National Security Council Intelligence Directive 6 (Dec. 12, 1947) *available at* http://www.foia.cia.gov/sites/default/files/document_conversions/50/NSCID_No_6_Foreign_Wireless_and_Radio_Monitoring_12_Dec_1947.PDF (noting that the DCI shall conduct all Federal monitoring of foreign propaganda and press broadcasts required for the collection of intelligence information to meet the needs of all Departments and Agencies in connection with the National Security and that the DCI shall disseminate such intelligence information to the various Departments and Agencies which have an authorized interest therein); and (3) Department of Defense Directive 5100.20 (Jan. 26, 2010) *available at* http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf. ("[T]he National Security Agency (NSA) is the U.S. Government (USG) lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS (DIRNSA/CHCSS). NSA/CSS provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers. . ."). In addition, some, but not all, of the SIGINT activities undertaken by NSA are governed by FISA. Declaration of Lieutenant General Keith B. Alexander at 34, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

When executing its SIGINT mission, NSA is only authorized to collect, retain, or disseminate information concerning U.S. persons consistent with Attorney General guidelines. The current procedures approved by the AG are located in the Department Defense Regulation 5240.1-R, Procedures Governing the Activities of DOD Intelligence components that Affect United States Persons at 24-37 (Dec. 11, 1982), as well as a classified annex to the regulation overseeing NSA's electronic surveillance. Declaration of Lieutenant General Keith B. Alexander at 34, In Re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

To administer the program, the NSA constructed two lists: the first, an "alert list," includes all identifiers (foreign and domestic) of interest to counterterrorism analysts. Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 10, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf. The second, the "station table", is a historical listing of all telephone identifiers that had undergone a reasonable, articulable suspicion determination, including the results. *Id. But see* Declaration of Lieutenant General Keith B. Alexander at 9, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (referring to the first source as the "Address Database" and describing it as "a master target database of foreign and domestic telephone identifiers").

[260] In Re Prod. of Tangible Things From [REDACTED], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13, at 2 (FISA Ct. Jan 28, 2009), *available at*

Judge Reggie Walton expressed concern "about what appears to be a flagrant violation of its Order in this matter."[261] The NSA had repeatedly misled the Court in its handling of the database.[262] FISC immediately issued an order, directing the NSA to undertake a comprehensive review of the NSA's handling of telephony metadata.[263] It gave the government until Feb. 17, 2009 to file a brief to defend its actions and to help the Court to determine whether further action should be taken against the government or its representatives.[264]

The NSA initially admitted only "that NSA's descriptions to the Court of the alert list process . . . were inaccurate and that the Business Records Order did not provide the Government with authority to employ the alert list in the manner in which it did."[265] It further acknowledged, "the majority of telephone identifiers compared against the incoming BR metadata in the rebuilt alert list were not RAS-approved."[266] The actual numbers, reported to FISC in February 2009, were staggering: as of January 15, 2009, "only 1,935 of the 17,835 identifiers on the alert list were RAS-approved."[267]

It was not that the NSA was unaware of the requirements established by the statute and by the Court. The Attorney General had, consistent with the primary order, established minimization procedures, amongst which was the following:

> Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [REDACTED][3] More specifically, access to the archived data shall occur only when NSA has identified a known telephone number for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [REDACTED] organization; provided, however, that a telephone number believed to be used by a U.S. person shall not

---

http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf.

[261] *Id.* at 4.

[262] *See, e.g.*, OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 94 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("The management controls designed by the Agency to govern the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order.").

[263] In re Prod. of Tangible Things From [Redacted], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13 (FISA Ct. Jan. 28, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf.

[264] *Id.* at 2.

[265] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 2, In re Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

[266] *Id.* at 11; *see also id.* at 6. Note the NSA refers to FISC-authorized Business Record metadata as "BR metadata". In re Prod. of Tangible Things from [REDACTED], Order, No. BR 08-13, at 4 (FISA Ct. Mar. 2, 2009) *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[267] Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 at 11, In re Prod. of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf; *see also* Declaration of Lieutenant General Keith B. Alexander at 8, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

> be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.[268]

Nevertheless, apparently, neither the Signals Intelligence Directorate nor the Office of General Council had caught the fact that nearly 90 percent of the queries to the bulk dataset had been illegal.[269] Nor had they realized that their reports to FISC claiming that only RAS-approved numbers were being run against the bulk metadata were false.[270]

In the meantime, the NSA had disseminated 275 reports to the FBI as a result of contact chaining and queries of NSA's archive of telephony metadata.[271] Thirty-one of these had resulted directly from the automated alert process.[272] In a careful use of language, the government noted, "NSA did not identify any report that resulted from the use of a non-RAS-approved 'seed' identifier."[273] The government did not detail how complete the NSA had been in considering the reports; nor did it claim that none of the reports had resulted from non-RAS-approved identifiers.[274] The government also did not address the dissemination of metadata reports within NSA and subsequent actions taken as a result of the process.

---

[268] Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 at 4, (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (citing Order No. BT 06-05, at 5).

[269] *Id.* at 11 ("Based upon NSA's recent review, neither NSA SID nor NSA OGC identified the inclusion of non-RAS-approved identifiers on the alert list as an issue requiring extensive analysis.").

[270] *See, e.g.*, NSA Report to the FISC, Aug. 18, 2006, docket number BR 06-05 (Ex. B to the Government's application in docket number BR 06-08), at 12-15, quoted in Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 13, In re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which include foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the standard set forth in the Court's May 24, 2006 [Order]. . . . To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so."). *See also* Declaration of Lieutenant General Keith B. Alexander at 7, In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (reprinting the same report text and stating, "in short, the reports filed with the Court incorrectly stated that the telephone identifiers on the alert list satisfied the RAS standard. In fact, the majority of telephone identifiers included on the alert list had not been RAS approved. . .").

[271] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 17, In re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf; Declaration of Lieutenant General Keith B. Alexander at 42, In re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (further noting that the 275 reports provided to the FBI tipped a total of 2,549 telephone identifiers as being in contact with identifiers used to query the system).

[272] *Id.*

[273] *Id.* at 17.

[274] *See also* Declaration of Lieutenant General Keith B. Alexander at 36, In re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("[The NSA] has. . . conducted a review of all 275 reports of domestic contacts NSA has disseminated as result of contact chaining [REDACTED] of the NSA's Archive of BR FISA material. NSA has identified no report that resulted from the use of a non-RAS approved identifier as the initial seed identifier for chaining through the BR FISA material.") (internal footnotes omitted).

Despite the gross violation of FISC's order, the Government argued that FISC should neither rescind nor modify its order.[275] As required by FISC, the NSA had undertaken an end-to-end system engineering and process review (technical and operational) of the NSA's handling of BR metadata; it had undertaken a review of domestic identifiers to ensure that they are RAS-compliant; and it had undertaken an audit of all queries made of the BR metadata repository since November 1, 2008 with the purpose of determining if any queries had been made using non-RAS-approved identifiers.[276] The NSA had again trained its employees and adopted new technologies to limit the number of "hops" permitted from an RAS-approved seed identifier to three.[277] The government offered to take additional steps to avoid having the program shut down, all of which amounted to involving DOJ's National Security Division more deeply in the telephony metadata program.[278]

b. Further Noncompliance

Although the January 2009 incident represents the first admission of noncompliance that was made public, it is far from the first – or only – time that the NSA acted outside the scope of its authority to collect records under §215 of the USA PTRIOT Act.[279] Recently-released documents provide myriad further examples.

In September 2006, for instance, the NSA's Inspector General expressed concern that the agency was collecting more data than authorized under the order.[280] (The NSA had been obtaining 16-digit credit card numbers as well as names/partial names contained in the records of Operator-assisted calls.[281]) It later emerged that an over-collection filter inserted in July 2008 failed to function.[282]

---

[275] Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009 at 2, 15-21, In re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf. Note that No. BR 06-05 is the initial authorization of the telephony metadata program, May 24, 2006. No. BR-08 was a renewal application, filed Aug. 18, 2006. No. BR 08-13 is a subsequent authorization. The May 2006 order, however, has seven tabs for different docket numbers, all of which have been redacted, suggesting that there are other, related programs underway.

[276] *Id.* at 19.

[277] *Id.* at 20.

[278] *Id.* at 20-21 (listing under "Additional Oversight Mechanisms the government Will Implement": (1) NSA's OGC consulting with NSD on "all significant legal opinions that relate the interpretation, scope and/or implementation" of FISC orders related to BR 08-13; (2) NSA's OGC providing NSD with copies of the mandatory procedures; (3) NSA's OGC promptly providing NSD with copies of all formal briefing and/or training materials; (4) arranging meetings among NSA's OGC, NSD, and NSA's SID prior to seeking renewal of the orders; (5) meetings once per period of future orders between NSA's OIG and NSD; (6) review and approval of all proposed automated query processes prior to implementation).

[279] *See, e.g.*, Memorandum of the United States In Response to the Court's Order Dated Jan. 28, 2009, In Re Production of Tangible Things From [REDACTED], Docket Number BR 08-13, p. 19, *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf (Citing notice of compliance filed Jan. 26, 2009, which reports that between Dec. 10, 2008, and Jan. 23, 2009, two analysts conducted 280 queries using non-RAS-approved identifiers).

[280] OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 95-96 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("[M]anagement controls do not provide reasonable assurance that NSA will comply with the following terms of the Order: 'NSA may obtain telephony metadata, which includes comprehensive communications, routing information, including but not limited to session identifying information, trunk identifier, and time and duration of a call. Telephony metadata does not include the substantive content of any communications, or the name, address, or financial information of a subscriber or customer.'").

[281] OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE

On October 17, 2008, the government reported to FISC that, after FISC authorized the NSA to increase the number of analysts working with the BR metadata, and had directed that the NSA train the newly-authorized analysts, thirty one (out of 85) analysts subsequently queried the BR metadata in April 2008 *without even being aware that they were doing so*.[283] The upshot was that NSA analysts used 2,373 foreign telephone identifiers to query the BR metadata without first establishing reasonable, articulable suspicion.[284] Despite taking corrective steps, on December 11, 2008, the government notified the Court that an analyst had not installed a modified access tool and, resultantly, had again queried the data using five identifiers for which no reasonable articulable suspicion standard had been satisfied.[285]

Just over a month later, the government informed the Court that, between December 10, 2008 and January 23, 2009, two analysts had used 280 foreign telephone identifiers to query the BR metadata without first establishing RAS.[286]

The process initiated in January 2009 identified additional incidents where the NSA had failed to comply with FISC's orders.[287] In February 2009 the NSA brought two further matters to the court's attention. The first centered on the NSA's use of one of its analytical tools to query the BR metadata, using non-RAS-approved telephone numbers.[288] This tool had been used since the Court's initial Order in May 2006 to search both the BR metadata and other NSA databases.[289] Also in February 2009, the NSA notified NSD that NSA's audit had identified three analysts who conducted chaining the BR metadata using fourteen telephone identifiers that had not been RAS-approved before the queries.[290]

COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 96 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf

[282] In Re Production of Tangible Things from [REDACTED] Order, Docket No. BR 08-13, Mar. 2, 2009, p. 17, *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf (citing Government's Response to the Court's Order of Jan. 16, 2009, at 13).

[283] Order at 9, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[284] *Id.*

[285] *Id.* at 10 (citing Preliminary Notice of Compliance Incident at 2, No. BR 08-08, (FISA Ct. Dec. 11, 2008))

[286] *Id.* (citing Notice of Compliance Incident at 2, No. BR 08-13, (FISA Ct. Jan. 26, 2009).

[287] Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 (U), In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf; *see also* DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA), Sept. 10, 2013, *available at* http://icontherecord.tumblr.com/; Section 215 White Paper, *supra* note 223, at 5 ("Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered. . . The incidents, and the Court's responses, were. . . reported to the Intelligence and Judiciary Committees in great detail.")

[288] Notice of Compliance Incidents (U) at 2, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 26, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2026%202009%20Notification%20of%20Compliance%20Incident.pdf.

[289] *Id.* at 3.

[290] According to Keith Alexander's Supplemental Declaration, "One analyst conducted contact chaining queries on four non-RAS-approved telephone identifiers on November 5, 2008; A second analyst conducted one contact chaining query on one non-RAS-approved telephone identifier on November 18, 2008; and A third analyst conducted contact chaining queries on three non-RAS-approved telephone identifiers on December 31, 2008; one non-RAS approved identifier on January 5, 2009; three non-RAS approved identifiers on January 15, 2009; and two non-RAS approved identifiers on January 22, 2009." Supplemental Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of the National Security

In May 2009, two additional compliance issues arose.[291] The first compliance incident is completely redacted. The second notes a dissemination-related problem: namely, that the unminimized results of some queries of metadata had been "uploaded [by NSA] into a database to which other intelligence agencies. . . had access."[292] According to the government, providing other agencies access to this information may have resulted in the dissemination of U.S. person information in violation of both US Signals Intelligence Directive 18 as well as the more restrictive restrictions imposed by the Court in BR 09-06.[293]

c. FISC Response

Repeatedly, instead of rescinding prior collection programs, FISC merely imposed further requirements on the government.[294] By spring of 2009, the Court had become fed up with the NSA—yet, not enough to actually halt the program. Instead, it insisted on two procedures designed to give FISC greater insight into how the NSA was using and distributing information related to the telephony metadata: that NSA return to FISC prior to each query of the database; and that NSA file weekly reports with FISC detailing any dissemination of the information. Both protections proved temporary.

FISC's first temporary solution was to require what traditional FISA actually required: namely, NSA application to FISC prior to targeting. Between institution of the review and the final report, FISC required the NSA to seek approval to query the database on a case-by-case basis. The Court was particularly concerned that the NSA had averred that having access to all call detail records,

> "is vital to NSA's counterterrorism intelligence mission" because "[t]he only effective means by which NSA analysts are able continuously to keep track of [REDACTED] and all affiliates of one of the aforementioned entities [who are taking steps to disguise and obscure their communications and identities], is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered."[295]

According to FISC, the NSA had also suggested that:

Agency at 8, In Re Production of Tangible Things, No. BR 08-13 (FISA Ct. Feb. 25, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2026%202009%20Notification%20of%20Compliance%20Incident.pdf.

[291] Order at 4, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 09-06 (FISA Ct. June 22, 2009) (referencing Government responses to the Court's May 29, 2009 Supplemental Order), *available at* http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf.

[292] *Id.* at 5 (quoting Preliminary Notice of Compliance Incident at 2, No. BR 09-06 (FISA Ct. June 16, 2009), in Docket No. BR 09-06, at 2.

[293] *Id.*

[294] The government cites multiple other cases, with key information redacted as follows: "[REDACTED] Primary Order, docket number [REDACTED] at 11-12 (requiring, in response to an incident of non-compliance, NSA to file with the Court every thirty days a report discussing, among other things, queries made since the last report to the Court and NSA's application of the relevant standard); see also [REDACTED] docket numbers [FULL LINE REDACTED] (prohibiting the querying of data using "seed" accounts validated using particular information)." Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009 (U) at 16, In Re Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

[295] Order at 2, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009) (quoting Application Exhibit A, Declaration of [REDACTED], Signals Intelligence Directorate Deputy Program Manager [REDACTED], NSA at 5, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Dec. 11, 2008)), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

> "[t]o be able to exploit metadata fully, the data must be collected in bulk. . . The ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of [REDACTED]."[296]

Because the Order being sought meant, if granted, that the NSA would be collecting call detail records of U.S. persons located within the United States, who were not themselves the target of any FBI investigation and whose metadata could not otherwise be legally obtained in bulk, FISC had adopted minimization procedures. It had required, inter alia, that:

> Access to the archived data shall occur only when NSA has identified a known telephone identifier for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone identifier is associated with [REDACTED].[297]

The Court had a difficult time believing the NSA's claim that its non-compliance with the Court's orders resulted from NSA personnel believing that the Court's restrictions on access to the BR metadata only applied to "archived data" (namely, data located in certain databases). "That interpretation of the Court's Orders," Judge Reggie Walton wrote, "strains credulity."[298] The NSA had compounded its bad behavior by repeatedly submitting inaccurate descriptions of how it developed and used the alert list process.[299] In return for its claim that the program was vital for U.S. national security, the NSA had offered as evidence the rather paltry claim that, after nearly three years of sweeping up all telephony metadata, the NSA had generated 275 domestic security reports that, in turn, had spurred three preliminary investigations.[300]

FISC objected to the government's assertion that "the Court need not take any further remedial action"[301] Until the NSA completed the review, "the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation – on February 18, 2009 – will be the last."[302] Accordingly, starting in March 2009, while the NSA could continue to collect data and to test the telephony metadata system, it would only be allowed to query it with a Court order—or, in an emergency, to query the database and then to inform the court by 5:00 pm, Eastern Time, on the next business day.[303] In September 2009, however, FISC lifted the requirement for the NSA to seek approval in every case.

The second protection introduced by FISC was, starting on July 3, 2009, to require the NSA to file a weekly report with the Court, listing each time, over the seven-day period ending the previous Friday, in which the NSA had shared, "in any form, information obtained or derived from the [REDACTED] BR metadata collections with

---

[296] *Id.* (quoting Application Exhibit A, Declaration of [REDACTED], Signals Intelligence Directorate Deputy Program Manager [REDACTED], NSA at 5–6, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Dec. 11, 2008)).

[297] *Id.* at 3 (referencing re-authorization to BR 08-13, dating from Dec. 12, 2008).

[298] *Id.* at 5.

[299] *Id.* at 6.

[300] *Id.* at 13 ("the mere commencement of a preliminary investigation, by itself, does not seem particularly significant. . . The time has come for the government to describe to the Court how, based on the information collected and analyzed during [the duration of the program], the value of the program to the nation's security justifies the continued collection and retention of massive quantities of U.S. person information.")

[301] *Id.* at 14 (quoting Notice of Compliance Incident at 6, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 26, 2009)).

[302] *Id.* at 16.

[303] *Id.* at 18–19.

anyone outside NSA." Again, consistent with traditional FISA, the Court added special protections for U.S. persons:

> For each such instance, the government shall specify the date on which the information was shared, the recipient of the information, and the form in which the information was communicated (e.g., written report, email, oral communication, etc.). For each such instance in which U.S. person information has been shared, the Chief of Information Sharing of NSA's Signals Intelligence Directorate shall certify that such official determined, prior to dissemination, the information to be related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance.[304]

In August 2009 the government submitted its end-to-end assessment of the NSA telephony metadata system.[305] FISC lifted its requirements, leaving dissemination decisions in the future up to the NSA. It is at least questionable the extent to which the requirements with which the NSA was left perform an effective check on the exercise of authorities. Prior to the dissemination of information of U.S. persons' information outside the Agency, an NSA official must determine that the information is "related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance."[306] Since the government already considers all of the information in the database to be relevant to counterterrorism investigations, and has already argued to FISC (and FISC as agreed), that the collection of such data is necessary to understand its counterterrorism information, the degree to which this really prevents such dissemination is open to question.

d. Technological Gap

A critical part of FISC's failure to provide effective oversight of the process relates to the Court's decision to have the NSA perform the targeting decision. Part of the problem also stems from the court's discomfort with the technological aspects of the collection and analysis of digital information. For much of the discussion of noncompliance incidents, for instance, it appears that neither the NSA nor FISC has an adequate understanding of how the algorithms operate. Neither did they understand the type of information that had been incorporated into different databases, and whether they had been subjected to the appropriate legal analysis prior to data mining.

A similar problem may accompany the reporting requirements to Congress. In March 2009, for example, the Department of Justice had submitted several FISC opinions and Government filings relating to the discovery and remediation of compliance incidents in its handling of bulk telephony metadata to the Chairmen of the Intelligence and Judiciary Committees.[307] A subsequent letter noted that the House and Senate Intelligence and

---

[304] Order at 7, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-06 (FISA Ct. June 22, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf.

[305] Report of the United States, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-09, (FISA Ct. Aug. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf.

[306] Section 215 White Paper, *supra* note 223, at 5.

[307] Letter from M. Faith Burton, Acting Assistant Attorney General, to the Hon. Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate; the Hon. Dianne Feinstein, Chairman, Select Committee on Intelligence, U.S. Senate, the Hon. John Conyers, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, the Hon. Silvestre Reyes, Chairman, Permanent Select committee on Intelligence U.S. House of Representatives, Mar. 5, 2009, *available at* http://www.dni.gov/files/documents/section/pub_Mar%205%202009%20Cover%20Letter%20to%20Chairman%20of%20Intel%20and%20Judiciary%20Committees.pdf.

Judiciary Committees had received briefings in March, April, and August, before receiving a copy of the NSA's review in September 2009.[308] To the extent that the representations of the agency are heavily dependent on technical knowledge, the implications may not be readily transparent to lawmaker.

2. Detailed Legal Reasoning and Creation of Precedent

To enforce the specialized probable cause standard encapsulated in the Foreign Intelligence Surveillance Act, Congress created a court of specialized but exclusive jurisdiction.[309] Its job was, narrowly, to ascertain whether sufficient probable cause existed for a target to be considered a foreign power, or an agent thereof, whether the applicant had provided the necessary details for the surveillance, and whether the appropriate certifications and findings had been made. It is thus surprising that the government considers these orders now to be evidence of precedent, on the basis of which, it argues, the programs are legal.[310] But even more surprising is the recent public discovery that the Foreign Intelligence Surveillance court has greatly broadened the "special-needs" exception to the Fourth Amendment to embrace wholesale data collection. [311] What is emerging is a complex body of law, establishing doctrines unrecognized by the Supreme Court, which is considered precedent for future applications to FISC.

Specifically, in 2008 FISCR looked back at its decision in *In re Sealed Case* to confirm "the existence of a foreign intelligence exception to the warrant requirement."[312] It acknowledged that FISCR had "avoided an express holding that a foreign intelligence exception exists by assuming arguendo that whether or not the warrant requirements were met, the statute could survive on reasonableness grounds."[313]

In *In Re Directives*, FISCR went on to determine that, as a federal appellate court, in the Fourth Amendment context, it would "review findings of fact for clear error and legal conclusions (including determinations about the ultimate constitutionality of government searches or seizures) de novo." [314] It then asserted, for the first time, a foreign intelligence surveillance exception to the Fourth Amendment:

> The question. . . is whether the reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States. Applying principles derived from the special needs cases, we

---

[308] DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA), Sept. 10, 2013, *available at* http://icontherecord.tumblr.com/; and Letter from Ronald Weich, Assistant Attorney General, to the Hon. Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate; the Hon. Dianne Feinstein, Chairman, Select Committee on Intelligence, U.S. Senate, the Hon. John Conyers, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, the Hon. Silvestre Reyes, Chairman, Permanent Select committee on Intelligence U.S. House of Representatives, Sept. 3, 2009, *available at* http://www.dni.gov/files/documents/section/pub_Sep%203%202009%20Cover%20letter%20to%20Chairman%20of%20the%20Intelligence%20and%20Judiciary%20Committees.pdf.

[309] *See* Theodore W. Ruger, *Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 244 (2007).

[310] *Hearing on Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Program before the S. Judiciary Comm.*, 118th Cong. (July 31, 2013).

[311] *See also* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, NEW YORK TIMES, July 7, 2013, at A1.

[312] In Re Directives [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1010 (FISA Ct. of Rev. 2008).

[313] *Id.*

[314] *Id.* at 1009.

> conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception.[315]

The court analogized the exception to the 1989 Supreme Court consideration of the warrantless drug testing of railway workers, on the grounds that a minimal intrusion on privacy could be justified by the government's need to respond to an overriding public danger.[316]

The government subsequently cited *In re Directives* decision in its August 9, 2013 *White Paper*, defending the telephony metadata program, in support of an exception to the Fourth Amendment warrant requirement.[317]

The Foreign Intelligence Surveillance Court continues to go beyond its mandate. In August 2013, for instance, the Court issued a 29-page Amended Memorandum Opinion regarding the July 18, 2013 application by the FBI for the telephony metadata program.[318] Appending the 17-page order to the opinion, Judge Claire V. Eagan considered Fourth Amendment jurisprudence, the statutory language of Section 215, and the canons of statutory construction, to justify granting the order.[319]

Similarly, in a per curiam opinion of 2002, FISCR suggested "this case raises important questions of statutory interpretation, and constitutionality. After a careful review of the briefs. . . we conclude that FISA, as amended by the Patriot Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."[320]

Congress did not design the Foreign Intelligence Surveillance Court or the Court of Review to develop its own jurisprudence. Particularly in light of the lack of adversarial process, it is deeply concerning that the Court's decisions have taken on a force of their own.

3. Judicial Design

Congress tried to construct an even-handed, neutral arbiter by requiring that (a) the FISC judges be selected by the Chief Justice of the Supreme Court from at least seven different federal districts; (b) the judges serve staggered terms of up to seven years; and (c) having once served, such judges are ineligible for further service.[321] To ensure diversity, any federal district court judge (including a senior judge), who has not previously served on FISC, may be selected.[322] The Foreign Intelligence Surveillance Court of Review, in turn, is comprised of judges selected by the Chief Justice.[323]

This system has been called into question on two grounds: first, in the lack of diversity with regard to the appointment of judges to the court and, second, with regard to the high rate of applications being granted by FISC. Some observers point to these characteristics to question how effectively FISC operates as a check on the executive exercise of power. The observations are important, but without more information, it is difficult to determine the extent to which the current state of affairs has substantively impacted the process.

---

[315] *Id.* at 1011.
[316] Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 620 (1989).
[317] Section 215 White Paper, *supra* note 223, at 15.
[318] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible things from [REDACTED], No. BR 13-109 (FISC. 2013).
[319] *Id.*
[320] In Re Sealed Case No. 02-002, (FISA Ct. of Rev., Sept. 9, 2002).
[321] 50 U.S.C. § 1803e -d (2006 & Supp. V 2011).
[322] 50 U.S.C. § 1803a (2006 & Supp. V 2011).
[323] 50 U.S.C. § 1803b (2006 & Supp. V 2011).

a. Appointments

To the extent that political ideology reflects in the appointments process, the court is heavily weighted towards one side of the political spectrum. The past two Chief Justices have been appointed by Republican presidents, and their selections for the FISC and FISCR have strongly favored judges that have been nominated by Republican Administrations. (See *Fig. 1*) Only one of the current eleven judges serving on FISC is a Democratic nominee. Over the past decade, of the 20 judges appointed to FISC and FISCR, only three have been democratic nominees to the bench.

While, as a presentational matter, this raises question about the even-handedness of the FISC appointments process, it would be premature to draw too many substantive conclusions based solely on the political makeup of the bench. Any meaningful examination of how it influences the outcome of cases would need to compare either decisions reached by FISC with other, more diverse, courts, or the individual decisions reached by FISC judges with decisions reached by judges appointed by the opposing party.

The problem with such studies is that they would be almost impossible to conduct. FISC opinions are classified. Beyond this, they are *sui generis*, in that it is the only court that considers FISA applications. It also may be that there are externalities that influence which judges opt for membership of FISC—i.e., it may be that more Republican appointees than Democratic appointees inquire or make clear that they would be interested in serving on FISC. No studies have yet been done demonstrating why the appointments process aligns with political party—making any conclusions as to the effect, absent more information, somewhat arbitrary.

To the extent that political ideology enters into the equation, the way in which it has interacted with the court's role in establishing precedent deserves notice, as it undermines the appearance of a neutral arbiter and emphasizes deference to and support for greater power for the executive. According to the public record, FISCR, for instance, has only met twice: once in 2002 and once in 2008.[324] On both occasions, the panels were constituted entirely of Republican appointees, some of whom had publicly argued that FISA was an unconstitutional usurpation of executive power.

Laurence Silberman, from the DC Circuit, testified to Congress in 1978 (when FISA was being debated) that the legislation violated the U.S. Constitution.[325] Silberman, who had previously served as Deputy Attorney General, was "absolutely convinced that the administration bill, if passed, would be an enormous and fundamental mistake which the congress and the American people would have reason to regret."[326] For Silberman, the judiciary's role in any national security electronic surveillance should be circumscribed. He explained,

> I find the notion that the President's constitutional authority to conduct foreign affairs and to command the armed forces precludes congressional intervention into the manner by which the executive branch gathers intelligence, by electronic or other means, to be unpersuasive, and in that respect I agree with my colleague here to the left. But to concede the propriety of a congressional role in this matter is by no means—and this is the burden of my testimony—to concede the

[324] *See* In re Sealed Case, 310 F.3d 717, (FISA. Ct. Rev. 2002); In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

[325] *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, 9745, 7308, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess. 221 (1978) (statement of Laurence H. Silberman, Feb. 8, 1978).

[326] *Id.*

propriety or constitutionality of the judicial role created by the administration's bill.[327]

The chief concern was not a so-called "imperial Presidency", but the advent of an "imperial judiciary." The authorities transferred to FISC thus represented an unconstitutional erosion of executive power.[328] Another FISC judge, Ralph Guy, similarly argued as a U.S. attorney for the government in *U.S. v. U.S. District Court* that the president did not need any type of a warrant to engage in national security surveillance.[329]

Along with Judge Leavy, a Reagan appointee, Silberman and Guy heard the first appeal in the history of FISA—issuing a decision that made it possible for the government to use the looser restrictions in FISA even in cases where the primary purpose of the investigation was criminal in nature.[330] The FISCR panel that appears to have created a foreign intelligence exception to the Fourth Amendment warrant requirement similarly lacked a diverse political base. It included Chief Judge Selya and Senior Circuit Judges Winter and Arnold—the first two appointees of Ronald Reagan and the last of George H.W. Bush.

To the extent that political appointments stand in as a proxy for political ideologies, such as greater deference to the executive branch, the lack of diversity in the appointments process—especially in regard to some of the most important and far-reaching secret decisions issued by the court—raises important questions about the extent to which FISC, as conceived by Congress, is performing in a role as neutral arbiter. Without more detailed information about the judicial process, however—much of which could not, under the current system, be studied—the extent to which this is the case as a substantive matter remains in question.

JUDGES APPOINTED TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND COURT OF REVIEW BY ORIGINAL APPOINTMENT TO THE BENCH[331]

District Judge	Court	Dates of appointment	Appointing President
Rosemary M. Collyer*	FISC	3/8/2013 – 3/7/2020	George W. Bush
Claire Eagan*	FISC	2/13/2013 – 5/18/2019	George W. Bush
Michael W. Mosman*	FISC	5/4/2013 – 5/3/2020	George W. Bush
Raymond J. Dearie*	FISC	7/2/2012 – 7/1/2019	Ronald Reagan
William C. Bryson**	FISCR	12/1/2011 – 5/18/2018	Bill Clinton
Jennifer B. Coffman	FISC	5/19/2011 – 1/8/2013	Bill Clinton
F. Dennis Saylor IV*	FISC	5/19/2011 – 5/18/2018	George W. Bush
Martin L.C. Feldman*	FISC	5/19/2010 – 5/18/2017	Ronald Reagan
Susan Webber Wright*	FISC	5/19/2009 – 5/18/2016	George H.W. Bush
Thomas Hogan*	FISC	5/19/2009 – 5/18/2016	Ronald Reagan
Morris Arnold**	FISCR	6/13/2008 – 5/18/2015	George H.W. Bush
James Zagel*	FISC	5/19/2008 – 5/18/2015	Ronald Reagan
Mary A. McLaughlin*	FISC	5/19/2008 – 5/18/2015	Bill Clinton
Reggie Walton*	FISC	5/19/2007 – 5/18/2014	George W. Bush
Roger Vinson	FISC	5/4/2006 – 5/3/2013	Ronald Reagan

[327] *Id.* at 219.
[328] *Id.*
[329] *United States v. U.S. Dist. Ct. for the E. Dist. of Mich.*, 407 U.S. 297 (1972).
[330] In re Sealed Case, 310 F.3d 717 (2002)..
[331] Dates of appointment obtained from the Federation of American Scientists, available at http://www.fas.org/.

John D. Bates	FISC	2/22/2006 – 2/21/2013	George W. Bush
Bruce M. Selya	FISCR	5/19/2005 – 5/18/2012	Ronald Reagan
Malcolm Howard	FISC	5/19/2005 – 5/18/2012	Ronald Reagan
Frederick J. Scullin	FISC	5/19/2004 – 5/18/2011	Ronald Reagan
Dee Benson	FISC	4/8/2004 – 4/7/2011	George W. Bush
Ralph Winter	FISCR	11/14/2003 – 5/18/2010	Ronald Reagan
George Kazen	FISC	7/15/2003 – 5/18/2010	Jimmy Carter
Robert Broomfield	FISC	10/1/2002 – 5/18/2009	Ronald Reagan
Colleen Kollar-Kotelly	FISC	5/19/2002 – 5/18/2009	Bill Clinton
James G. Carr	FISC	5/19/2002 – 5/18/2008	Bill Clinton
James Robertson	FISC	5/19/2002 – 12/19/2005	Bill Clinton
John Edward Conway	FISC	5/19/2002 – 10/30/2003	Ronald Reagan
Edward Leavy	FISCR	9/25/2005 – 5/18/2008	Ronald Reagan
Nathaniel M. Gorton	FISC	5/19/2001 – 5/18/2008	George W. Bush
Claude M. Hilton	FISC	5/18/2000 – 5/18/2007	Ronald Reagan
Michael J. Davis	FISC	5/18/1999 – 5/18/2006	Bill Clinton
Ralph B. Guy, Jr.	FISCR	10/8/1998 – 5/18/2005	Gerald Ford
Harold A. Baker	FISC	5/18/1998 – 5/18/2005	Jimmy Carter
Stanley S. Brotman	FISC	7/17/1997 – 5/18/2004	Gerald Ford
William Stafford	FISC	5/19/1996 – 5/18/2003	Gerald Ford
Royce C. Lamberth	FISC	5/19/1995 – 5/18/2002	Ronald Reagan
Laurence Silberman	FISCR	6/18/1996 – 5/18/2003	George W. Bush
Paul Roney	FISCR	9/13/1994 – 05/18/2001	Richard Nixon
John F. Keenan	FISC	7/27/1994 – 5/18/2001	Ronald Reagan
James C. Cacheris	FISC	9/10/1993 – 5/18/2000	Ronald Reagan
Earl H. Carroll	FISC	2/23/1993 – 5/18/1999	Jimmy Carter
Charles Schwartz Jr.	FISC	8/5/1992 – 5/18/1998	Gerald Ford
Bobby Ray Baldock	FISCR	6/17/1992 – 5/18/1998	Ronald Reagan
Ralph G. Thompson	FISC	6/11/1990 – 5/18/1997	Gerald Ford
Frank Freedman	FISC	5/30/1990 – 5/19/1994	Richard Nixon
Wendell A. Miles	FISC	9/21/1989 – 5/18/1996	Richard Nixon
Robert W. Warren	FISCR	10/30/1989 – 5/18/1996	Richard Nixon
Sidney Aronovitz	FISC	6/8/1989 – 5/18/1992	Gerald Ford
Joyce H. Green	FISC	5/18/1988 – 5/18/1995	Jimmy Carter
Conrad K. Cyr	FISC	5/18/1987 – 11/20/1989	Ronald Reagan
Collins Seitz	FISCR	3/19/1987 – 3/18/1994	Lyndon B. Johnson

** Denotes current members of FISC*
***Denotes current members of FISCR*

Figure 1

b. Order Rate

Augmenting the lack of diversity in terms of appointments to FISC and FISCR is the rather notable success rate enjoyed by the government in its applications to the court. Scholars have noted that it is "unparalleled in any other American court."[332] Over the first two and a half decades, for instance, FISC approved nearly every single application without any modification.[333] Between 1979 and 2003, FISC denied only 3 out of 16,450 applications.[334]

---

[332] Ruger, *supra* note 246, at 245.

[333] *See* 1 KRIS & WILSON, *supra* note 139, at 469. .; Letter from Attorney General William French Smith to Director, Administrative Office of the U.S. Courts(Apr. 22, 1981, *available at*

Looking more recently, since 2003, FISC has issued a ruling on 18,473 applications for electronic surveillance and/or physical search (2003-2008), and electronic surveillance (2009-2012). (See *Fig. 2*) Court supporters note that a significant number of these applications are either modified or withdrawn by the government prior to FISC ruling. But even here, the numbers are quite low: 493 modifications still only comes to 2.6% of the total number of applications. Simultaneously, only 26 applications have been withdrawn by the government prior to FISC ruling. (See *Figure 2*).

These numbers do speak to the presence of informal processes, whereby FISC appears to be influencing the contours of applications. Without more information about the types of modifications that are being required, however, it is impossible to gauge either the level of oversight or the extent to which FISC is altering the applications.

Critics also point to the risk of capture presented by in camera, ex parte proceedings, and note that out of 18,473 rulings, FISC has only denied eight in whole and three in part. Whatever the substantive effect might be, the presentational impact is of note.

FISC RULINGS ON ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH (2003-2008) AND ELECTRONIC SURVEILLANCE (2009 – 2012)[335]

Year	# of Applications on which FISC ruled	# Approved	# Modified	# Denied in Part	# Denied in Whole	# w/drawn by Gov't prior to FISC ruling
2003[336]	1,727	1,724	79	0	3[337]	0
2004[338]	1,756[339]	1,756	94	0	0	3
2005[340]	2,072[341]	2,072	61	0	0	2
2006[342]	2,176[343]	2,176	73	1	0	5
2007[344]	2,371	2,370	86	1	3[345]	0
2008[346]	2,082	2,083[347]	2	0	1	0

http://www.fas.org/irp/agency/doj/fisa/1980rept.html ("No orders were entered which modified or denied the requested authority, except one case in which the Court modified an order and authorized an activity for which court authority had not been requested.")

[334] Laura K. Donohue, The Cost of Counterterrorism: Power, Politics and Liberty 232 (2008).

[335] Starting in 2009, the Department of Justice began providing the breakdown of the number approved, modified, denied in part, denied in whole, or withdrawn by the government prior to the FISC ruling only for those applications involving electronic communications. Prior to that time, these numbers were combined.

[336] Letter from William E. Moschella, Assistant Attorney Gen., to Mr. L. Ralph Mecham, Dir., Admin. Office of the U. S. Courts (Apr. 30, 2004), , *available at* https://www.fas.org/irp/agency/doj/fisa/2003rept.pdf.

[337] An addition application was initially denied but later approved. *Id.*

[338] Letter from Office of Legislative Affairs, U.S. Department of Justiee, to The Honorable J. Dennis Hastert, Speaker, U.S. House of Representatives, (Apr. 1, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/2004rept.pdf.

[339] 1758 submitted, 3 of which were withdrawn prior to FISC ruling and 1 of which was resubmitted. *Id.*

[340] Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to The Honorable J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 28, 2006), *available at* https://www.fas.org/irp/agency/doj/fisa/2005rept.html.

[341] 2,074 submitted, 2 of which were withdrawn prior to FISC ruling, and 1 of which was resubmitted. *Id.*

[342] Letter from Richard A. Hertling, Acting Assistant Attorney Gen., to the Honorable Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 27, 2007) , *available at* https://www.fas.org/irp/ageney/doj/fisa/2006rept.pdf.

[343] 2,181 submitted, 5 of which were withdrawn prior to FISC ruling. *Id.*

[344] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justiee, to the Honorable Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 30, 2008), *available at* https://www.fas.org/irp/agency/doj/fisa/2007rept.pdf.

[345] Discrepancy in the numbers stems in part from holdover applications and denials. Two applications, for instance, filed in CY 2006 were not approved until 2007. *Id.*

2009[348]	1,321[349]	1,320	14	1	1	8
2010[350]	1,506[351]	1,506	14	0	0	5
2011[352]	1,674[353]	1,674	30	0	0	2
2012[354]	1,788[355]	1,788	40	0	0	1
Totals	***18,473***	***18,469***	***493***	***3***	***8***	***26***

Figure 2

Setting modifications aside for the moment, the deference that appears to exist with regard to straight denials or granting of orders seems to extend to FISC rulings with regard to business records. Almost no attention, however, has been paid to this area. It appears that FISC has *never* denied an application for an order under this section. That is, of 751 applications since 2005, all 751 have been granted. (See *Fig. 3*)

ORDERS FOR THE PRODUCTION OF TANGIBLE GOODS

Year	**Number of Applications to FISC under 50 USC 1862(c)(2)**	**Number of Applications Granted by FISC**
2005[356]	155	155
2006[357]	43	43

[346] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Majority Leader, U.S. Senate (May 14, 2009) *available at* https://www.fas.org/irp/agency/doj/fisa/2008rept.pdf.

[347] Discrepancy in the numbers stems in part from holdover applications and denials. Two applications filed in CY 2007 were not approved until CY 2008).

[348] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to The Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2010), *available at* https://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.

[349] For the first time since 2003, no numbers are available for modifications/denials for the full number of applications submitted (physical search, electronic surveillance, and combined applications). Instead, the report notes that of the 1,376 in total submitted in the former three categories, 1,329 were related to electronic surveillance. It was eight of these applications that were withdrawn, 1 denied in whole, 1 denied in part, and 14 modifications, with 1,320 approved. The number of applications is thus missing the numbers for physieal search and physical search combined applications. *Id.*

[350] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Majority Leader, U.S. Senate, (Apr. 29, 2011), *available at* https://www.fas.org/irp/agency/doj/fisa/2010rept.pdf.

[351] Total number of electronic surveillance, physical search, and combined applications was 1,579. The report, however, isolates the electronic applications (1,511), and provides breakdowns for modifications, denials, etc., for just that category. Of the total of 1,511, five were withdrawn by the Government prior to FISC ruling. *Id.*

[352] Letter from Ronald Weich, Assistant Attorney Gen., to The Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), , *available at* https://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[353] Note that there were 1,745 total applications that included electronic surveillance and/or physical searches for foreign intelligence purpose. It appears that approximately 70 of the orders related solely to physical search, since the breakdown for electronic surveillance is only done for the 1,674. Two of the initial orders were withdrawn prior to FISC ruling. *Id.*

[354] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., to the Honorable Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), *available at* https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.

[355] The government made a total of 1,856 applications for electronic surveillance and/or physical searches; of those, 1,789 included requests for electronic surveillance. Of those, one was withdrawn by the Government prior to FISC ruling. *Id.*

[356] Letter from William E. Moschella, Assistant Attorney Gen., to the Honorable Richard B. Cheney, President, United States Senate (Apr. 28, 2006), *available at* http://www.justice.gov/nsd/foia/foia_library/2005fisa-ltr.pdf.

[357] Letter from Richard A. Hertling, Acting Assistant Attorney Gen., to the Honorable Richard B. Cheney, President, United States Senate (Apr. 27, 2007), *available at* http://www.justice.gov/nsd/foia/foia_library/2006fisa-ltr.pdf.

2007[358]	6	6
2008[359]	13	13
2009[360]	21	21
2010[361]	96	96
2011[362]	205	205
2012[363]	212	212
Totals	***751***	***751***

Figure 3

It is important to underscore that the lack of more contextual data cautions against drawing too much, however, from the nonexistent rate of denial. For one, Congress tied the Court's hands, *requiring* FISC to grant applications once the statutory conditions are met.[364] To the extent, then, that FISC is deferential to the executive, responsibility lays at least in part at the door of the legislature.

For another, it is almost impossible to tell, outside of the classified world, the extent to which the Court pushes back on the Department of Justice—not just in regard to specific orders, but in relation to broader rules and procedures, as well as in an oversight capacity. Two examples come to mind.

In 2010, John D. Bates, the Presiding Judge of FISC issued a declassified *Rules of Procedure*, requiring notice and briefing of novel issues before the court.[365] This document suggested that FISC would not, in the future, simply accept applications in new areas of the law, without first considering the underlying legal issues.

In addition, the recently-released judicial opinions from 2009, in turn, suggest that FISC was pressuring the NSA with regard to their failure to ensure that the identifiers run against the database be subjected to a test of reasonable, articulable suspicion. The Court was clearly uncomfortable with the pattern of misinformation that had marked the government's previous representations to FISC. With that said, however, these same documents also reveal the extent to which the court relies on the NSA to police its own activities—again raising question about the extent to which FISC adequately performs the role envisioned for it.

---

[358] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., to the Honorable Richard B. Cheney (Apr. 30, 2008), *available at* http://www.justice.gov/nsd/foia/foia_library/2007fisa-ltr.pdf.

[359] Letter from Ronald Weich, Assistant Attorney Gen.l, to the Honorable Joseph R. Biden, Jr., President, United States Senate (May 14, 2009), *available at* http://www.justice.gov/nsd/foia/foia_library/2008fisa-ltr.pdf.

[360] Letter from Ronald Weich, Assistant Attorney Gen., to the Honorable Joseph R. Biden, Jr., President, United States Senate (Apr. 30, 2010), *available at* http://www.justice.gov/nsd/foia/foia_library/2009fisa-ltr.pdf.

[361] Letter from Ronald Weich, Assistant Attorney Gen., Department of Justice, to the Honorable Joseph R. Biden, Jr., President, U.S. Senate(Apr. 29, 2011), *available at* http://www.justice.gov/nsd/foia/foia_library/2010fisa-ltr.pdf.

[362] Letter from Ronald Weich, Assistant Attorney Gen., Department of Justice, to the Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), *available at* http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf.

[363] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., Department of Justice, , to the Honorable Joseph R. Biden, Jr., President, U.S. Senate(Apr. 30, 2013), *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf.

[364] 50 U.S.C. §1861c(1) (2006) ("Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b), the judge *shall* enter an ex parte order as requested, or as modified approving the release of tangible things.") (emphasis added)

[365] FISA Ct. R. 11, *available at* https://www.fas.org/irp/agency/doj/fisa/fiscrules-2010.pdf. The current rules, issued November 1, 2010, superseded 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.*

As a final note, it is important to recognize that the sheer volume of the numbers associated with the tangible goods provisions (751) are remarkable not least because any one order, as we have seen with the telephony metadata program, could result in the collection of millions of records on millions of U.S. persons. In light of the in camera, ex parte proceedings, these numbers raise further questions about FISC's role.

VI. BULK COLLECTION VIOLATES FISA'S STATUTORY PROVISIONS

The telephony metadata program violates the express statutory language in three primary areas: first, with regard to the language "relevant to an authorized investigation"; second, in relation to the requirement that the information sought can be obtained under subpoena duces tecum; and third, in its violation of the restrictions specifically placed on pen registers and trap and trace equipment.

A. "Relevant to an Authorized Investigation"

The government argues that the NSA's telephony metadata program is consistent with the language of 50 U.S.C. § 1861 in that *all* telephone calls in the United States, including those of a wholly local nature, are "relevant" to foreign intelligence investigations.

The word itself, the administration states, "is a broad term that connotes anything '[b]earing upon, connected with, [or] pertinent to' a specified subject matter. 13 Oxford English Dictionary 561 (2d ed. 1989)."[366] Turning to its "particularized legal meaning,"

> It is well-settled in the context of other forms of legal process for the production of documents that a documents is "relevant" to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter.[367]

The fact that massive amounts of data may be involved is of little import:

> Courts have held in the analogous contexts of civil discovery and criminal and administrative investigations that "relevance" is a broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated.[368]

Applied to the telephony metadata program, whilst recognizing that the telephony metadata program is "broad in scope", the government argues that there are nevertheless "reasonable grounds to believe" that the category of data (i.e., all telephone call data), when queried and analyzed, "will produce information pertinent to FBI investigations of international terrorism." [369] For communications data, the government argues, connections between individual data points can only be reliably identified through large-scale data mining.[370]

There are two sets of responses to the government's arguments. The first centers on the government's claim that all telephony metadata is relevant to authorized investigations; the center revolves around the connection in the statutory language between the relevance of the information to be obtained and "an authorized investigation."

---

[366] Section 215 White Paper, *supra* note 223, at 8.
[367] *Id.* at 9.
[368] *Id.* at 2–3.
[369] *Id.* at 3.
[370] *Id.*

1. Relevance Standard

The first problem with the government's argument is that it stretches credulity to state that there are "reasonable grounds" to believe that millions of daily telephone records are "relevant" to an authorized investigation.

The records sought by the government under the telephony metadata program detail the interactions, personal and business relationships, religious and political connections, and other intimate details – on a daily basis – of millions of Americans, not themselves connected in any way to foreign powers or agents thereof. They include private and public interactions between Senators, between members of the House of Representatives, and between judges and their chambers, as well as information about state and local officials. They include parents communicating with their children's teachers, and zookeepers arranging for the care of animals. Rape hotlines, abortion clinics, and political party headquarters—all telephony metadata data is being collected by the NSA.

Reading FISA to allow this type of collection would render meaningless the qualifying phrases contained in 50 U.S.C. §1861(b)(2)(A). The statute first requires that there be "reasonable grounds" to believe that the records being sought are relevant. Although FISA does not define "reasonable grounds", it has been treated as the equivalent of "reasonable suspicion".[371] This standard requires a showing of "specific and articulable facts, which, taken together with rational inferences from those facts, reasonably warrant" an intrusion into an individual's right to privacy.[372]

The FISC order requires that Verizon disclose all domestic telephone records—including those of a purely local nature. According to Verizon Communications News Center, as of last year, the company has 107.7 million wireless customers, connecting an average of 1 billion calls per day.[373] There is simply no way that the government provided specific and articulable facts relevant to each one of those customers or calls, sufficient to establish reasonable grounds to establish their relevance. Interpreting relevance as including all records is so broad as to make the "reasonable grounds" requirement obsolete.

Precisely what, in turn, makes a tangible good "relevant" to an authorized investigation is not explained in the statute. Nevertheless, the act suggests that tangible things are "presumptively relevant where they: "pertain to – (i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[374]

This section also appears not to apply to the telephony metadata program. It would be impossible to establish that all customer and subscriber records pertain to a foreign power or an agent thereof, or to a particular, suspected agent of the same, who is the subject of an authorized investigation. Perhaps five or ten customers may fall into this category, but millions simply pushes the bounds of common sense. So the telephony metadata is neither relevant nor presumptively relevant.

The government's interpretation is so broad that it establishes a dangerous precedent. If all telephony metadata is relevant to foreign intelligence investigations, then so is all email metadata, and all GPS metadata, all financial information, all banking records, all

---

[371] *See, e.g.*, United States v. Banks, 540 U.S. 31, 36 (2003); United States v. Henley, 469 U.S. 221, 227 (1985); United States v. Brinoni-Ponce, 422 U.S. 873, 881–82 (1975); Kris & Wilson, *supra* note 127, at §19:3.

[372] Terry v. Ohio, 392 U.S. 1, 21 (1968).

[373] Verizon Communications Company Statistics, reported by Verizon Communications News Center, Aug. 10, 2012, *available at* http://www.statisticbrain.com/verizon-communications-company-statistics/.

[374] 50 U.S.C. §1861(b)(2)(A) (2006).

social network participation, and all Internet use. Indeed, FISC has hinted that there may be other programs at there that operate in a similar fashion, and on September 28, 2013, the *New York Times* reported that the NSA began allowing analysis of phone call and email logs in November 2010 to begin examining American's networks of associations.[375] If all telephony metadata is relevant, then so is all other data—which means that very little would, in fact, be irrelevant to such investigations. If this is the case, then such an interpretation radically undermines not just the limiting language in the statute, but the very purpose for FISA in the first place.

Finally, the government's interpretation directly contradicts Congress' intent in adopting §215. At the introduction of the measure Senator Arlen Specter explained that the purpose of the language was to create an incentive for the government to use the authority only when it could demonstrate a connection to a *particular* suspected terrorist or spy.[376] During a House Judiciary Committee meeting on July 17, 2013, Representative James Sensenbrenner (R-WI), reiterated that the reason Congress inserted "relevant" into the statute was to ensure that only information *directly related* to national security probes would be included—not to authorize the ongoing collection of all phone calls placed and received by millions of Americans not suspected of any wrongdoing.[377] Members of the Committee made similar claims.[378]

2. Connection to "an Authorized Investigation"

There are three ways, in turn, in which the telephony metadata program violates FISA's requirement in §1861 that the order be sought for use in an "authorized investigation." First, the guidelines establishing when such an investigation exists relate solely to the moment of the collection of the information. The FISC order, in contrast, allows the collection of the data on an ongoing basis, tying instead the *search* of such information to authorized investigations. Second, under the Attorney General guidelines, for each of the levels, there is a predicate specificity required *prior* to the collection of information—namely, that the investigation be premised upon specific individuals, groups, or organizations, or violations of criminal law. The telephony metadata program, in contrast, requires no such specificity *prior* to the collection of the data. Third, the orders issued by FISC empower the NSA to conduct searches of the data in *future* authorized investigations. In other words, the collection of the metadata is relevant to the concept of investigations generally. This means that the orders do not, in fact, relate to (existing) authorized investigations.

a. Collection of the Information

FISA, as aforementioned, requires that the government submit a statement of facts demonstrating reasonable grounds to believe that the records being sought are relevant to an authorized investigation (other than a threat assessment).[379] It ties the definition of what constitutes an authorized investigation to guidelines approved by the Attorney General under Executive Order 12333.[380]

The most recent set of guidelines, the FBI's 2008 *Consolidated Domestic Operations Guidelines*, provides for three or four main categories of investigations: assessments

---

[375] James Risen and Laura Poitras, *NSA Gathers Data on Social Connections of U.S. Citizens*, NEW YORK TIMES, Sept. 28, 2013, at A1.
[376] 151 Cong. Rec. 13,441 (2005).
[377] *Oversight of the Administration's Use of FISA Authorities: Hearing Before H. Comm. on the Judiciary*, 113th Cong. (2013).
[378] *Id.*
[379] 50 U.S.C. §1861(b)(2)(A) (2006).
[380] *Id.*

(i.e., "threat assessments" under the 2003 guidelines and section 215); preliminary investigations; full investigations; and enterprise investigations (a variant of full investigations).[381]

FISA, as aforementioned, makes it clear that the tangible records in question may *not* be sought as part of the first level of national security investigations—i.e., the assessment stage. There is an important reason for this restriction. It is the most general level and, as such, lacks the factual predicate required for the use of more intrusive techniques of information-gathering.

Between 2003 and 2008, for instance, at the threat assessment stage, the FBI could collect information on individuals, groups, and organizations "of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats."[382] But the only types of methods allowed, as noted by the Attorney General, were "relatively non-intrusive investigative techniques." This included:

> [O]btaining publicly available information, accessing information available within the FBI or Department of Justice, requesting information from other government entities, using online informational resources and services, interviewing previously established assets, non-pretextual interviews and requests for information from members of the public and private entities, and accepting information voluntarily provided by governmental or private entities.[383]

Nowhere in the discussion of the threat assessment stage did the 2003 guidelines contemplate the use of court-ordered surveillance.

In 2008, the Attorney General expanded the tools that could be used during the assessment stage to include: publicly available information; all available federal, state, local, tribal, or foreign governmental agencies' records; online services and resources; human source information; interviews or requests for information from members of the public and private entities; information voluntarily provided by governmental or private

---

[381] *See* Michael B. Mukasey, Att'y Gen., The Attorney General's Guidelines for Domestic FBI Operations (Oct. 3, 2008), http://www.justice.gov/ag/readingroom/guidelines.pdf; Department of Justice, Fact Sheet: Attorney General Consolidated guidelines for FBI Domestic Operations (Oct. 3, 2008), http://www.justice.gov/opa/pr/2008/October/08-ag-889.html (noting that the new, consolidated guidelines replace five existing sets of guidelines separately addressing criminal investigations, national security investigations, foreign intelligence collection, and other matters. "In contrast to previous guidelines, the new guidelines are generally unclassified, providing the public with ready access in a single document to the basic body of operating rules for FBI activities within the United States.") For previous guidelines, *see* The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection at 3 (Oct. 31, 2003), http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf [Redacted in part] [hereinafter AG NSI Guidelines]. *See also* David S. Kris, On the Bulk Collection of Tangible Things 17 (Sept. 29, 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf. Also note that on December 16, 2008, the FBI issued a Domestic Investigations and Operations Guide to help to implement the September 2008 Guidelines for Domestic FBI Operations. FBI Records: the Vault, Federal Bureau of Investigation, available at http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)/fbi-domestic-investigations-and-operations-guide-diog-2008-version. A new FBI Domestic Investigations and Operations Guide was released Oct. 15, 2011 and updated June 15, 2012. *See* Domestic Investigations and Operations Guide, Federal Bureau of Investigation, June 15, 2012, available at http://www.aclu.org/files/pdfs/email-content-foia/FBI%20docs/June%202012%20FBI%20DIOG.pdf. In addition to the AG-Dom (Attorney General's Guidelines for Domestic FBI Operations), and the DIOG (Domestic Investigations and Operations Guide), every FBI HQ operational division has a PG (policy implementation guide) that supplements the DIOG. *Id.*, at xxix.

[382] *Id.* at 3.

[383] *Id.* at 3.

entities; observation or surveillance not requiring a court order; and grand jury subpoenas for telephone or electronic mail subscriber information.[384]

The addition of the last two items broadened the type of information that could be obtained. Similarly, whereas previously the guidelines noted that mail covers, mail openings, and nonconsensual electronic surveillance or any other investigative technique covered by Title 18 U.S.C. §§2510-2521 *shall not be used during a preliminary inquiry*,[385] the 2008 guidelines dropped any equivalent language.

Even with the broadening, however, under FISA, tangible goods may not be obtained under Section 215 during the assessment stage. The purpose is to place a higher burden on the government to justify the use of more intrusive surveillance. If such methods are to be used, and the related information collected, *there must be a factual predicate establishing a higher level of suspicion as to the presence of criminal activity or a threat to national security*.[386]

For preliminary investigations, this means that information or an allegation indicating the existence of criminal activity or a threat to U.S. national security exists. For a full investigation, there must be "an articulable factual basis for the investigation that reasonably indicates" criminal activity or a threat to U.S. national security.[387] For an enterprise investigation (a variant of a full investigation), there must be an articulable factual basis for the investigation reasonably indicating "that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for" racketeering, international terrorism or other threats to U.S. national security, domestic terrorism, furthering political or social goals wholly or in pat through activities that involve force or violence and a violation of federal criminal law, or a closed range of other offences.[388]

In short, the guidelines distinguish between the different levels based on a factual predicate of wrongdoing, which then acts as a valve on the level of intrusiveness that the government can adopt in collecting more information.

In contrast, the primary order for the telephony metadata program does not follow this approach. Instead, it authorizes the *collection* of data for 90-day periods without any factual predicate supporting the acquisition or collection of data. It is thus incompatible with the approach adopted in the attorney general guidelines. The order shifts the emphasis to the analysis of such data—which is to be conducted in connection with an authorized investigation. This is not, however, what is required by the FBI's own guidelines. It is the *collection* of such information that is premised upon the existence of an authorized investigation—not the *subsequent analysis* of data in the course of the same.

b. Specificity

According to the Attorney General guidelines, for predicate investigations (for which tangible items orders under section 215 may be sought) there is a *specificity* required prior to the collection of information—namely, that the investigation be premised upon

---

[384] *Id.*, at 20.

[385] Office of the Att'y Gen., Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations II(b)(5)(a)-(c) (1989), http://www.justice.gov/ag/readingroom/generalcrimea.htm#general.

[386] The guidelines explain: "A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based solely on the authority to collect foreign intelligence may be conducted only as a full investigation." Mukasey, The Attorney General's Guidelines for Domestic FBI Operations 21 (2008).

[387] *Id.* at 21-22.

[388] *Id.* at 23.

the past or present wrongdoing or foreign intelligence activities of specific individuals, groups, or organizations. The telephony metadata program, in contrast, collects all call records, without specifying the individuals, groups, or organizations of interest.

For the past decade, specificity has been integral to the guidelines' approach. Under the 2003 Attorney General guidelines, for instance, preliminary investigations were authorized "when there is information or an allegation indicating that a threat to the national security may exist."[389] Such investigations were particular, in that they related to specific individuals, groups, and organizations.[390]

Under the 2008 guidelines, a preliminary investigation must relate to "a" federal crime or threat to national security. For foreign intelligence gathering, the guidelines require that only full investigations may be used. These are defined in singular terms, such as "An activity constituting a federal crime or a threat to national security."[391] Alternatively, the circumstances may indicate that "An individual, group, organization, entity" is or may be a target of an attack, or "victimization, acquisition, infiltration, or recruitment in connection with criminal activity" is underway.[392] For enterprise investigations, the text of the guidelines clearly refers to "the group or organization".[393]

Not only are the investigations specific with regard to the targets, but they are specific with regard to the facts that support the initiation of the predicate investigation. For enterprise investigations, this means that there must be "an articulable factual basis for the investigation that reasonably indicates that the group or organization" was involved in the commission of certain crimes and activities.[394]

Full investigations, in turn, require specific and articulable facts giving reason to believe that a threat to national security may exist.[395] Like preliminary investigations, such inquiries as specific in that they may relate to individuals, groups, and organizations.[396]

In contravention of the Attorney General Guidelines, the telephony metadata program collects data, using precisely those tools that are limited to preliminary and full investigations, absent the specificity otherwise required.

c. Future Authorized Investigations

Third, FISA contemplates the relevance of information to an investigation already in existence at the time the order is granted. The statutory language is very specific. Applications must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[397] The word "are" before "relevant" suggests that at the time the records are being sought, their relevance to an investigation must be established.

The orders issued by FISC, however, depart from the statutory language, empowering the NSA to obtain the data in light of their relevance to "authorized investigations"—and requiring telecommunications companies to indefinitely provide such information in the future.[398] How can the court know that all such telephony data

---

[389] AG NSI Guidelines, *supra* note 328, at 3.
[390] *Id.* at 4.
[391] Michael B. Mukasey, The Attorney General's Guidelines for Domestic FBI Operations 21 (2008), *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf.
[392] *Id.*
[393] *Id.* at 23.
[394] *Id.*
[395] *Id.*
[396] *Id.*
[397] 50 U.S.C. §1861(b)(2)(A) (2006).
[398] Primary Order at 2, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 13-80 (FISA Ct. Apr. 25, 2013), *available at*

will continue to be relevant to investigations that are not yet opened? Indeed, as noted by amici in *In Re Electronic Privacy Information Center*, Congress could have used any number of alternative auxiliary verbs—"such as 'can'; 'could'; 'will' or 'might.' But it chose not to do so. Instead, Congress required relevance to an investigation existing at the time of the application."[399]

In addition, the information sought must be relevant "to an authorized investigation." This is both singular ("an") and past tense, in that is has already been "authorized." The House Report that accompanied the first introduction of the business records provisions explained that the purpose of this language was to provide "for an application to the FISA court for an order directing the production of tangible items such as books, records, papers, documents and other items upon certification to the court that the records sought are *relevant to an ongoing foreign intelligence investigation.*"[400] Yet how can the court with any certainty suggest that all investigations in the future will be authorized?

The government's argument, instead of centering on a particular investigation, appears to create a categorical exception for the collection of records. Namely, it argues that when the government "has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information", "the standard of relevance under Section 215 is satisfied."[401] That is, it is the nature of the information extracted, not the prior existence of a directly related, authorized investigation, that is of moment. "Authorized investigations" thus become merely a category for which the information is useful.[402] Indeed, the language in the FISC order is not "an authorized investigation", but, rather, "authorized investigations."

The fact that the government has one investigation open on al Qaeda—or even "thousands of open full or enterprise investigations on terrorist groups or targets and/or their sponsors, some or all of which could underlie the bulk telephony metadata collection applications and orders"[403] fails to account for the fact that most of the records collected are not in any way directly connected to these authorized investigations.

This interpretation, moreover, contradicts Congressional intent. As Representative F. James Sensenbrenner, one of the principal authors of the USA PATRIOT Act, noted, "Congress intended to allow the intelligence communities to access targeted information for specific investigations. How can every call that every American makes or receives be relevant to a specific investigation? This is well beyond what the Patriot Act allows."[404]

B. Subpoena Duces Tecum

The only express limit on the type of tangible item that can be subject to an order under 50 U.S.C. §1861 is that it "can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."[405] FISC, accordingly, took the position in its order authorizing the telephony

---

http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf ("[T]he court finds as follows: (1) There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI. . .")

[399] Brief for Cato Institute as Amicus Curiae Supporting Petitioner, In Re Electronic Privacy Information Center, No. BR 13-80 (FISA Ct. Apr. 25, 2013) (No. 13-58), at *4.

[400] H.R. REP. NO. 107-236, at 61 (2001) (emphasis in original).

[401] Section 215 White Paper, *supra* note 2, at 8–9.

[402] See *id.* at 6 ("The telephony metadata records are sought for properly predicated FBI investigations into specific international terrorist organizations and suspected terrorists.")

[403] Kris, supra note 328, at 19-20.

[404] Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, GUARDIAN (June 9, 2013 07:00 EDT), http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end.

[405] 50 U.S.C. §1861(c)(2)(D) (2006).

metadata program that "The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."[406] The court later explained, "Call detail records satisfy this requirement, since they may be obtained by (among other means) a 'court order for disclosure' under 18 U.S.C.A. §2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a criminal investigation."[407]

A subpoena duces tecum is a writ or process used to command a witness to bring with him and produce to the court books, papers, &c., over which he has control and which help to elucidate the matter in issue.[408] Unlike warrants, something less than probable cause is required. The rationale behind this is that the purpose of the instrument is not to conduct a search absent a suspect's consent, but, rather, to obtain documents and information that the prosecution has concluded will be material in a case.[409]

The authority to issue a subpoena is not unlimited. Under the Federal Rules of Criminal Procedure, "the court. . . may quash or modify the subpoena if compliance would be unreasonable or oppressive."[410] Precisely what counts as reasonable (or not) is heavily context-dependent.[411] In *United States v. Nixon*, the Court laid out a three-part test, requiring the Government to establish relevancy, admissibility, and specificity, in order to enforce a subpoena in the trial context.[412]

The *Nixon* standard does not apply in the context of grand jury proceedings.[413] In 1991 the Court explained:

> *Nixon's* multi-factor test would invite impermissible procedural delays and detours while courts evaluate the relevance and admissibility of documents sought by a particular subpoena. Additionally, requiring the Government to explain in too much detail the particular reasons underlying a subpoena threatens to compromise the indispensable secrecy of grand jury proceedings. Broad disclosure also affords the targets of investigation far more information about the grand jury's workings than the Rules of Criminal Procedure appear to contemplate.[414]

The Court went on to note that this does not mean that the grand jury's investigatory powers are limitless. To the contrary, it is still subject to Rule 17(c). Nevertheless, grand jury subpoenas are given the benefit of the doubt, with the burden of showing unreasonableness on the recipient seeking to avoid compliance.[415] For claims of irrelevancy, motions to quash "must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[416]

---

[406] *Id.* at 3.
[407] Supp. Op. at note 1, In Re Production of Tangible Things from [REDACTED], No. BR 08-13, (FISA Ct. [date]) (emphasis in original).
[408] 3 WILLIAM BLACKSTONE. COMMENTARIES *382.
[409] Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J. OF L. & TECH. 544 (2011).
[410] Fed. R. Crim. P. 17C.
[411] New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).
[412] United States v. Nixon, 418 U.S. 683, at 699-700 (1974).
[413] United States v. R. Enterprises, Inc., 498 U.S. 292 (1991).
[414] *Id.* at 292-93.
[415] *Id.* at 293.
[416] *Id.*

At the broadest level, then, FISC's assertion, at least with regard to a grand jury subpoena, appears to be valid. But there are three critical flaws in the court's reasoning: first, subpoenas may not be used for fishing expeditions; second, they must be focused on specific individuals or alleged crimes *prior to the collection of information*; and third, the emphasis is on past wrongdoing—not on potential future relationships and actions. In addition, remarkably, FISC has openly admitted that the telephony metadata order it issued violates the statutory language requiring that the information to be obtained comport with the requirements of a subpoena.

1. Not for Fishing Expeditions

Even with such deference granted to subpoenas issued by grand juries, such instruments may *not* be used for fishing expeditions—i.e., enabling individuals to obtain massive amounts of information whence evidence can be derived.[417] That is to say, a grand jury could not convene in Bethesda, Maryland, and simply begin collecting telephony metadata, which it could subsequently mine to find evidence of criminal behavior.

To the contrary, an investigator must have a reasonable suspicion that some document or communication exists, in order for the Court to order its production. A general suspicion that collecting and analyzing all telephone records in the United States might yield some evidence of criminality is many steps removed from the prior suspicion of a particular act of criminality that characterizes grand jury subpoenas.

Almost all of the telephony metadata collected is utterly unrelated to criminal activity. In Judge Reggie Walton's words,

> [N]early all of the call detail records collected pertain to communications of non-U.S. persons who are not the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are not the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities, and are data that otherwise could not be legally captured in bulk by the government. Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.[418]

Precisely because the information is not connected, in any way, to criminal activity, Walton suggests that it could not, in any other way, even be collected.

While new technologies may change what is possible in terms of the amount of records obtained or the level of insight that can be gleaned, they do not invalidate the underlying principle. In a world limited by the physical manifestation of evidence, practicality helped to cabin the scope of subpoenas. Digitization, however, does not alter the importance of tying the compulsion of evidence directly to an underlying crime.

2. Specificity

Grand jury investigations are specific. That is, they represent investigations into particular individuals, or particular entities, in relation to which there is reasonable suspicion that some illegal behavior has occurred. The compelled production of records or items is thus limited by reference to the target of the investigation.

If a grand jury were, for instance, focused on the potentially criminal acts of the head of a crime family in New York, absent reasonable suspicion of some sort of connection to

---

[417] *Id.* at 299 ("Grand juries are not licensed to engage in arbitrary fishing expeditions.").

[418] FISC Order, Mar. 5, 2009, p. 12, *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf. Order at 9, In Re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

the syndicate, it would not issue a subpoena for the telephone records of the Parent-Teacher's Association at Briarwood School in Santa Clara, California.

In contrast, the Section 215 orders are broad and non-specific. That is, on the basis of no particular suspicion, all call records, the "vast majority" of which (according to FISC's own language) are of a purely local nature, are swept up by the NSA.[419]

3. Past Crimes

Grand jury investigations are also retroactive, searching for evidence of a *past* crime. The telephony metadata orders, in contrast, are both past and forward-looking, in that they anticipate the possibility of illegal behavior in the future. Most of the individuals in the database are suspected of no wrongdoing whatsoever. Yet the minimization procedures allow for any information obtained from mining the data to then be used in criminal prosecution. This is an unprecedented use of subpoena information-gathering authority. It amounts to a permanent, ongoing grand jury investigation into all, possible, future criminal acts.

4. March 2009 FISC Opinion

FISC has openly recognized that the information it obtains from the metadata program could not otherwise be collected with any other legal instrument—including a subpoena duces tecum. In a secret opinion in March 2009 Judge Reggie Walton wrote:

> Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (U.S.) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata *could not otherwise be legally captured in bulk*, the government proposed stringent minimization procedures that strictly controlled the acquisition, accessing, dissemination, and retention of these records by the NSA and FBI.[420]

Later in the document, he again noted that the information "otherwise could not be legally captured in bulk by the government".[421]

This assertion directly contradicts the statutory requirement that the information could otherwise be obtained via subpoena duces tecum. It amounts to an admission, by the Court, that the program violated the statute.

What makes the failure of the Court to prevent the illegal program from continuing even more concerning, perhaps, is Judge Walton's explanation of why, even though the information could not legally be obtained in any other way, FISC allowed the government to proceed. He continues,

> Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and includes specific oversight requirements.[422]

---

[419] FISC Order at 2, No. 06-05 (FISA Ct. May 24, 2006), *available at* http://s3.documentcloud.org/documents/785206/pub-may-24-2006-order-from-fisc.pdf.

[420] In re Production of Tangible Things *From* [REDACTED], Order, No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[421] *Id.* at 12.

[422] *Id.*

In other words, FISC allowed an illegal program to operate because the government (1) promised that it was vital to U.S. national security, and (2) was directed by the court to police its own house by following the minimization procedures. The former is a flimsy excuse for allowing the executive branch to break the law. The latter highlights the extent to which the Court, precisely because of the size of the collection program in question, was dependent on the NSA: "in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified. . . and that it is being implemented in a manner that protects the privacy interests of U.S. persons."[423]

Returning to the earlier point, in relation to FISC's abdication of its responsibilities: it was to protect U.S. persons' privacy interests that FISC was created in the first place. Congress did not anticipate that FISC would simply hand over this responsibility to the NSA, once the NSA requested such a sweeping surveillance program that FISC lost the ability to conduct oversight.

C. Evisceration of Pen/Trap Provisions

All of the information obtained through the telephony metadata program is provided for in FISA's pen register and trap and trace provisions. In contrast to the process followed by the government with regard to section 215, however, the pen/trap provisions require prior targeting and limited collection of information. The use of second 215 to obtain seemingly limitless information amounts to an end-run around the pen/trap provisions.

D. Potential Violation of Other Provisions of Criminal Law

There are, in addition, other statutory provisions that raise question about the legality of the current telephony metadata program. Namely, in December 2008 FISC issued a Supplemental Opinion, noting the Court's reasons for concluding that the records to be produced pursuant to the telephony metadata orders were properly subject to production under 50 U.S.C. §1861.[424] The reason behind the document appears to be that although such orders were previously approved, for the first time the government cited 18 U.S.C.A. has identified the provisions of 18 U.S.C.A. §§2702-2703 as relevant to the question.

Under 50 U.S.C. §1861, Congress empowered the government to apply to the FISC "for an order requiring the production of *any* tangible things (including books, records, papers, documents, and other items."[425] The Court placed special emphasis on the use of the word "any", suggesting that it "naturally connotes 'an expansive meaning,' extending to all members of a common set, unless Congress employed 'language limiting [its] breadth.'"[426]

The Court had apparently considered "any" to be without limit, until 18 U.S.C.A. §§2702-2703 was brought to its attention. This statute laid out an apparently exhaustive set of circumstances under which telephone service providers could provide customer or

---

[423] *Id.*

[424] In re Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.

[425] 50 U.S.C.A. §1861(a)(1) (2006)(emphasis added).

[426] In re Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 1 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf (citing United States v. Gonzales, 520 U.S. 1, 5 (1997); *accord* Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)).

subscriber records to the government.[427] An order under 50 U.S.C. §1861 was not included in this list. At the same time that Congress had passed Section 215 of the USA PATRIOT Act, moreover, it had amended sections 2702 and 2703 in ways that appeared to re-affirm that communications service providers could only divulge records to the government in particular circumstances—without specifically noting FISC orders.[428]

Judge Reggie Walton reconciled this tension in a most curious manner. He pointed to National Security Letters—a completely different form of subpoena (i.e., an administrative subpoena), noting that Congress, in the USA PATRIOT Act, empowered the FBI, without prior judicial review, to compel a telephone service provider to produce "subscriber information and toll billing records information", on the basis of FBI certification of relevance to an authorized foreign intelligence investigation.[429] Judge Walton pointed to the heightened requirements of §1861, i.e., that the government provide a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence investigation, and that FISC determine that the application is sufficient. He then noted that §2703(c)(2) expressly permits the government to use administrative subpoenas to obtain certain categories of non-content information from a provider—and concluded that, surely, Congress could not have intended a higher standard for FISC orders.

The problem, of course, with his reasoning is that despite the precision of 18 U.S.C. §§2702-2703, and the concurrent amendment of these sections with the introduction of USA PATRIOT Act §215, Congress nowhere includes in the language of 18 USC §§2703-2703 provision for FISC orders as an exception to the closed set. Instead, it allows the provision of telephony metadata to the government only in two cases: first, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute; or, second, when a Federal or State grand jury or trial subpoena issues.[430] The next paragraph, moreover, ties the provision directly to the actual commission of a crime. A court order for disclosure under §2703(c) may only be issued by a court of competent jurisdiction where the government can provide "specific and articulable facts showing that there are reasonable grounds to believe that. . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[431] The types of records being sought by the FBI from FISC, in contrast, extended well beyond records either relevant or material to an ongoing criminal investigation. Furthermore, under 18 USC §2703(d), the judiciary is empowered to quash or modify such orders where the records being requested "are unusually voluminous in nature."[432] It would be difficult to imagine any telephony metadata database more voluminous than one collecting *all* call data in the United States. As such, the statute contemplates yet further limits on the collection of information.

---

[427] 18 U.S.C.A. § 2702(a)(3) (2013) (except as provided in §2702(c), a provider "shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer. . . to any governmental entity"); 18 U.S.C.A. §2703(c)(1) (2013) ("A governmental entity may require a provider. . . to disclose a record or other [non-content] information pertaining to a subscriber. . . or customer. . . only when the governmental entity" proceeds according to one of the potential routes laid out in §2703(c)(1)(A)-(E) (2013)).

[428] In re Production of Tangible Things From [REDACTED], Supplemental Opinion, No. BR 08-13, at 3 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.

[429] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, 18 U.S.C.A. § 2709(a) (2006).

[430] *Id.* at §2703(c)(2).

[431] *Id.* at §2703(d).

[432] *Id.*

VII. CONSTITUTIONAL CONSIDERATIONS

The government argues that the telephony metadata collection program complies with the Constitution.[433] In doing so, it relies on *Smith v. Maryland*, in which the court held that participants in telephone calls lack a reasonable expectation of privacy (for purposes of the Fourth Amendment) in the telephone numbers dialed and received on one's phone. The government also argues that the national security interests at stake override whatever privacy intrusion arises from the bulk collection of telephony metadata.[434] These arguments are problematic.

The telephony metadata program amounts to a general warrant, the prohibition of which gave rise to the Fourth Amendment. Reliance on *Smith v. Maryland*, moreover is misplaced: the case involved individualized, reasonable cause to believe that the target of the pen register had engaged in criminal behavior and threatening and obscene conduct. The placement of the pen register was obtained via consent. Significant technological and societal changes in the interim further render the third party doctrine a moot point. While lower courts might follow the Third Party Doctrine, the Supreme Court appears poised to recognize exceptions in light of modern interaction.

A. The Fourth Amendment Prohibition on General Warrants

At the time of the founding, English courts rejected general warrants. A different standard, however, marked the crown's treatment of the American colonies. This angered the colonists, who saw themselves, first and foremost, as Englishmen—and therefore deserving of all the rights and privileges accorded to English subjects.

Perhaps the most famous case establishing the right of Englishmen to be free of a general writ dates from November 1762, when King George III's messengers broke into a man's home to execute a warrant issued by the Secretary of State.[435] The warrant empowered the king's men "to make strict and diligent search for . . . the author, or one concerned in the writing of several weekly very seditious papers."[436] The men, who searched John Entick's home for four hours without his consent and against his will "broke open, and read over, pried into and examined all [of his] private papers [and]

---

[433] *See* Section 215 White Paper, *supra* note 223, at 3.

[434] *Id.*

[435] Entick v. Carrington, 19 Howell's State Trials 1029 (1765).

[436] The full warrant read:

> George Montagu Dunk, earl of Halifax, viscount Sunbury, and baron Halifax one of the lords of his majesty's honourable [sic.] privy council, lieutenant general of his majesty's forces, lord lieutenant general and general governor of the kingdom of Ireland, and principal secretary of state, etc. these are in his majesty's name to authorize and require you, taking a constable to your assistance, to make strict and diligent search for John Entick, the author, or one concerned in writing of several weekly very seditious papers, entitled the Monitor, or British Freeholder, No 357, 358, 360, 373, 376, 378, 379, and 380, London, printed for J. Wilson and J. Fell in Pater Noster Row, which contains gross and scandalous reflections and invectives upon his majesty's government, and upon both houses of parliament; and him, having found you are to seize and apprehend, and to bring, together with his books and papers, in safe custody before me to be examined concerning the premisses, and further dealt with according to law; in the due execution whereof all mayors, sheriffs, justices of the peace, constables, and other majesty's officers and military, and all loving subjects whom it may concern, are to be aiding and assisting to you as there shall be occasion; and for so doing this shall be your warrant. Given at St. James's the 6th day of November 1762, in the third year of his majesty's reign, Dunk Halifax. To Nathan Carrington, James Watson, Thomas Ardran, and Robert Blackmore, four of the majesty's 'messengers in ordinary.'

Id.

books."[437] Upon departure, the men seized Entick's documents, charts, pamphlets, and other materials.[438]

Chief Justice of the Common Pleas Charles Pratt, First Earl Camden, ruled that both the search and the seizure was unlawful. He explained:

> Suppose a warrant which is against law be granted, such as no justice of peace, or other magistrate high or low whomsoever, has power to issue, whether that magistrate or justice who grants such warrant, or the officer who executes it, are within the [statute] 24 Geo. 2, c. 44? To put one case. . . suppose a justice of peace issues a warrant to search a house for stolen goods, and directs it to four of his servants, who search and find no stolen goods, but seize all the books and papers of the owners of the house, whether in such a case would the justice of peace, his officers or servants, be within the [statute]?[439]

Two aspects to the case proved particularly troubling: first, the writ had empowered the crown to seize all documents—not just those of a criminal nature; and, second, no demonstration had been made prior to the search and seizure, establishing the probability that Entick was engaged in criminal activity:

> The warrant in our case was an execution. . . without any previous summons, examination, hearing the plaintiff, or proof that he was the author of the supposed libels; a power claimed by no other magistrate whatever. . . it was left to the discretion of these defendants to execute the warrant in the absence or presence of the plaintiff, when he might have no witness present to see what they did; for they were to seize all papers, bank bills, or any other valuable papers they might take away if they were so disposed; there might be nobody to detect them.[440]

The court suggested that since the Glorious Revolution and the restoration of William and Mary to the throne, such powers had been denied to the crown. It was precisely such aggrandizement of power that had led to revolution in the first place. The Chief Justice stated "we can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have."[441] The Court flatly rejected the use of such general warrants.

The use of writs of assistance played a central role in lending speed to the American Revolution. Acting under writs established by Parliamentary statute, officers of the crown had permission to search the homes, papers, and belongings of any person.[442] As early as 1660 legislation to prevent Fraudes and Concealments of His Majestyes Customes and Subsidyes empowered magistrates to:

> [I]ssue out a Warrant to any person or persons thereby enableing him or them with the assistance of a Sheriffe Justice of the Peace or Constable to enter into any House in the day time where such Goods are suspected to be concealed, and in case of resistance to breake open such Houses and to seize and secure the same goods soe concealed, and all Officers and Ministers of Justice are hereby required to be aiding and assisting thereunto.[443]

---

[437] *Id.*
[438] *Id.*
[439] *Id.*
[440] *Id.*
[441] *Id.*
[442] Officials could "enter and go into any House, Warehouse, Shop, Cellar, or other Place" to seize goods. M.H. SMITH, THE WRITS OF ASSISTANCE CASE 1 (1978) (quoting a 1767 measure by Parliament, establishing a new writ of assistance in America).
[443] An Act to Prevent Fraudes and Concealments of His Majestyes Customes and Subsidyes, 12 Car. II, c. 19 (1660). *See also* Act for Preventing Fraudes and Regulating Abuses in his Majesties Customes, 14 Car. II, c. 11 (1662). A good discussion of the early writs of assistance is located in Joseph R. Frese, EARLY

The writs came to be seen as the worst instrument of arbitrary power, turning colonists against the crown.

Their use was part of a general crack-down engineered by British Prime Minister William Pitt, who directed the American colonial governors and royal customs officers to more strictly enforce trade and navigation laws –specifically, to "make the strictedst [sic.] and most diligent [sic.] Enquiry into the State of this dangerous and ignominious Trade." He ordered that every step authorized by law be taken "to bring all such heinous Offenders to the most exemplary and condign [sic.] Punishment."[444]

In response to Pitt's order, the governor of Massachusetts Bay Colony began making use of the writ, prompting Boston merchants to hire James Otis to challenge their constitutionality. In what has become one of the most famous examples of early American legal oration, Otis argued that the writs were contrary to "the fundamental principles of law". Scholars hail Otis' argument in the case as helping "to lay the foundation for the breach between Great Britain and her continental colonies."[445] As A.J. Langguth observed, at the Writs of Assistance trial, "James Otis stood up to speak, and something profound changed in America."[446]

One of our best accounts of Paxton's Case comes from John Adams, who was present at the argument and whose mentor, Jeremiah Grindley, the most distinguished member of the bar in Boston, opened the case for the crown.[447] In replying to Grindley, Otis stated that his efforts were being made "out of regard to the liberties of the subject." The rights of British subjects were under assault, compelling him to oppose "all such instruments of slavery on the one hand and villainy on the other as this Writ of Assistance is."

For Otis, the writ was "the worst instrument of arbitrary power." He ignored the crown's claim of necessity—and current practice—noting that "the writ prayed for in this petition, being general, is illegal." He highlighted four concerns: first, it was universal—i.e., it could be executed by anyone in possession with it; second, it was perpetual in that it indefinitely allowed the holder of the writ to conduct searches; third, no prior evidence of wrongdoing need be involved in its execution; and fourth, there was no requirement to swear to suspicion of wrongdoing or, following execution, to inquire into its exercise. "One of the most essential branches of English liberty is the freedom of one's house," Otis opined. General warrants would annihilate the privilege associated with that right.[448]

Although the court ruled against Otis, John Adams later wrote that his arguments "breathed into this nation the breath of life."[449] Indeed, on June 12, 1776 the Virginia Constitutional Convention adopted the Virginia Declaration of Rights—a document that deeply influenced the Declaration of Independence, as well as other states' constitutions,

---

PARLIAMENTARY LEGISLATION ON WRITS OF ASSISTANCE, PUBLICATIONS OF THE COLONIAL SOCIETY OF MASSACHUSETTS (1959).

[444] Horace Gray, *Writs of Assistance in* JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY BETWEEN 1761 AND 1772 407-08 (Samuel M. Quincy ed. (1865).

[445] LAWRENCE HENRY GIPSON, THE COMING OF THE REVOLUTION, 1763-1777 39 (1954).

[446] A.J. LANGGUTH, PATRIOTS: THE MEN WHO STARTED THE AMERICAN REVOLUTION 22 1998. For excellent studies of the case Otis argued see Gray, supra note 444, at 395-511; M. H. SMITH, THE WRITS OF ASSISTANCE CASE (1978); James M. Farrell, *The Child Independence is Born: James Otis and Writs of Assistance in* RHETORIC, INDEPENDENCE AND NATIONHOOD, Stephen E. Lucas ed., Vol. 2 of A Rhetorical History of the United States: Significant Moments in American Public Discourse (Martin J. Medhurst ed.).

[447] Farrell, *supra* note 446, at 16. *See also Paxton's Case of the Writ of Assistance in* JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY BETWEEN 1761 AND 1772 (Samuel M. Quincy ed. (1865)

[448] Otis' speech is taken from L. KINVIN WROTH & HILLER B. ZOBEL, LEGAL PAPERS OF JOHN ADAMS VOL. 2 139-144 (1965). See also discussion in Farrell, *supra* note 446, at 19-22.

[449] THE WORKS OF JOHN ADAMS VOL. X. 276.

and became the basis for the Bill of Rights—without which, the Constitution would never have been ratified.

The Virginia Declaration of Rights stated, inter alia, "That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted."[450] The Massachusetts Constitution of 1780 similarly objected to the use of general warrants:

> Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws.[451]

The New Hampshire Constitution of 1784 lifted the clause almost verbatim.[452] The Virginia ratifying convention of 1788 made a point to ensure that the subsequent Constitution would incliude a provision affirming that "every freeman has a right to be secure from all unreasonable searches and siezures of his person, his papers and his property."[453] New York, in turn, required nearly identical language, as did North Carolina—even as Virginia, New York and North Carolina all condemned overbroad warrants as "'therefore' unreasonable—'grievous,' 'oppressive, and 'dangerous.'"[454] Consistent with these states' understandings, James Madison's first draft of the Fourth Amendment addressed the right of the people "to be secured in their persons, their houses, *their papers, and their other property*, from all unreasonable searches and seizures."[455] Madison understood the clause as a ban against general warrants.[456]

In 1886 the Supreme Court recognized the importance of the writs and the Founders' rejection of the same as encapsulated in the Fourth Amendment:

> In order to ascertain the nature of the proceedings intended by the Fourth Amendment ot the Constitution under the terms "unreasonable searches and

---

[450] Va. Decl. of Rights § 10.

[451] Mass. Const. of 1780, pt. 1, art. XIV.

[452] New Hampshire Const. 1784, Art. XIX.

> Every subject hath a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath, or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

Id.

[453] EDWARD DUMBAULD, THE BILL OF RIGHTS AND WHAT IT MEANS TODAY 184 (1957), quoted in Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 Suffolk U. L. Rev. 53, 68 (1996).

[454] *Id.*, at 184, 191, 200-01, quoted and cited in Amar, *supra* note 453, at 68.

[455] *Id.*, at 207, quoted in Amar, *supra* note 453, at 68. (emphasis added). Note that the historical antecedent suggests a broad reading of the "persons, houses, papers, and effects" language of the Fourth Amendment.

[456] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV., 547, 555 (1999). *See also* N. Lasson, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 103 (1937); Robert M. Bloom, *Warrant Requirement – The Burger Court Approach*, 53 UNIV. OF COLORADO L. REV. 691, 692 (1982).

> seizures," it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England. The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundmental principles of law, that ever was found in an English law book;" since they placed "the liberty of every man in the hands of every petty officer." This was in February, 1761, in Boston, and the famous debate in which it occurred was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Idependence was born.[457]

The Court acknowledged the importance of Lord Camden's decision in *Entick v. Carrington*, saying,

> [Camden's] great judgment on that occasion is considered as one of the landmarks of English liberty. It was welcomed and applauded by the lovers of liberty in the colonies, as well as in the mother country. It is regarded as one of the permanent monuments of th eBritish Constitution, and is quoted as such by the English authorities on that subject down to the present time.[458]

It was precisely general warrants that the Framers meant when referring to unreasonable searches and seizures.[459]

The Supreme Court has continued, throughout U.S. history, to recognize the special role played by general warrants and writs of assistance in shaping the contours of the Fourth Amendment. In 1980 the Court recognized that it is "familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."[460] General warrants were presumptively unreasonable. To drive the point home, the first Congress, which started out with just one sentence outlawing unreasonable search and seizure, went on to add a second clause to the Fourth Amendment, requiring that no warrant shall issue but upon probable cause—ensuring in the process that government officials could not issue general warrants and still comport with the Fourth Amendment.

Consistent with this reading, Professor Akhil Amar, inquiring as to what the warrant clause means—and what the relationship is between it and the earlier reasonableness clause—suggests that "broad warrants—warrants that fail to meet the various specifications of clause two—are inherently unreasonable under clause one."[461] Such a general warrant would immunize the officer who carried it out from a subsequent trespass suit.[462] In the case of *Entick v. Carrington*, "Armed with sweeping warrants issued by executive officials, various govenrment henchmen broke into Englishmen's houses, searched their papers, arrested their persons, and rummaged through their effects, in hopes of finding" wrongdoing.[463]

---

[457] Boyd v. United States, 116 U.S. 616, 624-25 (1886).
[458] *Id.* at 626.
[459] *Id.* at 627.
[460] Payton v. New York, 445 U.S. 573, 583 (1980).
[461] *See* Amar, *supra* note 453, at 60.
[462] *Id.*
[463] *Id.*, at 65.

Professor Thomas Davies similarly recognizes that "[t]he historical statements about search and seizure" in the fourth Amendment "focused on condemning general warrants. In fact, the historical concerns were almost exclusively about the need to ban house searches under general warrants."[464] Evidence suggests that "unreasonable searches and seizures" was a proxy for "the inherent illegality of any searches or seizures that might be made under general warrants."[465] Davies posits that the reason the Framers even bothered "to adopt constitutional bans against general warrants in light of the apparent consensus that the general warrant was illegal at common law" was because of genuine concern that Congress might edanger the right in the future.[466]

The FISC Order authorizing the telephony metadata program is, precisely, a general warrant. It authorizes the government to rummage through our papers and effects in the hope of finding wrongdoing. There is no previous suspicion of criminal activitiy. FISC admits that almost none of the information obtained relates to illegal behavior.

It matters little whether one stores ones papers in a filing cabinet in one's den, or places all financial documents on the iCloud—the digital equivalent, in modern times, of a filing cabinet. Sheer volume of information requires individuals to arrange for storage of everything from medical records to family photos. Email, in turn, holds our correspondence—papers that we place on a server with a company with whom we have a contractual relationship. Banking records may be accessible over the Internet.

This is our modern day equivalent of the papers and effects held by Entick in his home, and allowing the govenrment to obtain records of all of this information is the equivalent of a digital trespass on our private lives.[467] The trespass in which the NSA is engaging is not supported by probable cause, it is not even supported by reasonable suspicion—indeed, no suspicion of any wrongdoing whatsoever is contemplated by the collection of myriad records of all U.S. persons. It is the equivalent of a general warrant and, as such, is odius to the Fourth Amendment.

B. Third Party Data

In defending the telephony metadata program, the government relies on the Court's construction of a reasonable expectation of privacy in *Katz v. United States* (1967) and argues that, consistent with *Smith v. Maryland* (1979) third party information is not constitutionally-protected. This argument fails to appreciate the fact pattern in *Smith v. Maryland*, the evolution of technology, and the manner in which society now operates. It also ignores that the shadow majority in *U.S. v. Jones* (2012), that suggests that the Supreme Court is moving to recognize the world in which we now live and to re-evaluate the level of protection afforded, consistent with the Fourth Amendment.

---

[464] Davies, *supra* note 456, at, 551.

[465] *Id.*

[466] *Id.*, at 657.

467 Lord Camden explained in *Entick v. Carrington*:

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing, which is proved by every declaration in trespass where the defendant is called upon to answer for bruising the grass and even treading upon the soil. If he admits the fact, he is bound to show, by way of justification, that some positive law has justified or excused him. The justification is submitted to the judges, who are to look into the books, and see if such a justification can be maintained by the text of the statute law, or by the principles of the common law. If no such excuse can be found or produced, the silence of the books is an authority, against the defendant, and the plaintiff must have judgment. According to this reasoning, it is now incumbent upon the defendants to show the law by which this seizure is warranted. If that cannot be done, it is a trespass.

See Entick v. Carrington, 19 Howell's State Trials 1029 (1765).

In 1967 the Supreme Court held that the Fourth Amendment protects people, not places.[468] Justice Potter Stewart, writing for Court, explained, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[469]

The government suggests that a Section 215 order is not a "search" as to any person because the Supreme Court "has expressly held, participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed."[470] In the case in question, *Smith v. Maryland*, the Court held that a pen register placed on a telephone line did not constitute a search within the meaning of the Fourth Amendment, because persons making phone calls do not have a reasonable expectation that the numbers they dial will remain private.[471] The key sentence from the decision centered on the customer's relationship with the telephone company: namely "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[472] The government argues:

> Although the telephony metadata obtained through Section 215 includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information, under the reasoning adopted by the Supreme Court in Smith, there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes.[473]

For the government, the breadth of the program does not convert the collection of bulk data into a search.[474] Further, the government argues that even if it were a search, it would still satisfy the reasonableness standard established by the Supreme Court to govern large-scale, but minimally intrusive suspicionless searches. Of particular importance here is the overriding government interest in protecting national security.[475]

The problem with the government's argument is that it glosses over some glaring differences between the bulk collection program and the facts of *Smith v. Maryland.* On March 5, 1976, Ms. Patricia McDonough was robbed in Baltimore, Maryland. After giving the police a description of the robber and a 1975 Monte Carlo she had seen near the scene of the crime, she started receiving threatening and obscene phone calls from a man who identified himself as the robber. At one point, the caller asked her to go out in front of her house. When she did so, she saw the 1975 Monte Carlo moving slowly past her home. On March 16, the police observed a car of the same description in her neighborhood. Tracing the license plate, police discovered that the car was registered to Michael Lee Smith.[476]

The following day, the police asked the telephone company to install a pen register to trace the numbers called from Smith's home telephone. The company agreed, and that

---

[468] Katz v. United States, 389 U.S. 347, 351 (1967) (citation omitted).
[469] *Id.*
[470] Section 215 White Paper, *supra* note 223, at 19.
[471] *Id.*, citing Smith v. Maryland, 442 U.S. 735, 743-46 (1979).
[472] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[473] Section 215 White paper, *supra* note 223, at 20, citing in support SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); United States v. Miller, 425 U.S. 435, 443 (1976).
[474] Section 215 White Paper, *supra* note 223, at 20 ("The scope of the program does not alter the conclusion that the collection of telephony metadata under a Section 215 court order is consistent with the Fourth Amendment. Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search.")
[475] *Id.*, at 21.
[476] Smith v. Maryland, 442 U.S. 735 (1979).

day Smith called Patricia McDonough's home. On the basis of this and other information, the police applied for and obtained a search warrant. Upon executing the warrant, police found a telephone book in Smith's home, with the corner turned down to Patricia McDonough's name and number. In a subsequent six-man lineup, McDonough identified Smith as the person who robbed her.[477]

Although the police did not obtain a warrant prior to placing the pen register, at a minimum, reasonable suspicion had been established that the target of the surveillance, Michael Lee Smith, had robbed, threatened, intimidated, and harassed Patricia McDonough. The police, accordingly, placed the pen register consistent with their reasonable suspicion that Michael Lee Smith was engaged in criminal wrongdoing.

The telephony metadata program is an entirely different situation. The NSA is engaging in bulk collection absent any reasonable suspicion that the individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, the Foreign Intelligence Surveillance Court acknowledges that almost all of the information thus obtained will bear no relationship whatsoever to criminal activity. The government, however, wants to place a pen register and trap and trace on all U.S. persons—essentially treating everyone in the United States as though they are Michael Lee Smith.

In *Smith v. Maryland*, moreover, the police wanted only to record the numbers dialed from the suspect's telephone. Although it is now often forgotten, at the time the case was decided, telephone companies were treated as utilities, with local telephone calls billed by the minute. What was unique about the technology involved in the pen register was that it could both identify and record the numbers dialed from a telephone—a function that the phone company itself did not have.

In contrast, the bulk collection program now collects the numbers dialed, the numbers who call a particular number, trunk information, session times, and the like. And it has the ability to do that for not just one person, but for the entire country. Whereas the police in 1979 were concerned with whether Michael Lee Smith was calling a particular number, the NSA metadata program now collects all numbers called—in the process obtaining significant amounts of information about individuals. Calls to a rape crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in *Smith*. The sheer amount of information available is thus significantly different from what was at stake in the pen register placed on Michael Lee Smith's line.

Further characteristics distinguish the case. In 1979, the telephone company consented to placing the pen register on the line. Today, however, under the FISC order, telephone service providers are forced to comply with the government's request. Unlike the voluntary behavior that marked the case, the bulk collection program relies on coercive government power to obtain records on all telephone subscribers. And it is not for a limited time. In *Smith v. Maryland*, the police sought the information for an extremely limited period. The bulk metadata collection program has been operating for seven years now—and, the NSA argues—should be a permanent part of the government surveillance program.

Perhaps the most important difference between the two situations lies in the realms of technology and social construction. The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed at the time the Court heard arguments in *Smith*. Resultantly, the extent of information that can be learned about not just individuals, but neighborhoods, school boards, political parties, girl scout troops—indeed, any social,

[477] *Id.*

political, or economic network, is light years ahead of what the Court contemplated in 1979. The logic of the government's position has virtually no limit. Not only is telephony metadata more revealing than previously, but all forms of metadata are at stake.

Americans have a contractual relationship with myriad corporate entities now, to whom they have entrusted parts of their lives, such as friendships, correspondence, buying patterns, and financial records. Creating a contractual relationship with Safeway, however, to gain access to reduced prices for food, is something different in kind than giving all information to the federal government. Americans reasonably expect that their movements, communications, and decisions will not be recorded and analyzed by the intelligence agencies. And a majority of the Supreme Court seems to agree.

In 2012 the Court considered a case involving 28-day surveillance. The government had obtained a search warrant permitting it to place a Global-Positioning System (GPS) tracking device on a car registered to the wife of a suspected drug dealer. The day after the warrant expired, agents installed the device and followed the car's movements for nearly a month. Information thus obtained allowed the government to indict Antoine Jones and others on drug trafficking conspiracy charges.[478] The Supreme Court held that attaching the GPS device to the car and tracing its movements amounted to a search within the meaning of the Fourth Amendment.[479]

This case is important for determining the constitutionality of the telephony metadata program in two important ways. First, it recognized that Katz's reasonable expectation of privacy test did not supplant the rights in existence at the time the Fourth Amendment was forged. Justice Scalia, writing for the Court, explained:

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.[480]

Justice Scalia cited *Entick v. Carrington*, noting that the Court had previously described it as a "'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law' with regard to search and seizure."[481] For Justice Scalia, and for the Court, the reasonable expectation of privacy test was of no consequence: "At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[482]

Just as the Court eschewed the test in *Katz v. United States* as being inapposite for consideration of the rights that existed when the Fourth Amendment was adopted, it would be equally inapposite to dismiss the Fourth Amendment's rejection of general warrants. "[A]t a minimum," Justice Scalia wrote, the "18th century guarantee against unreasonable searches. . . . must provide. . . the degree of protection it afforded when it was adopted."[483]

The concept of a general warrant and the Court's conception of the tort of trespass are historically connected. The reason that general warrants were rejected at the time of the Founding was because they provided a carte blanche to the government to trespass at will upon one's property and to search through ones papers and effects without any reasonable suspicion.

---

[478] United States v. Jones, 132 S. Ct. 945 (2012).
[479] *Id.* at 949.
[480] *Id.*
[481] *Id.*
[482] *Id.*, at 947.
[483] *Id.* at 953.

The second point to draw out of *Jones* is that what can be considered a shadow majority appears to recognize that changed circumstances exist, so as to augment the need for new protections for privacy. At least five justices indicated unease with the intrusiveness of modern technology in light of changed times, offering in the process different aspects of a mosaic theory of privacy.

Even though he adopted *Katz* as the relevant standard, Justice Samuel Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investigations, long-term monitoring "impinges on expectations of privacy." New technologies mattered:

> Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of their convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.[484]

Unlike in the past, the daily business of living one's life creates a digital record with privacy implications. "Perhaps most significant," Justice Alito added, "cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States."[485] Before computers, practicality proved one of the greatest protectors of individual privacy. It was difficult and expensive to conduct long-term surveillance. But technology has changed the equation. The government now is more able to engage in long-term surveillance; but while relatively short-term monitoring of individuals' movements in public space might be consistent with the Fourth Amendment, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[486]

Justice Sotomayor went one step further. She suggested that, in light of the level of intrusiveness represented by modern technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[487] She pointed out:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to the cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[488]

Justice Sotomayor added, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[489]

VIII. CONCLUDING REMARKS

---

[484] *Id.* at 963 (Alito, J., concurring).
[485] *Id.*
[486] *Id.* at 964.
[487] *Id.* at 957 (Sotomayor, J., concurring).
[488] *Id.*
[489] *Id.*

The 1978 Foreign Intelligence Act sought to empower the NSA and others to take advantage of new technologies and to engage in necessary foreign intelligence gathering, while preventing the intelligence community from engaging in sweeping surveillance of U.S. citizens. Congress enacted a series of restrictions, requiring that the target of such surveillance be a foreign power, or an agent thereof, insisting that probable cause support such claims, and heightening the protections afforded to the domestic collection of U.S. citizens' information. FISA's expansion gradually brought physical searches, pen registers and trap and trace devices, as well as business records and tangible goods, within its remit. These new authorities retained much of the structure that defined the statute.

The NSA's bulk collection of metadata contradicts the general approach adopted by Congress in enacting FISA. The FISC orders lack the particularization required prior to the acquisition of information and the role FISC now plays departs from that envisioned by Congress. The bulk collection program, moreover, violates the statutory language in at least three ways: it does not comport with the requirement that the tangible goods sought "are relevant to an authorized investigation"; it violates the requirement that the information be otherwise obtainable via subpoena duces tecum; and it bypasses the statutory provisions governing pen registers and trap and trace devices. Compounding the illegality of the program are serious constitutional concerns. The FISC order governing the telephony metadata program amounts to a general warrant, which the Fourth Amendment precludes. Efforts by the government to save the program on grounds of third party doctrine are unpersuasive in light of the unique circumstances of Smith v. Maryland, new technologies, and changed circumstances. An end to the telephony metadata program and FISA reform are necessary to bring surveillance operations and emerging technologies within the bounds of the Constitution.

Written Testimony of Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States Senate, Committee on the Judiciary
Hearing on
Continued Oversight of the Foreign Intelligence Surveillance Act
October 2, 2013

Chairman Leahy, Ranking Member Grassley, and members of the Committee, I thank you for the opportunity to testify about technical issues related to surveillance.

My name is Edward W. Felten. I am a Professor of Computer Science and Public Affairs at Princeton University. I also serve as the founding Director of the Center for Information Technology Policy, an interdisciplinary research and teaching center at Princeton that focuses on public policy issues relating to computers and the Internet. My primary field is computer science, and my main research areas are computer security and privacy, and Internet technologies.

Throughout my career, I have worked to help policymakers respond effectively to technological change. In 2011-12 I served as the first Chief Technologist at the Federal Trade Commission. I have testified several times at Senate and House hearings. I am a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

Today, I will provide an overview of the tools and methods that computing technology can bring to the broad collection and analysis of metadata. I am not an expert on the law and I offer no opinion on the legal status of any program. Nor do I presume to say how best to balance the legitimate goals of conducting foreign intelligence surveillance against the legitimate goals of protecting privacy and promoting civil liberties. I hope that my testimony will help you appreciate the power of metadata and control its use appropriately, consistent with the need for effective foreign intelligence.

Metadata can now yield startling insights about individuals and groups, particularly when collected in large quantities across the population. It is no longer safe to assume that this "summary" or "non-content" information is less revealing or less sensitive than the content it describes. Just by using new technologies such as smart phones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many details of our lives can be gleaned by examining those trails. Taken together, a group's metadata can reveal intricacies of social, political, and religious associations. Metadata is naturally organized in a way that lends itself to analysis, and a growing set of computing tools can turn these trails into penetrating insights. Given limited analytical resources, analyzing metadata is often a far more powerful analytical strategy than investigating content: It can yield far more insight with the same amount of effort.

Advances in technology have transformed the role and importance of metadata. When focused on intelligence targets, metadata collection can be a valuable tool. At the same time, unfocused collection of metadata on the American population gives government access to many of the same sensitive facts about the lives of ordinary Americans that have traditionally been protected by limits on content collection. Metadata might once have seemed much less informative than content, but this gap has narrowed dramatically and will continue to close.

Today's hearing is a vital step in a process that must continue. Technical expertise is essential for effective oversight of these technologically complex programs, and I would respectfully urge you to consider how best to integrate technical expertise into the oversight system. The United States has the world's strongest and deepest community of technical experts. This community is eager to contribute constructively to the national discussion.

The NSA Is Collecting Massive Amounts of Telephony Metadata

On June 5, 2013, *The Guardian* disclosed an order issued by the Foreign Intelligence Surveillance Court ("FISC") pursuant to Section 215 of the Patriot Act (the "Verizon Order").[1] This order compelled Verizon to produce to the NSA on "an ongoing daily basis . . . all *call detail records* or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Director of National Intelligence (DNI) James R. Clapper subsequently acknowledged the authenticity of the Verizon Order.[2] Officials also acknowledged that the NSA's acquisition of call detail records extends to the country's three largest phone companies: Verizon, AT&T, and Sprint[3]. Because these companies provide at least one end of the vast majority of calls in this country, these statements suggest that the NSA is maintaining a record of the metadata associated with nearly every telephone call originating or terminating in the United States.

This is a large volume of data. Assuming that there are approximately 3 billion calls made every day in the United States, and that each call record takes approximately 50

---

[1] 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 Commc'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.

[2] James R. Clapper, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13jwuFc.

[3] *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, WALL ST. J., June 7, 2013, http://on.wsj.com/11uDoue ("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.").

bytes to store, the mass call tracking program collects about 140 gigabytes of data every day, or about 50 terabytes of data each year. Assuming that a page of text takes two kilobytes of storage, the program collects the equivalent of about 70 million pages of information every day, or about 25 billion pages every year.

The Verizon Order requires the production of "call detail records" or "telephony metadata." According to the order itself, that term encompasses, among other things, the originating and terminating telephone number and the time and duration of any call. Call detail records also typically include information about the location of the parties to the call.[4]

Although this latter definition of "call detail information" includes data identifying the location where calls are made or received, I will not address mobile phone location information in this testimony. While I understand that senior intelligence officials have asserted that they have the legal authority under Section 215 to collect mobile phone location information, they have stated that the NSA is not collecting phone location information "under this program."[5]

The information acquired from Verizon also includes "session identifying information"—*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, and International Mobile station Equipment Identity (IMEI) number. These are unique numbers that identify the user or device that is making or receiving a call. Although people who want to evade surveillance can make it difficult to connect these numbers to their individual identities, for the vast majority of ordinary Americans these numbers can be connected to the specific identity of a person.

The information acquired from Verizon also includes the "trunk identifier" of telephone calls. This provides information about how a call was routed through the phone network, which naturally reveals information about the location of the parties. For example, even if the NSA never obtains cell site location information about a call,[6], trunk identifier

---

[4] *See* 47 C.F.R. § 64.2003 (2012) (defining "call detail information" as "[a]ny information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call").

[5] *See* Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, WALL ST. J., June 16, 2013, http://on.wsj.com/13MnSsp; Pema Levy, *NSA FISA Metadata Surveillance: Is The Government Using Cell Phones To Gather Location Data?*, INT'L BUS. TIMES, Aug. 2, 2013, http://bit.ly/18WKXOV.

[6] Cell site location information ("CSLI") reflects the cell tower and antenna sector a phone is connected to when communicating with a wireless carrier's network. Most carriers log and retain CSLI for the start and end of each call made or received by a phone, and some carriers log CSLI for text messages and data connections as well. Wireless carriers can also obtain CSLI by "pinging" a phone whenever it is turned on, even if it is not engaged in an active call. The precision of CSLI varies according to several factors, and "[f]or a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS." *The Electronic*

information revealing that a domestic call was carried by a cable from Hawaii to the mainland United States will reveal that the caller was in the state of Hawaii at the time the call was placed.

Although officials have stated that the orders issued under the telephony metadata program do not compel the production of customers' names, it would be easy for the NSA to correlate many telephone numbers with subscriber names using publicly available sources. I understand that federal agencies also have available a number of legal tools to compel service providers to produce their customer's information, including their names, without probably cause or judicial preclearance.[7]

Metadata Is Easy to Analyze

Telephony metadata is easy to aggregate and analyze because it is, by its nature, *structured data*. Telephone numbers are standardized, and are expressed in a predictable format: in the United States, a three digit area code, followed by a three digit central office exchange code, and then a four digit subscriber number. Likewise, the time and date information associated with the beginning and end of each call will be stored in a predictable, standardized format.

By contrast, the contents of calls are unstructured. Some people speak English, others Spanish, French, Mandarin, or Arabic. Some speak using street slang or a pidgin dialect, which can be difficult for others to understand. Conversations lack a common structure: Some people get straight to the point, others engage in lengthy small talk. Speakers have different accents, and exhibit verbal stutters and disfluencies. Although automated transcription of speech has advanced, it is still a difficult and error-prone process.

The structured nature of metadata makes it easy to analyze massive datasets using sophisticated data-mining and link-analysis programs. That analysis is greatly facilitated by technological advances over the past decades in computing, electronic data storage, and digital data mining. Those advances have radically increased our ability to collect, store, and analyze personal communications, including metadata.

Further, the massive increases in electronic storage permit us to maintain, cheaply and efficiently, vast amounts of data. The ability to preserve data on this scale is, by itself, an unprecedented development—making possible the maintenance of a digital history that was not previously within the easy reach of any individual, corporation, or government.

Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. On the Judiciary, 113th Cong. (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), http://1.usa.gov/1awvgOa.

[7] *See* 18 U.S.C. § 2709 (national security letter); 18 U.S.C. § 2703(c), (d) (court order for records concerning electronic communication service).

This newfound data storage capacity has led to new ways of exploiting the digital record. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits, and behaviors. As a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives—details that we had no intent or expectation of sharing.

IBM's Analyst's Notebook and Pen-Link are two such computing tools. Both are widely used by law enforcement and intelligence agencies for this purpose.[8]

IBM's Analyst's Notebook product is a multi-purpose intelligence analysis tool that includes specific telephony metadata analysis features, which are "routinely" used to analyze large amounts of telephony metadata.[9] IBM even offers training courses entirely focused on using Analyst's Notebook to analyze telephone call records.[10]

Pen-Link is a tool that is purpose-built for processing and analyzing surveillance data. It is capable of importing subscriber Call Detail Record ("CDR") data from the proprietary formats used by the major telephone companies,[11] it can import and export call data to several federal surveillance databases,[12] as well as interact with commercial providers of public records databases such as LexisNexis. Pen-Link can perform automated "call

---

[8] *Public Safety & Law Enforcement Operations*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/1avGItq ("IBM® i2® solutions help law enforcers to turn huge volumes of crime data into actionable insights by delivering tools for tactical lead generation, intelligence analysis, crime analysis and predictive analysis."); *see also Defense and National Security Operations*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/18nateN ("IBM i2 solutions for military and national security organizations have been used across the world to process and analyze the vast quantities of information that they collect, to generate actionable intelligence and to share insights that help identify, predict and prevent hostile threats."); *see also* Pen-Link, *Unique Features of Pen-Link v8* at 16 (April 17, 2008), http://bit.ly/153ee9g ("Many U.S. Federal Law Enforcement and Intelligence agencies have acquired agency-wide site license contracts for the use of Pen-Link in their operations throughout the United States...Pen-Link systems are also becoming more frequently used by U.S. intelligence efforts operating in several other countries.").

[9] *Case Studies: Edith Cowan University, IBM i2 Solutions Help University Researchers Catch a Group of Would-Be Hackers*, International Business Machines (Mar. 27, 2013), http://ibm.co/13J2036 ("Analyzing this volume of data is nothing new to many law enforcement users who routinely analyze tens of thousands of telephone records using IBM® i2® Analyst's Notebook®.").

[10] *Course Description: Telephone Analysis Using i2 Analyst's Notebook*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/1d5QlB8 ("This intermediate hands-on 3-day workshop focuses on the techniques of utilizing i2 Analyst's Notebook to conduct telephone toll analysis...Learn to import volumes of call detail records from various phone carriers, analyze those records and identify clusters and patterns in the data. Using both association and temporal charts, discover how to use different layouts and more advanced tools to analyze telephonic data quickly and effectively.").

[11] *See* Pen-Link, *Unique Features of Pen-Link v8* at 4 (Apr. 17, 2008), http://bit.ly/153ee9g (describing the capability to import 170 different data formats, used by phone companies to provide call detail records).

[12] *Id.* at 4.

pattern analysis," which "automatically identifies instances where particular sequences of calls occur, when they occur, how often they occur, and between which numbers and names."[13] As the company notes in its own marketing materials, this feature "would help the analyst determine how many times Joe paged Steve, then Steve called Barbara, then Steve called Joe back."[14]

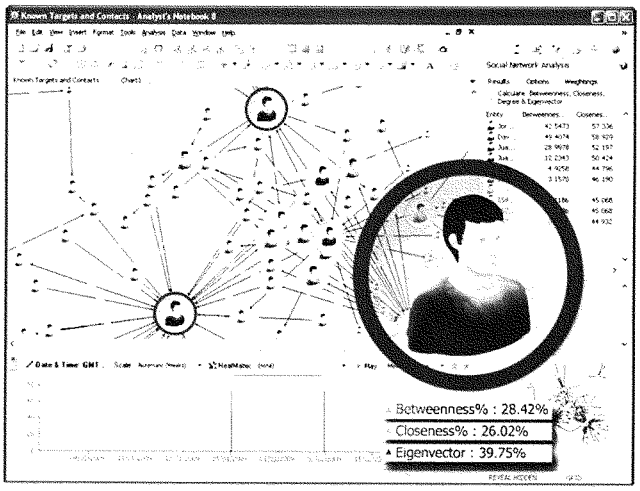

Figure 1: Screenshot of IBM's Analyst's Notebook.[15]

The contents of calls are far more difficult to analyze in an automated fashion due to their unstructured nature. The NSA would first have to transcribe the calls and then determine which parts of the conversation are interesting and relevant. Assuming that a call is transcribed correctly, the NSA must still try to determine the meaning of the conversation: When a surveillance target is recorded saying "the package will be delivered next week," are they talking about an order they placed from an online retailer, a shipment of drugs being sent through the mail, or a terrorist attack? Automatically parsing and interpreting such information, even with today's most sophisticated computing tools, is exceptionally difficult. To do so in an automated way, transcribing and data-mining the contents of hundreds of millions of telephone calls per day is an even more difficult task.

It is not surprising, then, that intelligence and law enforcement agencies often turn first to metadata. Examining metadata is generally more cost-effective than analyzing content. Of course, the NSA will likely still have analysts listen to every call made by the

[13] *Id.* at 7.
[14] *Id.*
[15] Image taken from *Data Analysis and Visualization for Effective Intelligence Analysis*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/16qT3hw.

highest-value surveillance targets, but the resources available to the NSA do not permit it to do this for all of the calls of 300 million Americans.

Americans Inevitably Create Metadata That Can Reveal Sensitive Details of Their Lives

Over the last three decades, and especially with the widespread adoption of mobile phones in the past decade, our reliance on telecommunications has significantly increased. Mobile phones are today ubiquitous, and their use necessarily requires reliance on a service provider to transmit telephone calls, text messages, and other data. These communications inevitably produce telephony metadata, which is created whenever a person places a call. There is no practical way to prevent the creation of telephony metadata, or to erase it after the fact. The only reliable way to avoid creating such metadata is to avoid telephonic communication altogether.

As a general matter, it is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or Internet voice chats.

After decades of research (much of it supported by the U.S. government), there now exist many tools that individuals and organizations can use to protect the confidentiality of their communications content. Smartphone applications are available that let individuals make encrypted telephone calls and send secure text messages.[16] Freely available software can be used to encrypt email messages and instant messages sent between computers, which can frustrate surveillance efforts traditionally performed by intercepting communications as they are transmitted over the Internet.

However, most of these secure communication technologies protect only the content of the conversation and do not protect the metadata. Government agents that intercept an encrypted email may not know what was said, but they will be able to learn the email address that sent the message and the address that received it as well as the size of the message and when it was sent. Likewise, Internet metadata can reveal the parties making an encrypted audio call and the time and duration of the call, even if the voice contents of the call are beyond the reach of a wiretap.

Some security technologies are specifically designed to hide metadata trails, but those technologies do not work quickly enough to allow real-time communication. The general technique for hiding the origin and destination information for an Internet communication involves sending data through a series of intermediaries before it reaches the destination, thus making it more difficult for an entity such as a government agency to learn both the source and destination of the communication. (Such

[16] Somini Sengupta, *Digital Tools to Curb Snooping*, N.Y. TIMES, July 17, 2013, http://nyti.ms/12JKz1s (describing RedPhone and Silent Circle).

information is conventionally encrypted so that the intermediaries cannot capture it; and a series of intermediaries is used so that no one intermediary knows the identities of both endpoints.)

The most popular and well-studied of these metadata hiding systems is The Tor Project, which was originally created by the U.S. Naval Research Lab, and has since received significant funding from the State Department. One important and widely acknowledged limitation of Tor is the noticeable delay introduced by using the tool. Web browsing conducted through Tor is much slower than through a direct connection to the site, as all data must be sent through a series of Tor relays, located in different parts of the world. These volunteer-run relays are oversubscribed—that is, the demands on the few relays from hundreds of thousands of Tor users are greater than the relays can supply, leading to slowdowns due to "traffic jams" at the relays.

Browsing the web using Tor can be painfully slow, in some cases requiring several seconds or longer to load a page. Real-time audio and video communications require a connection with minimal delay, which Tor cannot deliver. Internet telephony and video conferencing services are simply unusable over metadata-protecting systems like Tor.

As a result, although individuals can use security technologies to protect the contents of their communications, there are significant technical barriers that make it difficult, if not impossible, to hide communications metadata, particularly for real-time communications services such as Internet telephony and video conferencing.

Telephony Metadata Reveals Content

Telephony metadata can be extremely revealing, both at the level of individual calls and, especially, in the aggregate.

Although this metadata might, on first impression, seem to be little more than "information concerning the numbers dialed,"[17] analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content.

In the simplest example, certain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence[18] and rape.[19] Similarly,

[17] Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act* 15 (Aug. 9, 2013), http://huff.to/1ey9ua5.
[18] *National Domestic Violence Hotline*, The Hotline (last visited Aug. 22, 2013), http://www.thehotline.org.
[19] *National Sexual Assault Hotline*, RAINN: Rape, Abuse & Incest National Network (last visited Aug. 22, 2013), http://www.rainn.org/get-help/national-sexual-assault-hotline.

numerous hotlines exist for people considering suicide,[20] including specific services for first responders,[21] veterans,[22] and gay and lesbian teenagers.[23] Hotlines exist for sufferers of various forms of addiction, such as alcohol,[24] drugs, and gambling.[25]

Similarly, inspectors general at practically every federal agency—including the NSA[26]—have hotlines through which misconduct, waste, and fraud can be reported, while numerous state tax agencies have dedicated hotlines for reporting tax fraud.[27] Hotlines have also been established to report hate crimes,[28] arson,[29] illegal firearms[30] and child abuse.[31] In all these cases, the metadata alone conveys a great deal about the content of the call, even without any further information.

The phone records indicating that someone called a sexual assault hotline or a tax fraud reporting hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of these numbers will still reveal information that virtually everyone would consider extremely private.

In some cases, metadata is even more sensitive than the contents of a communication. For example, wireless telephone carriers permit subscribers to donate to certain charities by sending a text message from their mobile phones. These systems require the subscriber to send a specific text message to a special number, which will then cause the wireless carrier to add that donation to the subscriber's monthly telephone bill. For example, by sending the word HAITI to 90999, a wireless subscriber can donate $10 to the American Red Cross.

---

[20] *District of Columbia/Washington D.C. Suicide & Crisis Hotlines*, National Suicide Hotlines (last visited Aug. 22, 2013), http://www.suicidehotlines.com/distcolum.html.
[21] *Get Help Now! Contact us to Get Confidential Help via Phone or Email*, Safe Call Now (last visited Aug. 22, 2013), http://safecallnow.org.
[22] *About the Veterans Crisis Line*, Veterans Crisis Line (last visited Aug. 22, 2013), http://www.veteranscrisisline.net/About/AboutVeteransCrisisLine.aspx.
[23] *We Provide Crisis Intervention and Suicide Prevention for LGBTQ Youth*, The Trevor Project (last visited Aug. 22, 2013), thttp://www.thetrevorproject.org
[24] *Alcohol Addiction Helpline*, Alcohol Hotline (last visited Aug. 22, 2013), http://www.alcoholhotline.com.
[25] *What is Problem Gambling?*, National Council on Problem Gambling (last visited Aug. 22, 2013), http://bit.ly/cyosu.
[26] Barton Gellman, *NSA Statements to the Post*, WASH. POST, Aug. 15, 2013, http://wapo.st/15LliAB.
[27] *Report Tax Fraud – Tax Fraud Hotline*, North Carolina Department of Revenue (last visited Aug. 22, 2013), http://www.dor.state.nc.us/taxes/reportfraud.html.
[28] *Report Hate Crimes*, LAMBDA GLBT Community Services (last visited Aug. 22, 2013), http://www.lambda.org/hatecr2.htm.
[29] *ATF Hotlines – Arson Hotline*, Bureau of Alcohol, Tobacco, Firearms and Explosives (last visited Aug. 22, 2013), http://www.atf.gov/contact/hotlines/index.html.
[30] *ATF Hotlines – Report Illegal Firearms Activity*, Bureau of Alcohol, Tobacco, Firearms and Explosives (last visited Aug. 22, 2013), http://www.atf.gov/contact/hotlines/index.html.
[31] *Childhelp National Child Abuse Hotline*, Childhelp (last visited Aug. 22, 2013), http://www.childhelp.org/pages/hotline-home.

Such text message donation services have proven to be extremely popular. Today, wireless subscribers can use text messages to donate to churches,[32] to support breast cancer research,[33] and to support organizations such as Planned Parenthood.[34] Similarly, after a policy change in 2012 by the Federal Election Commission, political candidates such as Barack Obama and Mitt Romney were able to raise money directly via text message.[35]

In all these cases, the most significant information—the recipient of the donation—is captured in the metadata, while the content of the message itself is less important. The metadata alone reveals the fact that the sender was donating money to their church, to Planned Parenthood, or to a particular political campaign.

Metadata can expose an extraordinary amount about our habits and activities. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations.

Aggregated Telephony Metadata Reveals Our Relationships

When call metadata is aggregated and mined for information across time, it can be an even richer repository of personal and associational details.

Metadata can identify our closest relationships. Two people in an intimate relationship may regularly call each other, often late in the evening. If those calls become less frequent or end altogether, metadata will tell us that the relationship has likely ended as well—and it will tell us when a new relationship gets underway. More generally, someone you speak to once a year is less likely to be a close friend than someone you talk to once a week. Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a *social graph.*

Metadata also reveals the structure and activities of organizations. By building a social graph that maps all of an organization's telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the organization's membership, donors, political supporters, and so on. Analysis of the metadata belonging to these individual callers, by moving one "hop" further out, could help to classify each one, eventually yielding a detailed breakdown of the organization's associational relationships.

---

[32] *Several Ways to Give*, The Simple Church (2013), http://bit.ly/1508Mgw; *Other Ways to Give*, North Point Church (last visited Aug. 22, 2013), http://bit.ly/16S3IkO.
[33] *Donate by Text*, Susan G. Komen for the Cure (last visited Aug. 22, 2013), http://sgk.mn/19AjGP7.
[34] *Help Support a New Future for Illinois Women and Families*, Planned Parenthood of Illinois (last visited Aug. 22, 2013), http://bit.ly/1bXI2TX.
[35] Dan Eggen, *Text to 'GIVE' to Obama: President's Campaign Launches Cellphone Donation Drive*, WASH. POST, Aug. 23, 2012, http://bit.ly/16ibjCZ.

Even our relative power and social status can be determined by calling patterns. As *The Economist* observed in 2010, "People at the top of the office or social pecking order often receive quick callbacks, do not worry about calling other people late at night and tend to get more calls at times when social events are most often organized (sic), such as Friday afternoons."[36]

At times, by placing multiple calls in context, metadata analysis can even reveal patterns and sensitive information that would not be discoverable by intercepting the content of an individual communication.

For example, although metadata revealing a single telephone call to a bookie may suggest that the caller is placing a bet, analysis of metadata *over time* could reveal that someone has a gambling problem, particularly if the call records also reveal a series of calls to payday loan services.

With a database of telephony metadata reaching back five years, many of these kinds of patterns will emerge once the collected phone records are subjected to even the most basic analytic techniques.

In short, aggregated telephony metadata allows the NSA to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, or the social dynamics of a group of associates.

Data-Mining Across Many Individuals Is More Revealing

Advances in the area of "Big Data" over the past few decades have enabled researchers to observe even deeper patterns by mining large pools of metadata that span many telephone subscribers.

Researchers have studied databases of call records to analyze the communications reciprocity in relationships,[37] the differences in calling patterns between mobile and landline subscribers,[38] and the social affinity and social groups of callers.[39]

---

[36] *Mining Social Networks: Untangling the Social Web,* ECONOMIST, Sep. 2, 2010, http://econ.st/9iH1P7.

[37] Lauri Kovanen, Jari Saramaki & Kimmo Kaski, *Reciprocity of Mobile Phone Calls*, Dynamics of Socio-Economic Systems (Feb. 3, 2010), http://arxiv.org/pdf/1002.0763.pdf.

[38] Heath Hohwald, Enrique Frias-Martinez & Nuria Oliver, *User Modeling for Telecommunication Applications: Experiences and Practical Implications* 8, (Data Mining and User Modeling Group, Telefonica Research, 2013), http://bit.ly/1d7WkUU ("Interestingly, Monday is the day with most calls for landline users, while Friday is the day with most calls for mobile users. . . Mobile users spend less time on the phone than landline users.").

Researchers have discovered that individuals have unique calling patterns, regardless of which telephone they are using,[40] they have figured out how to predict the kind of device that is making the calls (a telephone or a fax machine),[41] developed algorithms capable of predicting whether the phone line is used by a business or for personal use,[42] identified callers by social group (workers, commuters, and students) based on their calling patterns,[43] and even estimated the personality traits of individual subscribers.[44]

The work of these researchers suggests that the power of metadata analysis and its potential impact on the privacy of individuals increases with the scale of the data collected and analyzed. Just as multiple calls by the same person reveal more than a single call, so too does a database containing calling data about millions of people reveal more information about the individuals contained within it than a database with calling data about just one person.

The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of a few days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people. Mass collection not only allows the NSA to learn information about more people, but it also gives the NSA the ability to learn new, previously private facts about innocent Americans that it could not have learned simply by collecting the information about a few, specific individuals.

Technical Expertise Bolsters Oversight and Public Understanding

Some of the frustration voiced by the Foreign Intelligence Surveillance Court in its declassified opinions seems to stem from the Court's discovery that the NSA had not disclosed significant technical information in earlier proceedings. One need not

---

[39] Sara Motahari, Ole J. Mengshoel, Phyllis Reuther, Sandeep Appala, Luca Zoia & Jay Shah, *The Impact of Social Affinity on Phone Calling Patterns: Categorizing Social Ties from Call Data Records*, The 6th SNA-KDD Workshop (Aug. 12, 2012), http://b.gatech.edu/1d6i4RY.

[40] Corrina Cortes, Daryl Pregibon & Chris Volinsky, *Communities of Interest*, AT&T Shannon Research Labs, http://www.research.att.com/~volinsky/papers/portugal.ps.

[41] Haim Kaplan, Maria Strauss & Mario Szegedy, *Just the Fax – Differentiating Voice and Fax Phone Lines Using Call Billing Data*, AT&T Labs, http://bit.ly/19Aa8Ua.

[42] Corinna Cortes & Daryl Pregibon, *Giga-Mining*, AT&T Labs-Research, http://bit.ly/153pMcI.

[43] Richard A. Becker, Ramon Caceres, Karrie Hanson, Ji Meng Loh, Simon Urbanek, Alexander Varshavsky & Chris Volinsky, *Clustering Anonymized Mobile Call Detail Records to Find Usage Groups*, AT&T Labs-Research, http://soc.att.com/16jmKdz.

[44] Rodrigo de Oliveira, Alexandros Karatzoglou, Pedro Concejero, Ana Armenta & Nuria Oliver, *Towards a Psychographic User Model from Mobile Phone Usage*, CHI 2011 Work-in-Progress (May 7–12, 2011), http://bit.ly/1f51mOy; *see also* Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic & Alex (Sandy) Pentland, *Predicting People Personality Using Novel Mobile Phone-Based Metrics*. Social Computing, Behavioral-Cultural Modeling and Prediction (2013), http://bit.ly/1867vWU.

postulate bad faith on the NSA's part to explain how this could have happened. Technologists within the NSA surely knew how their program operated, but this knowledge had to pass through intermediaries, some of them less attuned to the significance of certain technical details, before reaching the Court. A good faith effort to simplify the technical explanation for the Court's benefit could have led to the omission of information that the Court later found highly relevant. And the Court, without access to technical advice, was not able to ask the sort of probing technical question that might have elicited the missing information.

In order to ensure strong oversight of these complex programs, the overseers must have independent access to robust technical expertise. Fortunately, the United States has the world's strongest pool of experts in these areas. I look forward to your questions today and, more broadly, to continued constructive engagement between oversight officials and technical experts.

Statement for the Record

United States Senate

Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Carrie F. Cordero

Director of National Security Studies
& Adjunct Professor of Law

Georgetown University Law Center

Introduction

Mr. Chairman, Ranking Member Grassley, members of the Committee, thank you for this opportunity to share my views on the important issue of continued oversight of intelligence activities conducted under the Foreign Intelligence Surveillance Act (FISA). I am honored to be here with you today, and so pleased to share the panel today with my colleague at Georgetown Law, Professor Laura Donohue, as well as with Professor Edward Felten of Princeton.

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

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

In addition, there is another aspect of my experience that may not be readily apparent, but that significantly impacts my views on FISA reform: I started working in the national security component of the Justice Department in January 2000. Later that year, I supported investigative efforts after the bombing of the USS Cole. On the morning of September 11, 2001, I was dispatched to the FBI's Strategic Information Operations Center, or SIOC, to help stand up our office's base there for the days and months to come. I remember the moment that morning when

we thought it was possible that there could be as many as fifty to one hundred thousand people in the Twin Towers. I remember the announcement in SIOC that former FBI New York Special Agent John O'Neill had perished in the attack. And I remember the minutes when we were not sure whether there was an additional plane over Washington, D.C., only to learn later that it had been brought down in a field in Pennsylvania. I would also be remiss in recounting my memories from that morning if I did not mention perhaps the finest example of leadership I had ever seen, then, or, since: that of former FBI Director Mueller walking the floor of SIOC, just over a week into the job, alongside the rest of us: visible, present, reassuring.

But I remember other things, too, from that morning, and the hours and days that followed. I recall senior leaders of the Department of Justice racing to obtain the signatures of the Attorney General and the FBI Director on emergency FISA applications because, at that time, the law only provided 24 hours from the time of the Attorney General's oral authorization to the time the application had to be presented to a judge. I also remember being responsible for obtaining pages and pages of secure faxes, which we taped up onto the wall of our small, over-crowded office in SIOC. The faxes contained the signatures of federal prosecutors and analysts who were on the criminal side of the so-called "wall" that had been erected between law enforcement and intelligence investigators as a result of cautious interpretations of FISA that had developed, and then cemented, over time. In accordance with the FISC's orders, we had to obtain their signatures before passing them intelligence information that would assist the FBI's investigation of the attacks. We were tripping over process, but dutifully following court orders, even then.

As a result, I had an up-front view regarding how the USA Patriot Act of 2001, the Intelligence Reform and Terrorism Prevention Act of 2004, and later the FISA Amendments Act of 2008, all vastly improved the Intelligence Community's ability to protect the nation from another attack on the scale of September 11th.

Which brings me to where we are today. From my perspective, the challenge for members of this Committee is to identify whether there are actual problems with either the law or process, and then craft remedies that address those specific issues. I am here to urge caution in implementing "quick fixes" that may sound appealing based on public or media-driven pressure, but that could have lasting consequences at a practical level that could negatively impact Intelligence Community operations and the nation's security for years to come.

On that point, it is worth noting that the FISA process, for approximately the preceding fifteen years, was subject to the exact *opposite* criticism that it seems to be today: the Department of Justice was accused of being too reticent, too cautious, too unwilling to be aggressive under the law in order to protect the national security. This Committee is very familiar with this history. To provide just a few examples: in May 2000, the Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation was issued.[1] That report concerned the handling of the Wen Ho Lee case, a counterintelligence investigation, and included a critical analysis of the interaction between, and

[1] *Final Report, Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* (AGRT Report, also known as the Bellows report). (available at://www.justice.gov/ag/readingroom/bellows.htm).

the legal judgment of, the FBI and the Department of Justice concerning their interpretations of FISA standards, such as probable cause, in the late 1990s.[2] In a separate review of the FISA process, this Committee issued a report in February 2003 on FISA Implementation Failures. That report focused primarily on deficiencies in FBI operations, but focused in significant part on problems that prevented the FBI from "aggressively pursuing FISA applications..." [3]

A third example arose five years later. In an exchange of letters in October 2008, New York City Police Commissioner Raymond Kelly criticized the Department of Justice under Attorney General Michael Mukasey's tenure of being unwilling to present close or borderline cases to the FISC for consideration.[4] Attorney General Mukasey strongly rejected the NYPD's claims and defended the Department's practice before the Court, stating in part, "[o]ur successful advocacy before the Court depends on the accuracy of our factual representations and the reliability of our assessments of those facts...."[5] Although today's criticisms of FISA operations have now shifted from targeting one agency (FBI) to another (NSA), for those, like me, who worked in national security operational law components during these years, it is an ironic twist to hear today's criticisms that the Department of Justice attorneys in this process may not be adequately representing both the national security as well as civil liberties interests of Americans in their presentations made to the Court; that we need more lawyers scrutinizing already well-scrubbed applications; and that the government should be putting forth more cautious interpretations of the law.

So let's turn to what may or may not need fixing in FISA as it currently stands. Based on the public and legislative debate since the unauthorized disclosures by Edward Snowden in the *Guardian* and *Washington Post* beginning earlier this summer, I have observed three main critiques. These include: (i) that collection under section 702 of FISA and/or Section 215 of the USA Patriot Act are illegal; (ii) that there is a crisis of public confidence in NSA, the Intelligence Community, and activities conducted under FISA, and that this confidence could be restored by opening FISA practice to some form of adversarial process; and (iii) that FISA activities and legal rulings should be more transparent. Let me take each of those three critiques and some of the proposed reforms one-by-one.

---

[2] *See, eg.* Chapter 11, AGRT Report.

[3] *Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures*, February 2003 (available at www.fas.org/irp/congress/2003_rpt/fisa.html). The report criticized, in particular, FBI and DOJ's "too high" standard to establish probable cause, among other statutory requirements.

[4] *Letter from NYPD Police Commissioner Raymond W. Kelly to Attorney General Michael Mukasey*, October 27, 2008 (available at http://online.wsj.com/public/resources/documents/Mukasey111908.pdf).

[5] *Letter from Attorney General Michoel Mukasey to NYPD Police Commissioner Roymond W. Kelly*, October 31, 2008 (available at http://online.wsj.com/public/resources/documents/WSJ_200811202Kelly.pdf). In response to the NYPD's request that the Department lower the legal standard of submitting matters to the Court, the Attorney General stood firm, stating:

> "We are acutely aware of the stakes, and, as a result, already try to be as aggressive in our approach as we can within the bounds of reason and the law. If we were to lower the standard, the risk would not be limited, as you suggest, to a few more rejected applications. Rather, as should be apparent...the result would be counterproductive and would impair our ability to seek FISA coverage on worthy targets around the country. This I cannot, and will not, do."

Proposals to Restrict Foreign Intelligence Collection Under FISA

From my perspective, the arguments that these programs – and I am referring to both the section 702[6] collection and the section 215[7] collection – are illegal are mostly arguments about what the law *should be*, not what the law *is*. I note that the analysis under each of these sections is a different one, and, I would submit that the government's interpretation of section 215 is a more forward-leaning interpretation of the law than is its implementation of section 702. But generally, the arguments that either or both of these programs may be unlawful focus on the changes to technology, the differences in how our information is retained and how we communicate today versus decades ago, and on the Fourth Amendment concept concerning what constitutes a reasonable expectation of privacy.

Section 702 collection is targeted against non-U.S. persons reasonably believed to be outside the United States. These are not individuals with Constitutional protections, and the collection against them is conducted in accordance with the statutory framework passed by Congress in the FISA Amendments Act of 2008. The FISA Amendments Act enhanced protections for U.S. persons worldwide by requiring that an individual probable cause-based order be obtained from the FISC for electronic surveillance or physical search no matter where in the world that U.S. person is located. The minimization procedures governing 702 collection have now been declassified, and demonstrate the detailed procedures with which the NSA handles U.S. person information. The 702 framework was debated extensively and publicly, and members of this Committee have been kept informed of its implementation in accordance with the reporting provisions of FISA.

With respect to the metadata collection under section 215, it is a fair characterization that this program is large in scale. And reasonable minds can and do disagree about whether its interpretations of relevance under the statute, or reasonableness under the Fourth Amendment, are overly broad. But I would submit that the Government's arguments in this case are consistent with existing precedent, no matter what direction the courts may go in the future. Current Supreme Court precedent still holds that there is no expectation of privacy in our telephone metadata, that is, the numbers we dial or the numbers that dial us. A warrant is not required to obtain this information.[8] Likewise, Supreme Court precedent also still holds that we do not have a reasonable expectation of privacy in records voluntarily turned over to a third party.[9] The legal justification, both statutory and constitutional, is outlined in the Administration's White Paper dated August 9, 2013.[10]

In addition, the recently declassified opinion and order by FISC Judge Claire Eagan dated August 29, 2013, approving continuation of the business records metadata program, offers a straightforward analysis of the law. Judge Eagan wrote:

---

[6] Section 702 of FISA was added to FISA by the FISA Amendments Act of 2008.

[7] Section 215 refers to Section 215 of the USA Patriot Act, which can be found in section 501 of FISA.

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

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

[10] *Administration White Paper on Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act*, August 9, 2013 (available at http://www.scribd.com/doc/159211491/Obama-administration-white-paper-on-NSA-surveillance-oversight)

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

I do not mean to suggest that, over the course of the next several years or longer, that courts, including the Supreme Court, may come to different conclusions about expectation of privacy that may impact intelligence collection under FISA. They very well may. But I do suggest that the current collection activities, based on the FISC opinions and accompanying materials that have been declassified by the government, are consistent with *current* precedent and *existing* interpretations of the laws.

Moreover, with respect to 215 in particular and intelligence programs generally, I believe that they should be regularly reviewed and evaluated to determine whether they continue to be necessary and valuable. It is wholly appropriate to end a collection program that has outlived its usefulness, or perhaps is no longer necessary based on new technologies or methods of collecting intelligence that may be more efficient or productive. But, based on what senior leaders of the Intelligence Community are advising today, the 215 program remains a valuable part of the protective infrastructure that was implemented after September 11th. Therefore, in my view, it would be premature for Congress to end it altogether, abruptly through legislation.

Proposals Regarding a FISA Special Advocate and Efforts to Restore Public Confidence

A second critique of FISA is that it is a one-sided enterprise that only permits the government to argue its case to the FISC. That, of course, was by design in the original 1978 law, both in alignment with the manner in which federal criminal electronic surveillance applications and search warrants are presented to judges for review, as well as in order to protect the classified information, sources and methods that are involved in conducting national security electronic surveillance or search activities.

Two themes emerge in proposals to add a special advocate, or public interest advocate, to the FISA process. One view, suggested separately by two different two former FISC judges, is that the Court would benefit from an additional view, particularly in cases involving technical complexity and/or novel legal issues.[12] A second view is that a special advocate would go a long

---

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

[12] James G. Carr, *A Better Secret Court*, N.Y. Times, July 22, 2013 (available at http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html). Former FISC Judge James Robertson similarly endorsed the idea of an adversary in public remarks. Charlie Savage, *Nation Will Gain by Discussing*

way in restoring public confidence in the FISA process. I have concerns about both proposals, both as a matter of principle as well as a practical matter.

To begin, it would truly be a sea change to start *litigating* foreign intelligence collection *before* it takes place. There are already lawyers in the government who view it as their job to work in the public interest. In particular, the lawyers in the National Security Division in the Department of Justice work in the best tradition of *ex parte in camera* practice, where they present both supportive and derogatory information to the Court, when presenting a matter that raises factual or other issues. There are also legal advisors who work for the court who are an additional layer of independent review. And then there are the judges themselves, who are independent Article III federal district court judges.[13]

This is one area where the proposals put forth in Congress may not quite match the desired objective. In this case, if what the Court seeks – and it would be helpful to hear from the current Court on this issue – is simply an additional view beyond that which is presented by the Justice Department on behalf of the Intelligence Community, then I would submit that empowering the existing Civil Liberties Protection Officer (CLPO)[14] to present his views directly to the FISC would serve that purpose. The CLPO is a statutory-based position created by the Intelligence Reform and Terrorism Prevention Act, which amended the National Security Act of 1947. While this proposal would not provide the optic some may desire to add an outside government component, it certainly would address the substantive concern that the Court could benefit from an additional view when considering particularly complex issues that impact privacy and civil liberties. And it would do so without adding substantial layers of additional bureaucracy.

On the public confidence point, I would suggest that an outside advocate would not carry the weight that is hoped it might provide with the public in the longer term. If done in a manner protective of classified information, the advocate would necessarily work in secret, alongside the Executive Branch. On that count, with the passage of time, outside observers will just see the advocate as another participant in a secret process. As a practical matter, an outside advocate would require a tremendous amount of start-up time, effort and money in order to perform effectively. By start-up time and effort, what I am referring to is, in significant part, the knowledge and expertise that government participants in the FISA process maintain on an ongoing basis. For example, the recently declassified report of the 702 joint interagency oversight team reveals how frequently the interagency participants meet, discuss and are briefed

---

Surveillance, Expert Tells Privacy Board, N.Y. Times, July 9, 2013 (http://www.nytimes.com/2013/07/10/us/nation-will-gain-by-discussing-surveillance-expert-tells-privacy-board.html?_r=0).

[13] Judge Walton, Presiding Judge of the FISC, provided a detailed accounting of the interaction between the government and the Court, and the Court's consideration of matters before it, in a letter to Chairman Leahy on July 29, 2013 (available at http://www.uscourts.gov/uscourts/courts/fisc/honorable-patrick-leahy.pdf).

[14] The CLPO reports directly to the Director of National Intelligence and, by law, is responsible for ensuring "that the protection of civil liberties and privacy is appropriately incorporated into the policies and procedures developed for and implemented by the Office of the Director of National Intelligence and the elements of the intelligence community within the National Intelligence Program," among other duties. Section 103D of the National Security Act of 1947, as amended (50 U.S.C. § 403-3d].

on ongoing implementation matters.[15] It would be very difficult for an outsider to enter a proceeding on a complex issue, and meaningfully participate, without this substantial background and expertise. It would take time for the outside advocate to become sufficiently knowledgeable for the proceedings to begin. Accordingly, the start-up efforts likely would not provide an environment for the advocate to work expeditiously when important national security collection objectives may be at stake.

It is also useful to think about just what would the advocate's role be with respect to representing the public interest? Thinking back to the example of the wall that was corrected by the change to FISA's purpose standard by the USA Patriot Act in 2001 and the subsequent decision by the Foreign Intelligence Surveillance Court of Review in 2002,[16] the perpetuation of the wall was probably the most significant incorrect legal interpretation regarding FISA ever made by the Department of Justice and the FISC. According to the Foreign Intelligence Surveillance Court of Review in 2002, the conventional interpretation of the purpose requirement turned out to be a false premise.[17] Would an outside special advocate, had it existed back then, have argued for a *lessening* of restrictions that had been imposed by the Justice Department and later the FISC? In hindsight, *that* probably would have been in the public interest. Current conceptions of the public interest advocate seem only to focus on the public interest in terms of protecting the public's privacy and civil liberties. But acting in the public interest can sometimes mean making fulsome or even aggressive arguments under the law in order to protect the public from terrorist attacks and other threats to the national security.

So what would enhance public confidence? Perhaps the most frustrating part of the reaction to the leaks from my perspective has been the nearly complete lack of confidence in or comfort by the existing oversight mechanisms, particularly with respect to 702 collection. This oversight structure includes oversight internally at NSA, through its Office of the Director of Compliance, General Counsel's office, and Inspector General's office; by the Department of Justice and the Office of the Director of National Intelligence; by the FISC; and by Congress. The oversight is extensive, and exhaustive. The results of the oversight reviews are reported to the Intelligence and Judiciary Committees. The recently declassified report issued in August 2013[18] provides insight into the granularity of how this oversight process takes place, as well as into the nature of the compliance incidents themselves. Assuming that we intend to keep the basic framework of internal executive branch oversight and Congressional oversight through the committee structure,[19] then an area that requires focus is achieving a place where the

---

[15] *Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence*, covering the period June 1, 2012-November 30, 2012, August 2013 (available at http://www.scribd.com/doc/159211491/Obama-administration-white-paper-on-NSA-surveillance-oversight).

[16] *In Re Sealed Case*, 310 F.3d 717, 743 (For.Intel.Surv.Rev. 2002).

[17] *Id. at* 743.

[18] *Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence*, covering the period June 1, 2012-November 30, 2012, August 2013 (available at http://www.scribd.com/doc/159211491/Obama-administration-white-paper-on-NSA-surveillance-oversight).

[19] Prepared statement of Benjamin Wittes before the Senate Select Committee on Intelligence, "Legislative Changes to the Foreign Intelligence Surveillance Court," September 26, 2013 (available at

Congressional oversight committees can both gain, and then communicate to the public, their satisfaction with the oversight process and the underlying activities themselves. Here are a few suggestions for what might be steps in the right direction:

First, Congress can ensure that the offices conducting oversight, including the Office of the Director of Compliance at NSA, the Oversight Section in the Office of Intelligence, National Security Division, and the Office of General Counsel and Civil Liberties Protection Office, in the Office of the Director of National Intelligence, and any other offices involved in the compliance process at these or other Intelligence Community elements, are staffed and funded appropriately to their responsibilities. The internal Executive Branch oversight process that has been built requires a lot of man-hours to do right. The quality of oversight will suffer if any of these offices are stretched beyond their capabilities.

Second, Congress could consider requiring an annual or semi-annual public report that produces information currently contained in the classified joint compliance assessment in a summary fashion, instead of relying on the heavily redacted lengthy report. This report might help better inform Members of Congress beyond the Judiciary and Intelligence Committees regarding the oversight and compliance process.

Third, Congress should focus its oversight efforts in working with the NSA, the Justice Department, and other components of the Intelligence Community to *reduce* the complexity of internal procedures.[20] I recognize that this recommendation may sound counterintuitive, and may also be, perhaps, a role more appropriate for the Intelligence committees. But I will expand briefly, nonetheless. One aspect of reducing compliance incidents is reducing the complexity of internal operating procedures to ensure that operators at the working level have a clear understanding of what rules they are operating under. Several years ago, the Department of Justice had success in this area by reducing several sets of FBI investigative guidelines into one set of rules, and similarly redesigning several different sets of minimization procedures into clearer, more streamlined rules.

In my experience, various elements of the Intelligence Community tend to have different philosophies and practices on this front. Some elements, through their offices of General Counsel, believe that it is better for the lawyers to be the primary readers and interpreters of certain procedures and court orders, and then produce summary documents and training materials that operators at the line level can read, understand and use on a daily basis. Other legal offices tend to provide the underlying documents themselves to the line operators, and expect them to read and understand them, in addition to training that is provided. This practice would be more akin to criminal practice where law enforcement officers executing a search warrant read and understand it, before executing a search. What may be happening in the FISA context, is that the court orders and underlying procedures are so complicated, so complex, that, in some cases,

---

http://www.lawfareblog.com/wp-content/uploads/2013/09/Wittes-SSCI-Hearing-Statement_Final-Draft_9.26.13.pdf).

[20] *See, eg.*, the recently declassified *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf)

only the lawyers understand what they mean. That opens the door for internal summary documents for the workforce and training materials to inadvertently depart from what the procedures actually are. Or, the converse happens, where the procedures are written in language or format that has come to be expected, but something gets lost in translation from what the technical or operational personnel originally intended. Accordingly, my own view is that the better practice is to have clear, straightforward, comprehensible rules from the outset.

Note that I am not suggesting, in any way, a loosening of restrictions. Indeed, the FISC's approvals of the collection programs at issue are heavily reliant on the substance and rigor of the underlying procedures.[21] And I am also not suggesting that what I am describing is necessarily responsible for the specific compliance matters described in the documents that have recently been declassified. But, although the current compliance incident rate is very low, there is always value in continuing to find ways to improve compliance. The committees should know that undertaking work in this area is hard, time consuming and completely unglamorous. But it might go some distance in reducing the gap in translation between what the rules are, and what is actually happening at the ground level, thereby reducing compliance incidents and improving confidence.

Proposals to Enhance Transparency

The third main critique is that the FISA process, both in terms of collection activities and legal interpretations, should be more transparent. There are a number of constituencies that have called for greater transparency for some time. The current Administration, in the post-Snowden environment, similarly seems to have embraced a level of transparency the Intelligence Community has not previously experienced.[22] On this point, I would suggest that there is room for Congress to act. My own view is that the seemingly ad hoc nature of the recent government declassification releases is not actually helping the Intelligence Community as much as they might think. To some extent, the periodic and sudden releases of significant legal opinions only continues to feed the media frenzy and keeps attention on the Intelligence Community. Congress needs to help the Intelligence Community get out of the news, and one way to do that would be to work with the Director of National Intelligence and Attorney General to determine what might be a more regularized and consistent method of releasing information. For example, Congress could amend the reporting provisions in FISA to provide additional public information—whether it is statistics, declassified legal opinions, summaries of implementation actions or reports on compliance matters—semi-annually, quarterly, or at some other appropriate regular interval. In my view, this would cut back on each release being an event unto itself.

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

[22] Prepared remarks of DNI James Clapper before the Senate Select Committee on Intelligence, September 26, 2013 (available at http://icontherecord.tumblr.com/tagged/testimony).

Conclusion

At the end of the day, the Committee will need to evaluate whether it seeks to scale back the actual intelligence activities that the Intelligence Community advises continues to provide important protection for our national security, or instead focus on measures that will substantively enhance the Congress' own confidence in the Intelligence Community, and subsequently, public confidence. As I have outlined above, my perspective is that the intelligence activities currently conducted under FISA are conducted lawfully, and with care. That said, there is substantial value in restoring public confidence in these activities through focusing oversight efforts on substantive areas that will achieve the intended results. I thank the Chairman, Ranking Member and Committee Members for providing me with this opportunity to share my views on current FISA reform proposals.

Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing on "Continuing Oversight of the Foreign Intelligence Surveillance Act"
October 2, 2013

Today, the Judiciary Committee meets to conduct further oversight of the intelligence community's use of the Foreign Intelligence Surveillance Act, or FISA. No one knows for sure how long the Federal government will be shut down, but I feel strongly that the Senate Judiciary Committee must continue its work on this important subject. I consulted with Senator Grassley about this, and I appreciate that Director Clapper and General Alexander have agreed to proceed with the hearing today as scheduled. I am certain that they join me in thanking all of the dedicated intelligence community professionals who are also doing their jobs today despite the needless shutdown of the Federal government. That said, I have decided to cancel the committee's weekly business meeting tomorrow in light of the government shutdown.

As we continue to re-examine the intelligence community's use of FISA authorities, let's be clear that no one underestimates the threats that our country continues to face, or the difficulty of identifying and meeting those threats. We can all agree that we should equip the intelligence community with the necessary and appropriate tools to help keep us safe. But I hope that we can also agree that there have to be limits on the surveillance powers we give to the government. Just because something is technologically possible, and just because something may be deemed technically legal, does not mean that it is the right thing to do.

This summer, many Americans learned for the first time that 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. The American public also learned more about the government's collection of internet content data through the use of Section 702 of FISA.

Since the Committee's last hearing on these revelations in late July, the American people have learned a great deal more. They have learned that the NSA has engaged in repeated, substantial legal violations in its implementation of both Section 215 and Section 702 of FISA. For example, the NSA collected, without a warrant, the content of tens of thousands of wholly domestic emails of innocent Americans. The NSA also violated a FISA Court order by regularly searching the Section 215 phone records database without meeting the standard imposed by the Court.

These repeated violations led to several reprimands from the FISA Court for what it called "systemic noncompliance" by the government. The Court also has admonished the government for making a series of substantial misrepresentations to the Court. Though we have seen no evidence of intentional abuse of FISA authorities, this pattern of misuse is deeply troubling.

The American people also have learned that the NSA in 2011 started searching for Americans' communications in its Section 702 database – a database containing the contents of communications acquired without individualized court orders. And just this past weekend, the *New York Times* reported that the NSA is engaging in sophisticated analysis of both domestic and international metadata to determine the social connections of Americans.

As a result of these revelations, it is no surprise that the intelligence community faces a trust deficit. After years of raising concerns about the scope of FISA authorities and the need for stronger oversight, I am glad that many Members of Congress are now interested in taking a close look at these programs – at both the government's legal and policy justifications for them, and the adequacy of the existing oversight regimes.

In my view, it is time for a change. Additional transparency and oversight are important parts of that change, but I believe we must do more.

That is why I am working on a comprehensive legislative solution with Congressman Sensenbrenner, Chairman of the Crime and Terrorism Subcommittee in the House, as well as other members of Congress across the full political spectrum. Our bipartisan, bicameral legislation will address Section 215 and Section 702, and a range of surveillance authorities that raise similar concerns.

Our legislation would end Section 215 bulk collection. It also would ensure that the FISA pen register statute and National Security Letters (NSLs) could not be used to authorize bulk collection. The government has not made its case that bulk collection of domestic phone records is an effective counterterrorism tool, especially in light of the intrusion on Americans' privacy. In addition, I find the legal justification for this bulk collection to be strained at best, and the classified list of cases involving Section 215 to be unconvincing. As the Deputy Director of the NSA himself acknowledged at our last hearing, there is no evidence that Section 215 phone records collection helped to thwart dozens or even several terrorist plots.

In addition to stopping bulk collection, our legislation would improve judicial review by the FISA Court and enhance public reporting on the use of a range of surveillance activities. The bill would also require Inspector General reviews of the implementation of these authorities – putting into law a request that Senator Grassley and I, and eight other members of this Committee, made last week to the Inspector General for the Intelligence Community. This is a commonsense, bipartisan bill – and I look forward to working on this effort in the coming months with those in the Senate, in the House, and in the administration.

I appreciate the concrete steps that both Director Clapper and General Alexander have made in recent months to brief members of Congress and move towards more transparency and further declassification of documents. I also welcome the participation of the legal and technical experts on our second panel, and would note with particular pride that my alma mater, Georgetown Law, is well-represented among those witnesses.

I hope that today's hearing will help inform our legislative efforts. We must do all that we can to ensure our nation's security, restore the trust of the American people in our intelligence community, and protect the fundamental liberties that make this country great.

#####

"Continued Oversight of the Foreign Intelligence Surveillance Act" Hearing
Senator Franken Questions for the Record

(1) Professor CORDERO, in your written testimony you criticized what you called, quote, "the ad hoc nature of the recent government declassification releases." You said you thought that these disclosures weren't helping the Intelligence Community as much as they might think. And you suggested that Congress could amend the reporting provisions in FISA to require additional public information at regular intervals. What specific information do you think these reports should include?

"Continued Oversight of the Foreign Intelligence Surveillance Act" Hearing
Senator Franken Questions for the Record

(1) Professor DONOHUE, in August the Office of the Director of National Intelligence announced that it would start annually disclosing to the public the number of orders issued under key surveillance authorities, as well as the number of quote, "targets" affected by these orders. Are these promised disclosures enough? Or are actual changes to the law necessary to achieve greater transparency?

Senate Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Questions for the Record from Ranking Member Charles E. Grassley

General Keith Alexander, NSA Director

1. 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 accessed and 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? Please answer this question in an unclassified format, to the extent possible.

Senate Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Questions for the Record from Ranking Member Charles E. Grassley

James Clapper, Director of National Intelligence

1. Why aren't essential and necessary national security functions of the executive branch excepted under the Antideficiency Act as "authorized by law" under 31 U.S.C. § 1341 (a)(1)(B), even if their suspension does not imminently threaten the safety of human life or the protection of property under 31 U.S.C. § 1342, as determined by the Congressional Research Service? *See* Pat Towell & Amy Belasco, "Government Shutdown: Operations of the Department of Defense During A Lapse In Appropriations," Congressional Research Service, R41745, October 1, 2013, p. 13.

Senate Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Professor Carrie Cordero

1. As this Committee considers changes to the FISC process, including the possibility of creating some kind of independent advocate to appear before the Court, what important operational considerations would you urge the Committee to consider?

2. What would be the effect of a change in the law that would require prosecutors to obtain a search warrant in order to obtain materials, such as phone records, that are in the possession of third parties, instead of obtaining them through a subpoena?

3. Why shouldn't there be specific criminal sanctions against those who intentionally or knowingly misuse the phone metadata that is collected?

Senate Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Professor Laura Donohue

1. Do you believe that in a typical criminal investigation, the government should be required to obtain a search warrant in order to obtain telephone records or other telephone metadata, even though these materials are in the possession of a third party? If so, how would that legal rule affect these investigations, in which prosecutors currently obtain such records with a grand jury subpoena?

2. There is some precedent in the law for the government to collect large categories of records in bulk that may be relevant to an investigation and then to later analyze those records to determine what specific items are in fact relevant. For example, in one case a federal appeals court upheld the use of a grand jury subpoena to acquire all money order applications from a particular location above a certain monetary threshold over a period of years. The court upheld the subpoena even though, inevitably, most of the records acquired would not be associated with any criminal activity. That case is *In Re Grand Jury Proceedings: Subpoena Duces Tecum*, 827 F.2d 301 (8th Cir. 1987). Obviously, bulk collection of metadata under Section 215 is much broader than that example. Are there other ways you would distinguish cases like this, in which this type of collection has been upheld as legal, from the government's acquisition of telephone metadata under Section 215, which you contend is illegal? Would you contend that cases such as the above are wrongly decided?

Senator Mazie K. Hirono

Questions for the Record following hearing on October 2, 2013 entitled:

"Continued Oversight of the Foreign Intelligence Surveillance Act"

The Honorable Keith B. Alexander, Director, National Security Agency

1. At the hearing I asked if the Intelligence Community and the NSA specifically are focusing on evolving the technology of privacy safeguards as the surveillance technology is clearly evolving.

    a. Can you give examples of what kinds of new technical capacity to protect privacy we can expect to benefit from in the future?

    b. Is the NSA working to develop narrower, more targeted collection or is all the research and development focused on expanding access to information?

2. It has been reported that certain data collected by the NSA are shared with domestic law enforcement agencies.

    a. What is the legal authority that allows the NSA to give Section 215 of the Patriot Act and FISA Amendments Act Section 702 data to other agencies such as the FBI, DEA, or other law enforcement agencies?

    b. Does such sharing require the demonstration of "probable cause" before such data are shared?

    c. Is the FISA court involved in such approvals on a case-by-case basis?

3. At the hearing I asked if PRISM is the only intelligence program NSA runs under FISA Section 702 and what other programs are run under sections 215 and 702.

    a. Please provide a complete list of the programs and their purposes that are operated by the NSA under the authorities provided by sections 215 and 702?

4. In conducting the programs under Sections 215 and 702 authorities, could less intrusive methods of collection have yielded the same information?

5. At the hearing several questions were asked related to the recent disclosure by the NSA Inspector General that 12 instances of intentional misused of signals intelligence authorities of the Director of the National Security Agency.

a. You indicated that "highlighting the punishments that go along with this" type of misuse should help prevent future instances of this type of misuse. Do you believe that increased criminal penalties for this type of privacy violation by intelligence analysts would help with deterrence?

Senator Mazie K. Hirono

Questions for the Record following hearing on October 2, 2013 entitled:

"Continued Oversight of the Foreign Intelligence Surveillance Act"

The Honorable James R. Clapper, Director of National Intelligence

1. At the hearing I asked if the Intelligence Community and the NSA specifically are focusing on evolving the technology of privacy safeguards as the surveillance technology is clearly evolving.

    a. Can you give examples of what kinds of new technical capacity to protect privacy we can expect to benefit from in the future?

    b. Are the NSA and other Intelligence Community agencies working to develop narrower, more targeted collection or is all the research and development focused on expanding access to information?

2. It has been reported that certain data collected by the NSA are shared with domestic law enforcement agencies.

    a. What is the legal authority that allows the NSA to give Section 215 of the Patriot Act and FISA Amendments Act Section 702 data to other agencies such as the FBI, DEA, or other law enforcement agencies?

    b. Does such sharing require the demonstration of "probable cause" before such data are shared?

    c. Is the FISA court involved in such approvals on a case-by-case basis?

3. At the hearing I asked if PRISM is the only intelligence program NSA runs under FISA Section 702 and what other programs are run under sections 215 and 702.

    a. Do any other agencies run intelligence programs under Section 215?

    b. Do any other agencies run intelligence programs under Section 702?

    c. Please provide a complete list of the programs and their purpose that are operated by the NSA or other agencies under the authorities provided by sections 215 and 702?

4. In conducting the programs under Sections 215 and 702 authorities, could less intrusive methods of collection have yielded the same information?

QUESTIONS FOR THE RECORD
Senate Judiciary Committee
"Continued Oversight of the Foreign Intelligence Surveillance Act"
October 2, 2013
Senator Amy Klobuchar

Questions for General Keith B. Alexander

As discussed at the hearing, in mid-August 2013, the media began reporting about an internal audit from May 2012, which found that the NSA violated privacy rules numerous times. This audit was not brought to the Senate Judiciary Committee's attention at the July 31, 2013 hearing on FISA surveillance programs.

- Can you describe how the results of internal audits or investigations of the Intelligence Community, and the NSA in particular, are communicated to Congress or the public?

- Will you consider disseminating the results of internal audits or investigations more widely to Congress and the public in order to help improve the transparency of Intelligence Community activities linked to bulk collection?

QUESTIONS FOR THE RECORD
Senate Judiciary Committee
"Continued Oversight of the Foreign Intelligence Surveillance Act"
October 2, 2013
Senator Amy Klobuchar

Questions for the Honorable James R. Clapper

As discussed at the hearing, in mid-August 2013, the media began reporting about an internal audit from May 2012, which found that the NSA violated privacy rules numerous times. This audit was not brought to the Senate Judiciary Committee's attention at the July 31, 2013 hearing on FISA surveillance programs.

- Can you describe how the results of internal audits or investigations of the Intelligence Community, and the NSA in particular, are communicated to Congress or the public?

- Will you consider disseminating the results of internal audits or investigations more widely to Congress and the public in order to help improve the transparency of Intelligence Community activities linked to bulk collection?

QUESTIONS FOR THE RECORD
Senate Judiciary Committee
"Continued Oversight of the Foreign Intelligence Surveillance Act"
October 2, 2013
Senator Amy Klobuchar

Question for Edward Felten

I am very interested in your recommendation that the FISC should have greater in-house technological expertise to assess the government's bulk collection and surveillance requests. I'd like to ask you to flesh this out a bit more.

- How would you recommend working technology experts into the current FISC process?

QUESTIONS FOR THE RECORD – Chairman Leahy
10/2/13 FISA Hearing

Questions for NSA Director Alexander

1. During the hearing, you disagreed with the *New York Times'* characterization that the NSA has been analyzing social networks, including those of Americans, using communications metadata as well as other records. While you clarified that much of this analysis is done on foreign targets, it remains unclear how extensively the government is analyzing and chaining communications and other data involving U.S. persons.

   a. Please provide a detailed description of how this program operates and a copy of the Supplemental Procedures and Guidelines for Governing Metadata Analysis that you referenced in your testimony.
   b. Specify the types of data that are used and from whom they are obtained.
   c. Specify the particular rules that apply to the use of data involving U.S. persons and queries focused on U.S. persons.
   d. Under what legal authority or authorities is this analysis being conducted?
   e. Is the Foreign Intelligence Surveillance Court aware of this social network analysis, and has it approved the practice?
   f. What oversight is conducted of this program, and by whom?

2. You testified that in 2010 and 2011 the NSA received samples of "locational information" in order to test the ability of NSA systems to handle the data format. While you noted that the project ended without any actual analysis of that data, you also indicated that acquiring this type of information might be a future requirement to keep our country safe.

   a. What types of locational data did the NSA acquire in 2010 and 2011?
   b. Was the locational data of U.S. persons acquired during this test?
   c. Under what legal authority was this test conducted?
   d. What was the result of this test project?
   e. What happened to the sample location data following the conclusion of the test?
   f. How and when were the Intelligence and Judiciary Committees notified when this project was initiated?
   g. The statement released by the NSA stated that Congress would be notified if locational data were to be obtained in the future. Please confirm that the Senate and House Judiciary Committees, in particular, will be notified.

3. In Judge Bates' October 2011 FISA Court opinion, he described so-called "about" collection under Section 702 of FISA, in which communications are acquired that are not to or from a target but rather contain a reference to the name of the tasked account. Have you conducted analysis of the effectiveness of this type of collection? If so, please provide the following:

a. An explanation of the instances in which obtaining "about" communications has proven to be a uniquely valuable tool;
b. The number of terrorist plots that have been thwarted as a result of "about" collection; and
c. The number of terrorist plots with a domestic nexus that have been thwarted by the use of "about" collection.

4. On October 14, the *Washington Post* reported that the NSA is harvesting hundreds of millions of contact lists and inboxes from e-mail and instant messaging accounts around the world, including many belonging to American citizens. In relation to this program, please answer the following questions:

a. Under what legal authority is the NSA collecting these contact lists and inboxes?
b. What legal standard are analysts required to meet in order to query or disseminate this information?
c. When did this collection program begin and how many e-mail and instant messaging contact lists and inboxes have been acquired under this program?
d. Please provide an estimate of the number of Americans who have had their contact lists and/or inboxes collected under this program.
e. Please explain what the NSA does with the contact lists and inboxes once they are collected.
f. Has the NSA ever acquired the contents of any communications under this collection program?
g. What safeguards are in place to protect the privacy rights of Americans?
h. Is the Foreign Intelligence Surveillance Court aware of this collection program, and has it approved such collection?
i. What oversight is conducted of this program, and by whom?

QUESTIONS FOR THE RECORD – Chairman Leahy
10/2/13 FISA Hearing

Questions for DNI Clapper

1. I appreciate the efforts of the administration to be more transparent by declassifying several Foreign Intelligence Surveillance Court opinions about Section 215.
   a. How many Foreign Intelligence Surveillance Court opinions containing significant legal interpretations relating to Section 215 of the USA PATRIOT Act remain classified?
   b. Will you commit to declassifying, with appropriate redactions to protect national security, all remaining Foreign Intelligence Surveillance Court opinions containing significant legal interpretations relating to Section 215 of the USA PATRIOT Act?

2. As Congress considers reforms to surveillance authorities, will you commit to declassifying, with appropriate redactions to protect national security, additional material from the Department of Justice Inspector General reports on Section 215, the National Security Letter authority, and exigent letters?

3. At a hearing of the Senate Select Committee on Intelligence on September 26, 2013, Senator Udall asked you if you had a position on declassification of the full history of the bulk collection program. You said you would consider this. Have you come to a decision about declassifying that history?

4. Which FISA authority does the Intelligence Community currently rely on to obtain the location data of U.S. person targets? Has it previously relied on any other FISA authorities to obtain location data of U.S. persons?

5. Does any element of the Intelligence Community use National Security Letters to engage in bulk collection on a scale similar to the use of Section 215 for telephony metadata? Has any element of the Intelligence Community in the past used National Security Letters to engage in such bulk collection?

6. In Judge Bates' October 2011 FISA Court opinion, he describes so-called "about" collection under Section 702 of FISA, in which communications are acquired that are not to or from a target but rather contain a reference to the name of the tasked account. Have you conducted analysis of the effectiveness of this type of collection? If so, please explain in what instances obtaining "about" communications has proven to be an effective tool.

Hearing: "Continued Oversight of the Foreign Intelligence Surveillance Act"
Sen. Sheldon Whitehouse
Questions for the Record

Questions for The Honorable Keith B. Alexander, Director, National Security Agency

1. The sudden, unauthorized disclosure of classified information by Edward Snowden appeared to catch the intelligence community without a protocol for responding to such an eventuality. How have you revised your procedures since the Snowden incident to respond more effectively to sudden, unauthorized disclosures of classified information?

2. As the Snowden incident revealed, the Intelligence Community relies heavily on private contractors for a variety of functions. What ensures that the government's reliance on contractors is not so great that appropriate legal redress cannot be taken against contractors in cases of misconduct, and that defense and intelligence contractors are not, in effect, "too big to sue"?

3. While the bulk telephony metadata collection program under Section 215 of the USA PATRIOT Act appears to be legal and constitutional, the program is potentially susceptible to abuse. Robust oversight is critical to preventing and addressing such abuse. Please list all of the executive, legislative, and judicial oversight that reviews the program.

4. Please provide an unclassified, simple summary of the mitigation procedures that govern the bulk telephony metadata collection program.

5. Has the Foreign Intelligence Surveillance Court's review of the bulk telephony metadata program yet considered the Supreme Court case *United States v. Jones*, 132 S. Ct. 945 (2012), and particularly Justice Sotomayor's concurring opinion in *Jones*? Please share any relevant analysis by the FISC in an unclassified format.

Hearing: "Continued Oversight of the Foreign Intelligence Surveillance Act"
Sen. Sheldon Whitehouse
Questions for the Record

Questions for The Honorable James R. Clapper, Director of National Intelligence

1. The sudden, unauthorized disclosure of classified information by Edward Snowden appeared to catch the intelligence community without a protocol for responding to such an eventuality. How have you revised your procedures since the Snowden incident to respond more effectively to sudden, unauthorized disclosures of classified information?

2. As the Snowden incident revealed, the Intelligence Community relies heavily on private contractors for a variety of functions. What ensures that the government's reliance on contractors is not so great that appropriate legal redress cannot be taken against contractors in cases of misconduct, and that defense and intelligence contractors are not, in effect, "too big to sue"?

3. While the bulk telephony metadata collection program under Section 215 of the USA PATRIOT Act appears to be legal and constitutional, the program is potentially susceptible to abuse. Robust oversight is critical to preventing and addressing such abuse. Please list all of the executive, legislative, and judicial oversight that reviews the program.

4. Please provide an unclassified, simple summary of the mitigation procedures that govern the bulk telephony metadata collection program.

5. Has the Foreign Intelligence Surveillance Court's review of the bulk telephony metadata program yet considered the Supreme Court case *United States v. Jones*, 132 S. Ct. 945 (2012), and particularly Justice Sotomayor's concurring opinion in *Jones*? Please share any relevant analysis by the FISC in an unclassified format.

Questions for the Record
Senate Committee on the Judiciary Hearing on FISA
2 October 2013

QUESTIONS FOR THE RECORD – Chairman Leahy
10/2/13 FISA Hearing

Questions for NSA Director Alexander

1. During the hearing, you disagreed with the *New York Times'* characterization that the NSA has been analyzing social networks, including those of Americans, using communications metadata as well as other records. While you clarified that much of this analysis is done on foreign targets, it remains unclear how extensively the government is analyzing and chaining communications and other data involving U.S. persons.

   a. Please provide a detailed description of how this program operates and a copy of the Supplemental Procedures and Guidelines for Governing Metadata Analysis that you referenced in your testimony.
   b. Specify the types of data that are used and from whom they are obtained.
   c. Specify the particular rules that apply to the use of data involving U.S. persons and queries focused on U.S. persons.
   d. Under what legal authority or authorities is this analysis being conducted?
   e. Is the Foreign Intelligence Surveillance Court aware of this social network analysis, and has it approved the practice?
   f. What oversight is conducted of this program, and by whom?

NSA Response

a. Please provide a detailed description of how this program operates and a copy of the Supplemental Procedures and Guidelines for Governing Metadata Analysis that you referenced in your testimony.

CLASSIFIED RESPONSE OMITTED

b. Specify the types of data that are used and from whom they are obtained

NSA Response

CLASSIFIED RESPONSE OMITTED

c. Specify the particular rules that apply to the use of data involving U.S. persons and queries focused on U.S. persons.

NSA Response

The applicable rules are discussed in the answer to question 1(d) below.

d. Under what legal authority or authorities is this analysis being conducted?

NSA Response

CLASSIFIED RESPONSE OMITTED

The use and analysis of enrichment data acquired pursuant to Executive Order 12333 is also conducted pursuant to DoD Regulation 5240.1-R. Under the DoD regulation, the collection, retention, and dissemination of U.S. person information, such as that which might be included within address books and buddy lists, is subject to limitations, even if the information is publicly-available.

e. Is the Foreign Intelligence Surveillance Court aware of this social network analysis, and has it approved the practice?

NSA Response

CLASSIFIED RESPONSE OMITTED

f. What oversight is conducted of this program, and by whom?

NSA Response

Internal oversight of intelligence activities conducted pursuant to the general SIGINT authority provided in Section 1.7(c)(1) of Executive Order 12333 is performed by a number of NSA offices, to include the Office of the Inspector General and the Office of the General Counsel, as well as the Oversight and Compliance Office of the Signals Intelligence Directorate. The oversigbt measures include not only those pursuant to SPCMA but also the procedures outlined in the attached letter sent by NSA to the Department of Justice in 2006, when the Attorney General's approval of the procedures was requested. In addition to the terms of the letter, NSA requires analysts to identify any query known to concern a U.S. person, and such queries are subject to additional oversight to ensure that there is a valid foreign intelligence purpose for them. In addition to multiple levels of internal oversight of the SPCMA and data enrichment activities, these activities are subject to oversight by the Department of Defense IG, the Intelligence Community IG, the President's Intelligence Oversight Board and the Congress. In particular, any violation of the SPCMA procedures, like any other violation of procedures that govern NSA's handling of U.S. person information, are also covered in the quarterly intelligence oversight reports provided to the Assistant to the Secretary of Defense for Intelligence Oversight for onward reporting to the President's Intelligence Oversight Board. In addition, NSA provides an annual report to the Attorney General on (i) the kinds of information that NSA is collecting and processing as communications metadata; (ii) NSA's implementation of the SPCMA procedures; and (iii) any significant new legal or oversight issues that have arisen in connection with NSA's collection, processing or dissemination of communications metadata of U.S. persons.

2. You testified that in 2010 and 2011 the NSA received samples of "locational information" in order to test the ability of NSA systems to handle the data format. While you noted that the project ended without any actual analysis of that data, you also indicated that acquiring this type of information might be a future requirement to keep our country safe.

   a. What types of locational data did the NSA acquire in 2010 and 2011?
   b. Was the locational data of U.S. persons acquired during this test?
   c. Under what legal authority was this test conducted?
   d. What was the result of this test project?
   e. What happened to the sample location data following the conclusion of the test?
   f. How and when were the Intelligence and Judiciary Committees notified when this project was initiated?
   g. The statement released by the NSA stated that Congress would be notified if locational data were to be obtained in the future. Please confirm that the Senate and House Judiciary Committees, in particular, will be notified.

a. What types of locational data did the NSA acquire in 2010 and 2011?

NSA Response

CLASSIFIED RESPONSE OMITTED

The mobility data in the test files was kept separate from the operational dataflows. The test files were not ingested into the operational databases and were not accessible to NSA target analysts.

b. Was the locational data of U.S. persons acquired during this test?

NSA Response

CLASSIFIED RESPONSE OMITTED

c. Under what legal authority was this test conducted?

NSA Response

NSA obtained the test records pursuant to the Foreign Intelligence Surveillance Court orders in effect for the Section 215 authority at the time. NSA consulted with the Department of Justice (DoJ), which notified the Court, regarding this testing effort.

d. What was the result of this test project?

NSA Response

CLASSIFIED RESPONSE OMITTED

e. What happened to the sample location data following the conclusion of the test?

NSA Response

CLASSIFIED RESPONSE OMITTED

f. How and when were the Intelligence and Judiciary Committees notified when this project was initiated?

NSA Response

CLASSIFIED RESPONSE OMITTED

g. The statement released by the NSA stated that Congress would be notified if locational data were to be obtained in the future. Please confirm that the Senate and House Judiciary Committees, in particular, will be notified.

NSA Response

The current Primary Order requires NSA to obtain approval of the FISA Court before seeking to obtain location information in the future. As NSA has previously committed, the Senate and House Judiciary Committees would also be notified, as well as the Senate and House Intelligence Committees.

3. In Judge Bates' October 2011 FISA Court opinion, he described so-called "about" collection under Section 702 of FISA, in which communications are acquired that are not to or from a target but rather contain a reference to the name of the tasked account. Have you conducted analysis of the effectiveness of this type of collection? If so, please provide the following:

a. An explanation of the instances in which obtaining "about" communications has proven to be a uniquely valuable tool;
b. The number of terrorist plots that have been thwarted as a result of "about" collection; and
c. The number of terrorist plots with a domestic nexus that have been thwarted by the use of "about" collection.

NSA Response

NSA's authorities and capabilities work in complementary ways. The tools and methods NSA uses for tracking "use" of collected communications are based on targets and collection sources and not the specific ways in which individual communications are identified for collection from those sources. "About" communications provide unique information concerning NSA's foreign intelligence targets and provides a unique tool for target discovery and development purposes which concern analytic judgments, to include judgments about who might be involved in a terrorist plot. NSA does not specifically track the use of "about" communications and there is no reliable manner to determine how often the acquisition of such communications has played a role in thwarting a terrorist plot.

4. On October 14, the *Washington Post* reported that the NSA is harvesting hundreds of millions of contact lists and inboxes from e-mail and instant messaging accounts around the world, including many belonging to American citizens. In relation to this program, please answer the following questions:

    a. Under what legal authority is the NSA collecting these contact lists and inboxes?
    b. What legal standard are analysts required to meet in order to query or disseminate this information?
    c. When did this collection program begin and how many e-mail and instant messaging contact lists and inboxes have been acquired under this program?
    d. Please provide an estimate of the number of Americans who have had their contact lists and/or inboxes collected under this program.
    e. Please explain what the NSA does with the contact lists and inboxes once they are collected.
    f. Has the NSA ever acquired the contents of any communications under this collection program?
    g. What safeguards are in place to protect the privacy rights of Americans?
    h. Is the Foreign Intelligence Surveillance Court aware of this collection program, and has it approved such collection?
    i. What oversight is conducted of this program, and by whom?

    a. Under what legal authority is the NSA collecting these contact lists and inboxes?

NSA Response

CLASSIFIED RESPONSE OMITTED

b. What legal standard are analysts required to meet in order to query or disseminate this information?

NSA Response

CLASSIFIED RESPONSE OMITTED

c. When did this collection program begin and how many e-mail and instant messaging contact lists and inboxes have been acquired under this program?

NSA Response

CLASSIFIED RESPONSE OMITTED

d. Please provide an estimate of the number of Americans who have had their contact lists and/or inboxes collected under this program.

NSA Response

CLASSIFIED RESPONSE OMITTED

e. Please explain what the NSA does with the contact lists and inboxes once they are collected.

NSA Response

CLASSIFIED RESPONSE OMITTED

f. Has the NSA ever acquired the contents of any communications under this collection program?

NSA Response

CLASSIFIED RESPONSE OMITTED

g. What safeguards are in place to protect the privacy rights of Americans?

NSA Response

CLASSIFIED RESPONSE OMITTED

h. Is the Foreign Intelligence Surveillance Court aware of this collection program, and has it approved such collection?

NSA Response

CLASSIFIED RESPONSE OMITTED

i. What oversight is conducted of this program, and by whom?

NSA Response

CLASSIFIED RESPONSE OMITTED

October 2, 2013
Questions for the Record from Ranking Member Charles E. Grassley

General Keith Alexander, NSA Director

1. 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 accessed and 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? Please answer this question in an unclassified format, to the extent possible.

NSA Response

There are several internal and external safeguards in place to enable NSA's authorized use of the telephone metadata acquired under the Section 215 provision. Many of these safeguards are prescribed by the FISC's Primary Order and are also described in the attached opinions the FISC issued concerning the program on 29 August 2013 and 11 October 2013.

NSA employs a selector management tool that houses all Reasonable Articulable Suspicion (RAS)-approved selectors and their required nomination justification. The system also provides for the enforcement of the approval process, required by the FISC Order, that all RAS nominations are approved by one of the twenty-two officials named in accordance with the Order and that any nominated selector known to be used by a U.S. person is reviewed and approved by NSA's Office of General Counsel to ensure that the justification was not solely based on activities that are protected by the First Amendment to the Constitution.

Access controls prohibit query access by personnel who have not been appropriately and adequately trained or who do not have the proper credentials authorizing them to conduct queries of the acquired telephony metadata. NSA employs technical safeguards that allow only authorized personnel to query the BR metadata repository, for intelligence analysis purposes, using only selectors on the RAS-approved list (prohibiting queries of non-RAS approved selectors), and that allow queries to be conducted only out to the authorized three hops (again, prohibiting queries from continuing beyond the authorized third hop). These queries are then audited to assess their compliance with the Court's requirements. NSA audits these queries every 30 days.

The telephone metadata is subject to a 5-year retention limitation pursuant to the FISC Order.

In accordance with the FISC Order, NSA and DoJ meet quarterly for the purpose of assessing NSA's compliance with the Court's orders. DOJ audits all U.S. person RAS determinations from the previous quarter and a sampling of non-US. person RAS determinations from the previous quarter.

To safeguard against improper dissemination of information related to U.S persons obtained as a result of a query into the metadata, NSA relies on management controls, the training regimen required of the analyst to include an enhanced training course specifically on the requirements of handling data under this authority, and internal NSA policy. As it relates to this authority, prior to disseminating any U.S. person information outside NSA, an official holding one of the seven positions named within the Order must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

In accordance with the FISC Order, approximately every thirty days, NSA files with the Court a report that includes a discussion of NSA's application of the RAS standard and the number of instances since the preceding report in which NSA has shared, in any form, results from the queries of the telephony metadata, that contain U.S. person information, in any form, with anyone outside the NSA and includes an attestation that one of the officials authorized to approve such disseminations determined that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

All RAS determinations are documented. Intelligence analysis queries are audited, analysts are trained on the use of the data, and all BR metadata is tagged and only accessible by personnel with appropriate credentials. Here again, NSA relies heavily upon management controls, the training regimen required by NSA employees that includes enhanced training on the requirements of handling data under this authority, as well as internal NSA policy.

Executive Branch oversight of the BR FISA program includes the following practices for reporting instances of non-compliance and conducting oversight of the program:

- NSA reports instances of noncompliance to DoJ and ODNI. These reports include details about the non-compliance.
- DoJ and ODNI meet with NSA at least once during the authorization period (typically 90 days) to review NSA's processes and its assessment that only approved metadata is being acquired.
- NSA's Inspector General and Office of the Director of Compliance are assigned specific BR FISA oversight responsibilities by the Court.
- NSA consults with DoJ on all significant legal interpretations of the BR FISA authority.
- As noted above, DoJ reviews a sample of the selection terms approved to query the telephony metadata.

- NSA also provides an Intelligence Oversight Quarterly Report to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight. This report, which includes details about noncompliance incidents, is produced by the NSA Office of the Inspector General and the NSA Office of General Counsel, and signed by the NSA Inspector General, the NSA General Counsel, and NSA Director.

Judicial Branch oversight includes:

- The Foreign Intelligence Surveillance Court Rules of Procedure require the Government to report to the Court in writing any non-compliance with the Court's approvals or authorizations, including incidents of noncompliance with Court-approved minimization procedures or applicable law. The Government must include a description of the facts and circumstances of the non-compliance, any modifications the Government has made or proposes to make in its implementation of the affected authority, and how the Government intends to dispose of or treat any information obtained as a result of the non-compliance.
- NSA also provides regular 30 day reports to the FISC that describe its application of the RAS standard, its implementation, and the operation of an authorized automated query process (described below), and the number of disseminations of query results that contain U.S. person information made during the reporting period.
- NSA reports upon renewal any significant changes in the way NSA receives call detail records or changes to NSA's controls to receive, store, process, and disseminate BR metadata.
- The FISC must renew the authorization the BR FISA program every 90 days.

Legislative oversight includes:

- The National Security Act and FISA impose requirements to report certain incidents of noncompliance to the designated congressional oversight committees. These reports include details about the compliance incidents, and at a committee's request, NSA will provide detailed classified briefing(s) regarding the incident.
- ODNI and NSA also provide extensive briefings to the Congressional intelligence and judiciary committees on NSA's operation of the BR FISA bulk telephony metadata program.
- ODNI and NSA also provide Congress with written notifications regarding all significant developments in the program.
- The Department of Justice provides Congress with copies of all significant FISC opinions regarding the BR FISA program.

In addition, the BR FISA statutory provision requires the Attorney General, on an annual basis, to report to the intelligence and judiciary committees of the Congress (50 U.S.C. 1862):

- The total number of BR FISA applications;
- The total number of BR FISA orders either granted, modified, or denied; and

- The total number of orders either granted, modified, or denied that concerned library circulation records, firearms sales records, tax return records, educational records, or medical records that would identify a person.

NSA takes appropriate remedial action with respect to any compliance incident. NSA personnel may be subject to disciplinary action in connection with compliance matters whenever appropriate. There have been no identified instances of willful noncompliance in connection with the BR FISA program.

Hearing: "Continued Oversight of the Foreign Intelligence Surveillance Act"
Sen. Sheldon Whitehouse
Questions for the Record

Questions for The Honorable Keith B. Alexander, Director, National Security Agency

1. The sudden, unauthorized disclosure of classified information by Edward Snowden appeared to catch the intelligence community without a protocol for responding to such an eventuality. How have you revised your procedures since the Snowden incident to respond more effectively to sudden, unauthorized disclosures of classified information?

   Response

   An interagency response will be provided under separate cover.

2. As the Snowden incident revealed, the Intelligence Community relies heavily on private contractors for a variety of functions. What ensures that the government's reliance on contractors is not so great that appropriate legal redress cannot be taken against contractors in cases of misconduct, and that defense and intelligence contractors are not, in effect, "too big to sue"?

   Response

   An interagency response will be provided under separate cover.

3. While the bulk telephony metadata collection program under Section 215 of the USA PATRIOT Act appears to be legal and constitutional, the program is potentially susceptible to abuse. Robust oversight is critical to preventing and addressing such abuse. Please list all of the executive, legislative, and judicial oversight that reviews the program.

   Response

   An interagency response will be provided under separate cover.

   NSA Response

There are several internal and external safeguards in place to enable NSA's authorized use of the telephone metadata acquired under the Section 215 provision. Many of these safeguards are prescribed by the FISC's Primary Order and are also described in the attached opinions the FISC issued concerning the program on 29 August 2013 and 11 October 2013.

NSA employs a selector management tool that houses all Reasonable Articulable Suspicion (RAS)-approved selectors and their required nomination justification. The system also provides for the enforcement of the approval process, required by the FISC Order, that all RAS

nominations are approved by one of the twenty-two officials named in accordance with the Order and that any nominated selector known to be used by a U.S. person is reviewed and approved by NSA's Office of General Counsel to ensure that the justification was not solely based on activities that are protected by the First Amendment to the Constitution.

Access controls prohibit query access by personnel who have not been appropriately and adequately trained or who do not have the proper credentials authorizing them to conduct queries of the acquired telephony metadata. NSA employs technical safeguards that allow only authorized personnel to query the BR metadata repository, for intelligence analysis purposes, using only selectors on the RAS-approved list (prohibiting queries of non-RAS approved selectors), and that allow queries to be conducted only out to the authorized three hops (again, prohibiting queries from continuing beyond the authorized third hop). These queries are then audited to assess their compliance with the Court's requirements. NSA audits these queries every 30 days.

The telephone metadata is housed in a segregated database and the metadata is subject to a 5-year retention limitation pursuant to the FISC Order.

In accordance with the FISC Order, NSA and DoJ meet quarterly for the purpose of assessing NSA's compliance with the Court's orders. DOJ audits all U.S. person RAS determinations from the previous quarter and a sampling of non-US. person RAS determinations from the previous quarter.

To safeguard against improper dissemination of information related to U.S persons obtained as a result of a query into the metadata, NSA relies on management controls, the training regimen required of the analyst to include an enhanced training course specifically on the requirements of handling data under this authority, and internal NSA policy. As it relates to this authority, prior to disseminating any U.S. person information outside NSA, an official holding one of the seven positions named within the Order must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

In accordance with the FISC Order, approximately every thirty days, NSA files with the Court a report that includes a discussion of NSA's application of the RAS standard and the number of instances since the preceding report in which NSA has shared, in any form, results from the queries of the telephony metadata, that contain U.S. person information, in any form, with anyone outside the NSA and includes an attestation that one of the officials authorized to approve such disseminations determined that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

All RAS determinations are documented. Intelligence analysis queries are audited, analysts are trained on the use of the data, and all BR metadata is tagged and only accessible by personnel with appropriate credentials. Here again, NSA relies heavily upon management controls, the training regimen required by NSA employees that includes enhanced training on the requirements of handling data under this authority, as well as internal NSA policy.

Executive Branch oversight of the BR FISA program includes the following practices for reporting instances of non-compliance and conducting oversight of the program:

- NSA reports instances of noncompliance to DoJ and ODNI. These reports include details about the non-compliance.
- DoJ and ODNI meet with NSA at least once during the authorization period (typically 90 days) to review NSA's processes and its assessment that only approved metadata is being acquired.
- NSA's Inspector General and Office of the Director of Compliance are assigned specific BR FISA oversight responsibilities by the Court.
- NSA consults with DoJ on all significant legal interpretations of the BR FISA authority.
- As noted above, DoJ reviews a sample of the selection terms approved to query the telephony metadata.
- NSA also provides an Intelligence Oversight Quarterly Report to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight. This report, which includes details about noncompliance incidents, is produced by the NSA Office of the Inspector General and the NSA Office of General Counsel, and signed by the NSA Inspector General, the NSA General Counsel, and NSA Director.

Judicial Branch oversight includes:

- The Foreign Intelligence Surveillance Court Rules of Procedure require the Government to report to the Court in writing any non-compliance with the Court's approvals or authorizations, including incidents of noncompliance with Court-approved minimization procedures or applicable law. The Government must include a description of the facts and circumstances of the non-compliance, any modifications the Government has made or proposes to make in its implementation of the affected authority, and how the Government intends to dispose of or treat any information obtained as a result of the non-compliance.
- NSA also provides regular 30 day reports to the FISC that describe its application of the RAS standard, its implementation, and the operation of an authorized automated query process (described below), and the number of disseminations of query results that contain U.S. person information made during the reporting period.
- NSA reports upon renewal any significant changes in the way NSA receives call detail records or changes to NSA's controls to receive, store, process, and disseminate BR metadata.
- The FISC must reauthorize the BR FISA program every 90 days.

Legislative oversight includes:

- The National Security Act and FISA impose requirements to report certain incidents of noncompliance to the designated congressional oversight committees. These

reports include details about the compliance incidents, and at a committee's request, NSA will provide detailed classified briefing(s) regarding the incident.

- ODNI and NSA also provide extensive briefings to the Congressional intelligence and judiciary committees on NSA's operation of the BR FISA bulk telephony metadata program.
- ODNI and NSA also provide Congress with written notifications regarding all significant developments in the program.
- The Department of Justice provides Congress with copies of all significant FISC opinions regarding the BR FISA program.

In addition, the BR FISA statutory provision requires the Attorney General, on an annual basis, to report to the intelligence and judiciary committees of the Congress (50 U.S.C. 1862):

- The total number of BR FISA applications;
- The total number of BR FISA orders either granted, modified, or denied; and
- The total number of orders either granted, modified, or denied that concerned library circulation records, firearms sales records, tax return records, educational records, or medical records that would identify a person.

NSA takes appropriate remedial action with respect to any compliance incident. NSA personnel may be subject to disciplinary action in connection with compliance matters whenever appropriate. There have been no identified instances of willful noncompliance in connection with the BR FISA program.

4. Please provide an unclassified, simple summary of the mitigation procedures that govern the bulk telephony metadata collection program.

NSA Response

Query Terms: Under the FISC orders authorizing the collection, authorized analytic queries may begin only with selection term that is associated with one of the FISC-approved foreign terrorist organizations. An identifier used to commence a query of the data is referred to as a "seed." Specifically, under Court-approved rules applicable to the program, there must be a "reasonable, articulable suspicion" that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. No more than twenty-two designated NSA officials can make a finding that there is "reasonable, articulable suspicion" that a seed identifier proposed for query is associated with a specific foreign terrorist organization. Further, when the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. NSA's Office of the General Counsel must review and approve any such findings for selection terms believed to be used by U.S. persons.

Query results: Raw results of authorized queries are available only to those analysts trained in the restrictions on the handling and dissemination of the metadata. Query results can be further analyzed only for valid foreign intelligence purposes.

Retention: The raw metadata collected as part of this program is destroyed no later than five years (60 months) after its initial collection.

Dissemination: NSA may disseminate any results from queries of the metadata subject to its generally applicable dissemination requirements governing its E.O. 12333 collection. Additionally, prior to disseminating any U.S. person information outside NSA, one of seven specified NSA officials must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. More detailed descriptions of the Court-ordered minimization procedures applicable to this program may be found in the recently declassified and published Primary Orders issued by the FISC. See http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

5. Has the Foreign Intelligence Surveillance Court's review of the bulk telephony metadata program yet considered the Supreme Court case *United States v. Jones*, 132 S. Ct. 945 (2012), and particularly Justice Sotomayor's concurring opinion in *Jones*? Please share any relevant analysis by the FISC in an unclassified format.

NSA Response

On 11 October 2013, Judge McLaughlin of the FISC issued a Memorandum Opinion, which has been declassified and published by the FISC, explaining her decision to grant the Government's Application renewing the program. Judge McLaughlin addressed the *Jones* decision on pages 4–6 of the Memorandum Opinion. A copy of the Memorandum Opinion is attached and also is available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf.

QUESTIONS FOR THE RECORD
Senate Judiciary Committee
"Continued Oversight of the Foreign Intelligence Surveillance Act"
October 2, 2013
Senator Amy Klobuchar

Questions for General Keith B. Alexander

As discussed at the hearing, in mid-August 2013, the media began reporting about an internal audit from May 2012, which found that the NSA violated privacy rules numerous times. This audit was not brought to the Senate Judiciary Committee's attention at the July 31, 2013 hearing on FISA surveillance programs.

- Can you describe how the results of internal audits or investigations of the Intelligence Community, and the NSA in particular, are communicated to Congress or the public?

NSA Response

NSA conducts a number of internal audits, inspections, compliance reviews, and incident reporting, both as part of its internal oversight and compliance programs and to support specific external reporting requirements, as mandated by law and policy.

The referenced document, "NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January-31 March 2012 – EXECUTIVE SUMMARY, is used internally at NSA to improve its oversight and compliance programs. Information contained in the document (and other internal NSA documents regarding oversight and compliance) forms the basis of a number of submissions to Congress, including but not limited to:

1. Semi-Annual Report to Congress – As required by Section 5 of the IG Act of 1978 (as amended), the NSA Office of the Inspector General (OIG) prepares and sends a *Semi-annual Report to Congress*, which includes descriptions of reports produced by the OIG during the reporting period and significant outstanding recommendations from previous reports. The report is furnished to the Director of NSA, who provides the report, along with his own statutorily required report, to the Chairman and Vice Chairman of the SSCI and to the Chairman and Ranking Member of the HPSCI.

2. Annual FAA §702 Report – The NSA OIG prepares an annual report to Congress on compliance with the targeting and minimization procedures of Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA §702).

- The report is due to Congress by 31 December of each year. It has been prepared and submitted yearly since the FY 2009 report. This report is provided to the Chairman (and Vice Chairman where applicable) and Ranking Members of the House and Senate Intelligence and Judiciary Committees.

3. Other – NSA's Office of the Inspector General responds to Committee requests for information, most recently by a letter date 11 September 2013 to Chairman Leahy and Ranking Member Grassley.

- Will you consider disseminating the results of internal audits or investigations more widely to Congress and the public in order to help improve the transparency of Intelligence Community activities linked to bulk collection?

NSA Response

NSA, along with ODNI and DoJ, will continue our efforts to promote greater transparency while carefully protecting information that we cannot responsibly release because of national security concerns, and we will work with the Intelligence and Judiciary Committees if additional information is required beyond what is already being furnished.

Senator Mazie K. Hirono

Questions for the Record following hearing on October 2, 2013 entitled:
"Continued Oversight of the Foreign Intelligence Surveillance Act"

The Honorable Keith B. Alexander, Director, National Security Agency

1. At the hearing I asked if the Intelligence Community and the NSA specifically are focusing on evolving the technology of privacy safeguards as the surveillance technology is clearly evolving.

    a. Can you give examples of what kinds of new technical capacity to protect privacy we can expect to benefit from in the future?
    b. Is the NSA working to develop narrower, more targeted collection or is all the research and development focused on expanding access to information?
    c. Can you give examples of what kinds of new technical capacity to protect privacy we can expect to benefit from in the future?

NSA Response

CLASSIFIED RESPONSE OMITTED

NSA's internal compliance program, spearheaded by the Office of the Director of Compliance (ODOC), includes formation of a novel rules architecture designed to accurately reflect the complete set of rules protecting privacy. This rules architecture is an essential component of NSA's Smart Data initiatives, as it enables systems to apply critical data tags that discern the specific authorization under which NSA collected or acquired specific data. That information informs access controls which prevent an individual from seeing data for which they have not been trained and/or do not have a mission need.

ODOC developed and manages Verification of Accuracy procedures to provide an increased level of confidence that factual representations are based on an ongoing shared understanding among operational, technical, legal, policy, and compliance officials. NSA has applied them to authority-related documentation, especially when describing complex technical matters to NSA's overseers.

NSA also leverages a number of technology solutions to ultimately assist and audit analysts as they perform their job. For example, NSA uses an access control architecture that prevents personnel from accessing collected data unless they have the required credentials and training. NSA also uses appropriate mission sponsorship and an accountability system that provides a repository of queries to NSA data and the ability to perform post-query auditing. NSA continues to explore new ways to develop and enhance its use of technology to support and enforce privacy protections for its SIGINT and other mission data.

2. Is the NSA working to develop narrower, more targeted collection or is all the research and development focused on expanding access to information?

NSA Response

CLASSIFIED RESPONSE OMITTED

3. It has been reported that certain data collected by the NSA are shared with domestic law enforcement agencies.

   a. What is the legal authority that allows the NSA to give Section 215 of the Patriot Act and FISA Amendments Act Section 702 data to other agencies such as the FBI, DEA, or other law enforcement agencies?
   b. Does such sharing require the demonstration of "probable cause" before such data are shared?
   c. Is the FISA court involved in such approvals on a case-by-case basis?
   d. What is the legal authority that allows the NSA to give Section 215 of the Patriot Act and FISA Amendments Act Section 702 data to other agencies such as the FBI, DEA, or other law enforcement agencies?

NSA Response

NSA disseminates foreign intelligence information derived from both lawful queries of Section 215 data and FAA Section 702 targeting to intelligence components of law enforcement agencies, including the intelligence components of the FBI, in response to approved foreign intelligence requirements. The Foreign Intelligence Surveillance Act also requires minimization procedures to include "procedures that allow for the retention and dissemination of information that is evidence of a crime . . . and that is to be retained or disseminated for law enforcement purposes (section 101 of the FISA). Section 106 of the FISA also sets forth specific requirements that are applicable to law enforcement use of certain types of FISA collection.

Section 215

The legal authority that allows NSA to disseminate information derived from lawful queries of Section 215 data is found within the applicable orders of the FISC. The FISC's Primary Order permits NSA to disseminate any results from queries of the Section 215 metadata subject to the minimization and dissemination requirements and procedures of United States Signals Intelligence Directive SP0018 (USSID 18). The Primary Order also requires that, prior to disseminating any U.S. person information outside NSA, one of seven specified NSA officials must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. Certain disseminations are not subject to the foregoing requirement. The Primary Order states that "Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch personnel (1) in order to enable them to

determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions."

NSA disseminates information derived from queries of Section 215 data for counterterrorism intelligence purposes, not law enforcement purposes. Apart from the FBI, which has a counterterrorism intelligence mission, NSA does not as a matter of practice disseminate Section 215 results directly to any agencies with a law enforcement mission, including the DEA.

FAA Section 702

FAA Section 702 provides for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. NSA processes FAA Section 702 acquired data in accordance with FISA Court-reviewed minimization procedures and disseminates foreign intelligence information in accordance with the standards set forth in those procedures to recipients who require the information in the performance of official duties.

The legal authority that allows NSA to disseminate information derived from FAA Section 702 targeting is found within the minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, and approved by the FISA Court. See 50 U.S.C. § 1881a(e). These procedures authorize NSA to disseminate 702-acquired information not concerning any U.S. persons in accordance with other applicable law, regulation and policy. The procedures impose stringent requirements for the dissemination of communications of or concerning a U.S. person; such communications may be disseminated only if certain conditions are satisfied (e.g., a report containing the identity of a U.S. person may be disseminated if the identity is necessary to understand foreign intelligence information or assess its importance.) Foreign intelligence includes information concerning international terrorist activities, and other hostile activities directed against the U.S. by foreign powers, entities, persons and their agents. While there are numerous foreign intelligence topics which are of interest both to the foreign intelligence and law enforcement communities, NSA's core mission is to disseminate information for the purpose of advancing national security interests not criminal prosecutions. The Attorney General-adopted and FISA Court-approved minimization procedures applicable to NSA's FAA Section 702 collection separately authorize the retention and dissemination to appropriate law enforcement authorities of information that is reasonably believed to contain evidence of a crime.

Other authorities separately require NSA to report to DoJ information relating to potential crimes. For example, Section 1.7(a) of Executive Order 12333 requires NSA to "report to the Attorney General possible violations of the federal criminal laws by employees and of specified federal criminal laws by any other person . . . as specified in [agreed upon] procedures."

a. Does such sharing require the demonstration of "probable cause" before such data are shared?

NSA Response

NSA does not need to demonstrate "probable cause" prior to disseminating the results of either a lawful Section 215 query or FAA Section 702 targeting, but rather must comply with the requirements listed above in the answer to Question 2(a). Any recipient agency may use the disseminated information as permitted by its own legal authorities.

b. Is the FISA court involved in such approvals on a case-by-case basis?

NSA Response

Section 215

The FISA Court does not approve disseminations of Section 215 data on a case-by-case basis. The FISA Court receives a monthly report from NSA that includes a list of all disseminations, in any form, of U.S. person information that occurred within the period covered by the report. This list includes the date of the dissemination, the recipient(s) of the dissemination, and the form of the dissemination (e.g., formal intelligence report, e-mail, verbal communication).

FAA Section 702

The FISA Court does not approve disseminations of FAA Section 702 data on a case-by-case basis. All disseminations of FAA section 702 data are available for review by DoJ and ODNI, whose representatives conduct oversight of NSA's exercise of the authority under FAA section 702 approximately once every 60 days. DoJ and ODNI review disseminations to ensure that NSA complies with the applicable minimization procedures, including any disseminations regarding criminal activity.

4. At the hearing I asked if PRISM is the only intelligence program NSA runs under FISA Section 702 and what other programs are run under sections 215 and 702.

   a. Please provide a complete list of the programs and their purposes that are operated by the NSA under the authorities provided by sections 215 and 702?

NSA Response

CLASSIFIED RESPONSE OMITTED

5. In conducting the programs under Sections 215 and 702 authorities, could less intrusive methods of collection have yielded the same information?

NSA Response

CLASSIFIED RESPONSE OMITTED

6. At the hearing several questions were asked related to the recent disclosure by the NSA Inspector General that 12 instances of intentional misuse of signals intelligence authorities of the Director of the National Security Agency.

    a. You indicated that "highlighting the punishments that go along with this" type of misuse should help prevent future instances of this type of misuse. Do you believe that increased criminal penalties for this type of privacy violation by intelligence analysts would help with deterrence?

NSA Response

It is difficult to predict whether increased criminal penalties for intentional violations of SIGINT authorities would help to deter the kinds of misuse reported by NSA's Inspector General. The small number of reported incidents suggests that existing remedies may be sufficient to deter unlawful conduct for the vast majority of the workforce.

United States Senate

Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

on October 2, 2013

Responses to Questions for the Record

submitted October 29, 2013

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

Senate Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Questions for the Record from Ranking Member Charles E. Grassley

1. **As this Committee considers changes to the FISC process, including the possibility of creating some kind of independent advocate to appear before the Court, what important operational considerations would you urge the Committee to consider?**

There are important operational considerations that come into play with respect to the proposals to create an independent advocate to appear before the Court. With respect to consideration of adding adversarial process before a request for surveillance, physical search or foreign intelligence acquisition is granted and conducted, this additional process could delay important foreign intelligence gathering. Bringing an outside advocate up-to-speed would take time. Particularly if the special advocate is an entity outside the existing interagency group of Intelligence Community and Department of Justice personnel involved in preparing requests to the Foreign Intelligence Surveillance Court (FISC), then the special advocate would have to request documents, briefings, and any additional information it requires in order to develop an informed view and prepare its presentation to the FISC. In order to be effective, the special advocate would likely need to continually be kept up-to-date regarding the technologies involved in collection, as well as targeting and minimization rules and guidelines. Creating a special advocate may turn out to be far more extensive than simply appointing an outside or inside lawyer to challenge government proposals: it could potentially mean creating an entire new office of lawyers, paralegals, support, security personnel and facilities accommodations to support the advocate's work.

In addition to the time this would add to the FISC's consideration of the collection request, this process would also necessarily take Intelligence Community personnel, such as NSA operators, analysts, oversight personnel and attorneys off-mission because it is often these same personnel who would need to be involved in informing the special advocate. These Intelligence Community operators and experts are likely already involved in providing extensive briefings and information to the existing oversight personnel at the Department of Justice, the Office of the Director of National Intelligence, and Congress.

2. **What would be the effect of a change in the law that would require prosecutors to obtain a search warrant in order to obtain materials, such as phone records, that are in the possession of third parties, instead of obtaining them through a subpoena?**

A change in the law imposing a warrant requirement for the production of records would bring criminal prosecutions and investigations to a screeching halt. It has long been established under existing Supreme Court precedent that records voluntarily turned over to a third party are not subject to an expectation of privacy and therefore law enforcement authorities do not need to secure a warrant to obtain them. Every day, criminal prosecutors and investigators use legal process such as grand jury subpoenas and administrative subpoenas to obtain records relevant to investigations across the wide range of criminal activity. In addition, third party records are also a daily part of civil proceedings such as document requests in civil litigation and administrative inquiries.

3. **Why shouldn't there be specific criminal sanctions against those who intentionally or knowingly misuse the phone metadata that is collected?**

As the NSA Inspector General's letter to the Ranking Member dated September 11, 2013 provides, there have been 12 instances of NSA personnel improperly misusing signals intelligence information maintained by NSA since January 1, 2003. It does not appear, based on the letter, that any of those instances pertain to information acquired pursuant to FISA. Therefore, the current public record does not suggest that NSA personnel have misused the phone metadata collected pursuant to Section 215 of the USA Patriot Act, calling in to question the need for any such sanction in the law. In my view, the types of incidents that did occur as stated in the Inspector General's letter are best handled administratively, through re-training, discipline or termination, depending on the facts and circumstances of the particular case, similar to the way that professional responsibility matters in other contexts are handled across Executive Branch agencies.

"Continued Oversight of the Foreign Intelligence Surveillance Act" Hearing

Senator Franken Questions for the Record

1. **Professor CORDERO, in your written testimony you criticized what you called, quote, "the ad hoc nature of the recent government declassification releases." You said you thought that these disclosures weren't helping the Intelligence Community as much as they might think. And you suggested that Congress could amend the reporting provisions in FISA to require additional public information at regular intervals. What specific information do you think these reports should include?**

A key area that would benefit from further attention is expanding the quality of information publicly available regarding the oversight and compliance process of surveillance activities under FISA. In August 2013, the Office of the Director of National Intelligence released a declassified version of the Attorney General and Director of National Intelligence's joint compliance assessment concerning acquisition under Section 702 of FISA. This document contained valuable information regarding how the oversight and compliance process takes place, and the results of the compliance reviews. However, this was also a somewhat heavily redacted document. It would be more useful to the public, as well as to Members of Congress beyond the Intelligence and Judiciary Committees, to have a summary, written-for-release version of the compliance assessment that is made publicly available at some regular interval, perhaps semi-annually, for example. In addition, it may better inform the public and broader Congress if there were, perhaps annually, a report that describes the oversight and compliance structure and activities for FISA activities beyond just section 702 collection.

A second area that would benefit from a regularized process is the release of FISC opinions. It may be helpful for Congress to work with the Department of Justice, the Office of the Director of National Intelligence and the Foreign Intelligence Surveillance Court (FISC) to evaluate options that are available to release FISC opinions that are in the public's interest. For example, should opinions be released as soon as they are issued and have undergone declassification review? Or, would it be better to have them released on a regular schedule, quarterly, for example? If releasing such opinions is going to happen on a more frequent basis going forward, then it may cut down on the novelty if they were released on a schedule, than on any given day which then generates several days' worth of hurried media attention directed at the Intelligence Community. A quarterly release of significant opinions could also, because it would be done in a deliberate way, provide opportunity for the FISC or Executive Branch to prepare a summary of the opinion(s). A summary document might be useful so that these releases have a broader distribution and better inform the public, beyond just the national security

legal or academic communities which are more likely to read and digest the full opinions themselves.

Third, I would suggest that there is value in working with the Department of Justice, FISC and the Intelligence Community to determine if there is additional information regarding the cooperation of the private sector that can be released publicly, in a way that is protective of national security information. The private sector has important interests in maintaining the trust of their customers and investors while complying with lawful requests from the government to assist in both criminal investigations and national security matters. While I would imagine that publicly disclosing numbers of persons or facilities targeted for collection under FISA would likely be of concern to the Intelligence Community, perhaps enabling release of information regarding numbers of requests broken down by federal, state, and local requests, and within the federal category, criminal investigatory versus national security requests, could be one path for discussions. Facilitating the companies' abilities to put the national security requests in a broader context of how it cooperates with national security and law enforcement, both within the United States and with foreign governments, is a worthwhile endeavor in order to maintain the important role that the private sector plays in supporting national security and law enforcement activities.

Senate Committee on the Judiciary

"Continued Oversight of the Foreign Intelligence Surveillance Act"

October 2, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Professor Laura Donohue

1. **Do you believe that in a typical criminal investigation, the government should be required to obtain a search warrant in order to obtain telephone records or other telephone metadata, even though these materials are in the possession of a third party? If so, how would that legal rule affect these investigations, in which prosecutors currently obtain such records with a grand jury subpoena?**

Response:

In *Smith v. Maryland*, the Supreme Court held that a pen register placed on a telephone line did not constitute a search within the meaning of the Fourth Amendment, because persons making phone calls do not have a reasonable expectation that the numbers they dial will remain private.[1] The key sentence from the decision centered on the customer's relationship with the telephone company. Namely "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[2] It is this sentence that spawned what has come to be known as "third party doctrine."[3]

The government relies on this opinion and the resultant third party doctrine to argue that, as in a typical criminal investigation, the bulk collection of U.S. persons' records in the telephony metadata program is constitutional. In its August 2013 *White Paper*, for instance, the Department of Justice suggests that a Section 215 order is not a search, because the Supreme Court "has expressly held [that] participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone

[1] Smith v. Maryland, 442 U.S. 735, 743-46 (1979). For more detailed discussion of the questions posed and further exposition of the points raised in this response, *see* Laura K. Donohue, *Written Testimony*, Senate Committee on the Judiciary, Continued Oversight of the Foreign Intelligence Surveillance Act, Oct. 2, 2013; and Laura K. Donohue, *Bulk Metadata Collection:*

[2] *Id.*

[3] *See also* U.S. v. Miller, 425 U.S. 435 (1976) (extending third party doctrine to banking records). *But see* U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010) (declining to extend third party doctrine to email stored with an Internet Service Provider on the grounds that customers have a reasonable expectation of privacy in their email).

numbers dialed."[4] In *ACLU v. Clapper*, the government again cites to the Court's reasoning in *Smith v. Maryland*, that, even if a subscriber harbored a subjective expectation that the numbers dialed would remain private, it would not be reasonable, since individuals have "no legitimate expectation of privacy in information" voluntarily turned over "to third parties."[5] The government suggests that because Courts subsequently followed *Smith* to find no reasonable expectation of privacy in email to/from and Internet protocol addressing information, as well as subscriber information, "*Smith* is fatal to Plaintiffs' claim that the collection of metadata records of their communications violates the Fourth Amendment."[6]

Judge Claire Eagan of the Foreign Intelligence Surveillance Court similarly relied almost exclusively on *Smith v. Maryland* in her recently-declassified August 2013 opinion: "The production of telephone service provide metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*."[7] In the normal course of business, she explained, telephone service providers maintain call detail records—records about which customers are aware. Customers therefore assume the risk that the telephone company will provide the information to the government.[8] That bulk collection of such information was involved was of no consequence: "[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[9]

The problem with these arguments is that they fail to consider the specific facts and circumstances that the Court faced in *Smith*, in which the police targeted one suspect for a limited period of time, for a specific purpose. They also fail to address critical ways in which the privacy interests impacted by the use of pen registers and their application to broad sectors of the population have changed as technology has advanced.[10] These factors distinguish the way in which third party doctrine works in the typical criminal case contemplated by Senator Grassley's question from the way in which the government is now collecting metadata under Section 215.

In 1976, Patricia McDonough was robbed in Baltimore, Maryland. After providing a description of the robber and a 1975 Monte Carlo she had seen near the scene of the crime to the police, she started

[4] Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act 2 (Aug. 9, 2013), at 19, *available at* https://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html.
[5] Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint, ACLU v. Clapper, 13 Civ. 3994,32-33 (quoting Smith v. Maryland, 432 U.S. 735 (1979) at 743-744).
[6] *Id.* at 33.
[7] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible things from [REDACTED], No. BR 13-109, slip op. at 6.. The only other case directly cited in her Fourth Amendment discussion appears to be a decision of the FISC court itself, with secondary citations. The details of the secret court opinion that she cites as precedent, however, are redacted.
[8] *Id.* at 7-8.
[9] *Id.* at 9.
[10] This failure underscores the absence of opposing counsel—an omission that would seem to be of particular import when assessing constitutional concerns.

receiving threatening and obscene phone calls from a man who identified himself as the robber. The caller at one point asked her to step out onto her front porch. When she did so, she saw the 1975 Monte Carlo driving slowly past her home. The police observed a car of the same description in her neighborhood. Tracing the license plate, police discovered that the car was registered to Michael Lee Smith.[11] The following day, the police asked the telephone company to install a pen register to trace the numbers called from Smith's home telephone. The company agreed, and that day Smith called McDonough's home. On the basis of this and other information, the police obtained a search warrant. Upon executing it, they found a telephone book in Smith's home, with the corner turned down to McDonough's name and number. In a six-man lineup, McDonough identified Smith as the person who robbed her.[12]

The police did not obtain a warrant prior to placing the pen register. But reasonable suspicion had been established that the target of the surveillance, Michael Lee Smith, had robbed, threatened, intimidated, and harassed Patricia McDonough. The police, accordingly, placed the pen register consistent with their reasonable suspicion that Smith was engaged in criminal wrongdoing.

This is the context of ordinary criminal investigations, which, when conducted consistent with *Smith v. Maryland*, do not require a search warrant for third party records. The telephony metadata program takes place in an entirely different context.

The National Security Agency ("NSA") is engaging in bulk collection *absent* any reasonable suspicion that individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, the Foreign Intelligence Surveillance Court ("FISC") acknowledges that almost *all* of the information thus obtained will bear *no* relationship whatsoever to criminal activity. The government, however, wants to place a pen register and trap and trace on everyone in the United States—essentially treating every U.S. citizen as though they are Michael Lee Smith.

In *Smith v. Maryland*, the police wanted only to record the numbers dialed from the suspect's telephone. At the time the case was decided, telephone companies were treated as utilities, with local telephone calls billed by the minute. What was unique about the technology involved in the pen register was that it could identify and record the numbers dialed from a telephone—a function that the phone company itself did not have. Its purpose was specific and limited.

In contrast, the bulk collection program collects the numbers dialed, the numbers who call a particular number, trunk information, and session times. Thus, while the police in 1979 were concerned with whether Michael Lee Smith was calling a particular number, the NSA metadata program now collects all

[11] 442 U.S. 735 (1979).
[12] *Id.*

numbers called—in the process obtaining significant amounts of information about individuals. Calls to a rape crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in *Smith*. This makes the amount of information available significantly different.

Trunk information, moreover, reveals not just the target of a particular telephone call, but where the callers (and receivers) are located. At the time of *Smith*, the police were only able to tell when someone was located at Smith's home. The telephone did not follow Smith around. What mobile technologies mean is that the police can now ascertain where people are located—creating a second layer of surveillance based simply on trunk identifier information. The bulk collection of records means that the government has the ability to do that for not just one person, but for the entire country.

Further characteristics distinguish the case. In *Smith v. Maryland*, the police sought the information for a short period. The bulk metadata collection program, in contrast, while continued at 90-day intervals, has been operating for seven years now—and, the NSA argues—should be a permanent part of the government surveillance program.

Perhaps the most important difference between the two situations lies in the realms of technology and social construction. The extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and complexity than the situation that existed at the time the Court heard arguments in *Smith*. Resultantly, the information that can be learned about not just individuals, but neighborhoods, political parties, Girl Scout troops—indeed, any social, political, or economic network—simply by the placement of a pen register or trap and trace, is light years ahead of what the Court contemplated in 1979.

The volume of communications being monitored further distinguishes the telephony metadata program from the question posed by Senator Grassley with regard to criminal investigations. Although the FISC orders that have been released and acknowledged by the government relate solely to one company (Verizon), officials have also acknowledged that the acquisition of telephony metadata extends to the largest telephone service providers in the United States: Verizon, AT&T, and Sprint.[13] This means that every time most U.S. citizens make a telephone call, the NSA is collecting the location, the number called, the time of the call, and the length of the conversation.[14] The numbers are worth noting. According to the *Wall Street Journal,* Verizon has 98.9 million wireless customers and 22.2 million

[13] Siobhan Gorman et al, *U.S. Collects Vast Data Trove*, WALL ST. J., June 7, 2013, at A1, *available at* http://on.wsj.com/11uDoue.
[14] *Id.*

landline customers; AT&T has 107.3 million wireless customers and 31.2 million landline customers, and Sprint has 55 million customers in total.[15] The program monitors hundreds of millions of people.

As for the type of information obtained, the FISC order requests that the telephone service providers give the government all "call detail information", a term that is defined by regulatory provision as:

> Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call.[16]

The FISC order further directs that the company provide "session identifying information", such as originating and terminating number, International Mobile Subscriber Identity number, and the International Mobile station Equipment Identity number. For most Americans, these numbers are connected to the identity of the user.[17] In addition, the FISC order directs the company to provide trunk identifier information. This data traces the route a telephone call takes, in the process establishing the location of the people taking part in the conversation.[18]

What can be done with this information is a significantly deeper intrusion on Americans' right to privacy than was at issue in *Smith*. It is easier to aggregate and analyze telephony metadata than content information precisely because it is structured.[19] Sophisticated data-mining and link-analysis programs can be applied this information, and it can do so faster, deeper, and more cheaply than in the past. Even the amount of data that can be retained for such analysis is of a radically different scale than was conceivable in 1979. From this information, the government can determine patters and relationships, such as personal details, habits, and behaviors that U.S. citizens had no intention or expectation of sharing.[20] The government can also obtain content.[21]

Even if U.S. citizens wanted to opt out of having this information collected, it would be virtually impossible to do so. There have been advances in encryption. But these technologies all revolve around content—not the metadata. Although some technologies are focused on metadata, these are not

---

[15] *Id.*
[16] 47 C.F.R. §64.2003 (2012). Senior intelligence officials have repeatedly asserted that, while they have the authority to collect GPS data, and have in the past, they are not currently doing so under the section 215 telephony metadata program. See, e.g., Statements of General Keith Alexander and Director of National Intelligence Clapper, Senate Judiciary Committee Hearing, Oct. 2, 2013; Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, WALL ST. J., June 16, 2013, http://onlwsj.com/13MnSsp.
[17] *Continued Oversight of the Foreign Intelligence Surveillance Act, Hearing Before the S. Comm. on the Judiciary*, 113 Cong. 3 (2013) (written testimony by Edward W. Felten).
[18] *Id.*
[19] *Id.*, at 4.
[20] *Id.*, at 5.
[21] *Id.*, at 8-9.

sufficiently advanced to allow for real-time communication.[22] The option is therefore not to use a telephone. The cost of doing so, however, would lean towards divesting oneself of a role in the modern world—impacting one's social relationships, employment, and ability to conduct financial and personal affairs.

Notably, all of these considerations are focused on telephony metadata. But the logic of the government's argument, as applied to metadata generally, has virtually no limit. One could equally argue that all financial flows, Internet usage, and email exchanges are relevant to ongoing terrorism investigations under Section 215. Almost all forms of metadata could be at stake.

In summary, the situation is fundamentally different than that which prevails with regard to third party data in ordinary criminal investigations, in the course of which, consistent with *Smith v. Maryland*, the government is not required to obtain a search warrant to obtain pen register information.

2. **There is some precedent in the law for the government to collect large categories of records in bulk that may be relevant to an investigation and then to later analyze those records to determine what specific items are in fact relevant. For example, in one case a federal appeals court upheld the use of a grand jury subpoena to acquire all money order applications from a particular location above a certain monetary threshold over a period of years. The court upheld the subpoena even though, inevitably, most of the records acquired would not be associated with any criminal activity. That case is *In Re Grand Jury Proceedings: Subpoena Duces Tecum*, 827 F.2d 301 (8th Cir. 1987). Obviously, bulk collection of metadata under Section 215 is much broader than that example. Are there other ways you would distinguish cases like this, in which this type of collection has been upheld as legal, from the government's acquisition of telephone metadata under Section 215, which you contend is illegal? Would you contend that cases such as the above are wrongly decided?**

[22] *Id.*, at 7-8.

Response:

In *In Re Grand Jury Proceedings*, the government served two grand jury subpoenas *duces tecum* on Western Union.[23] The first required production of monthly wire transactions at the Royalle Inn, Kansas City, Missouri, for a period of 13 months.[24] The second required production of Telegraphic Money Order Applications above $1,000 from the Royalle Inn, Kansas City, Missouri, between January 1984 and February 1986.[25] Western Union moved to quash the subpoenas on the ground that they amounted to an unreasonable search and seizure in violation of the fourth amendment.[26] The government responded by alleging that drug dealers in Kansas City were using Western Union to transmit money.[27]

The 8th Circuit Court of Appeals noted that it had previously held that Western Union customers have no privacy interest in Western Union records.[28] The Court cited the Supreme Court's holding in *United States v. Miller,* in which the Supreme Court determined, consistent with *Smith v. Maryland*, that bank customers do not enjoy a legitimate expectation of privacy in bank records subject to subpoena.[29]

The Court in *In re Grand Jury* specifically noted that the request at issue—namely, the production of records from Royalle Inn—was not as sweeping as subpoenas that the judiciary had found to be outside the bounds of acceptability. In *Federal Trade Commission v. American Tobacco Co.*, for instance, the Supreme Court refused to uphold the FTC's direction to two tobacco companies to produce letters and contracts.[30] The FTC had claimed "an unlimited right of access to the respondents' papers. . . relevant or irrelevant, in the hope that something [would] turn up."[31] The 8th circuit similarly declined to uphold a subpoena calling for an attorney's records over a ten-year period.[32]

The collection of all U.S. persons' telephony metadata is more properly considered in the same league as *FTC v. American Tobacco Co.* and *Schwimmer v. United States*, in which the Court recognized the overbroad use of government authority, as opposed to the more limited collection of information at issue in *In Re Grand Jury Proceedings.*

---

[23] *In Re Grand Jury Proceedings: Subpoena Duces Tecum*, 827 F.2d 301 (8th Cir. 1987).
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] United States v. Gross, 416 F.2d 1205, 1213 (8th Cir.), *cert. denied*, 397 U.S. 1013, 90 S.Ct. 1245, 25 L.Ed.2d 427 (1969); accord, Newfield v. Ryan, 91 F.2d 700, 703 (5th Cir.), *cert denied,* 302 U.S. 729, 58 S.Ct. 54, 82 L.Ed. 563 (1937).
[29] United States v. Miller, 425 U.S. 435, 440-443, 96 S. Ct. 1619, 48 L.Ed.2d 71 (1976).
[30] FTC v. American Tobacco Co., 264 U.S. 298, 305, 44 S.Ct. 336, 337, 68 L.Ed. 696 (1924).
[31] Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 207 n. 40, 66 S.Ct. at 505 n. 40 (quoting FTC, 264 U.S. at 305, 44 S.Ct. at 337).
[32] Schwimmer v. United States, 232 F.2d 855, 861-62 (8th Cir.), *cert denied*, 352 U.S. 833, 77 S.Ct. 48, 1 L.Ed. 2d 52 (1956).

Three points help to further distinguish the bulk collection of telephony metadata from ordinary use of subpoenas *duces tecum*: they are not to be used for fishing expeditions, they are specific, and they relate to past crimes. Remarkably, even FISC recognizes that the information collected as part of the bulk metadata program under Section 215 could not otherwise be obtained—including via subpoena *duces tecum*.

The government's contention, consistent with *United States v. R. Enters, Inc.*, is that to fall outside the statutory confines, there must be no reasonable possibility that the category of materials sought under Section 215 will produce relevant information.[33] The government is correct that *United States v. R. Enters, Inc.* gave a fair amount of latitude to the standard of relevancy applied to grand jury subpoenas. But the case also established important limits. "Grand juries," the Court wrote, "are not licensed to engage in arbitrary fishing expeditions."[34]

Subpoenas may not be used to try to obtain massive amounts of information whence evidence of wrongdoing—absent prior suspicion—can be derived.[35] A grand jury, for example, could not convene in Cedar Rapids, Iowa, and simply begin collecting telephony metadata, which it could subsequently mine to find evidence of criminal behavior. To the contrary, an investigator must have a reasonable suspicion that some document or communication exists, and that it is directly relevant to the investigation in question, in order for the Court to order its production.

The courts have used this logic to quash a subpoena *duces tecum* requiring that computer hard drives and floppy disks be produced. The request was overbroad because the materials "contain[ed] some data concededly irrelevant to the grand jury inquiry."[36] In that case, the government acknowledged that irrelevant material was included in the sweep.[37] Judge Michael Mukasey quashed the subpoena on the grounds that the government could narrow the documents requested prior to acquisition. He also rejected the claim that a broad sweep of information was justified by the breadth of the investigation underway: even an "expanded investigation" did "not justify a subpoena which encompassed documents "completely irrelevant to its scope."[38]

---

[33] *See also* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 587 (1993).
[34] United States v. R. Enterprises, Inc., 498 U.S. 29, 2992 (1991).
[35] *Id.*.
[36] In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12 (S.D.N.Y. 1994).
[37] *Id.* at 13.
[38] *Id.* (quotation marks omitted). *See also* Cessante v. City of Pontiac, No. CIV. A. 07-cv-15250, 2009 WL 973339, at *7 (E.D. Mich. Apr. 9, 2009) ("While some of the information sought may be relevant or lead to relevant information, the request for 'anything and everything' is overly broad and not narrowly tailored to meet the relevancy requirements of Fed. R. Civ. P. 26(b)."); Hale v. Henkel, 201 U.S. 43, 76-77 (1906) (finding a "*subpoena duces tecum*. . . far too sweeping in its terms to be regarded as reasonable" where it did not "require the production of a single contract, or of contracts with a particular corporation, or a limited number of documents, but all understandings, contracts, or correspondence between" a company and six others, over

Almost none of the telephony metadata collected under Section 215 is related to criminal activity. In Judge Reggie Walton's words, "Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.[39] The principle at work here was recognized by the Eastern District of New York: "While the standard of relevancy [as applied to subpoenas] is a liberal one, it is not so liberal as to allow a party 'to roam in shadow zones of relevancy and to explore matter which does not presently appear germane on the theory that it might conceivably become so.'"[40] A subpoena *duces tecum* may not be used to compel the production of records simply because at some point, in the future, they might become relevant.

In a world limited by the physical manifestation of evidence, practicality helped to cabin the scope of subpoenas. Technology may have changed what is possible in terms of the volume and nature of records that can be obtained and stored, and the level of insight that can be gleaned. But it does not invalidate the underlying principle. Subpoenas, even those issued by grand juries, may not be used to engage in fishing expeditions.

Grand jury investigations also are specific. That is, they represent investigations into particular individuals, or particular entities, in relation to which there is reasonable suspicion that some illegal behavior has occurred. The compelled production of records or items is thus limited by reference to the target of the investigation.

If a grand jury were, for instance, focused on the potentially criminal acts of the head of a crime family in Des Moines, absent reasonable suspicion of some sort of connection to the syndicate, it would not issue a subpoena for the telephone records of the Parent-Teacher's Association at Clark Elementary School in Sioux City.

In contrast, the Section 215 orders are broad and non-specific. That is, on the basis of no particular suspicion, all call records, the "vast majority" of which (according to FISC's own language) are of a purely local nature, are swept up by the NSA.[41]

Grand jury investigations are also targeted at current and prior criminal activity. The telephony metadata orders, in contrast, are both past and forward-looking, in that they anticipate the possibility of illegal

---

a multi-year period); Ealy v. Littlejohn, 569 F.2d 219, 227 (5th Cir. 1978) ("When the grand jury goes on a fishing expedition in forbidden waters, the courts are not powerless to act.") Cases cited in Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction, ACLU v. Clapper, 13 CV0399411-12.

[39] In Re Production of Tangible Things from [REDACTED], No. BR 08-13, Order at 9, 12 (FISA Ct.2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[40] In re Fontaine, 402 F. Supp. 1219, 1221 (E.D.N.Y. 1975) (quoting In re Surety Ass'n of Am., 388 F.2d 412, 414 (2d Cir. 1967)).

[41] In re Application of the Federal Bureau of Investigation for an Order Requiring the production of Tangible Things, No. BR 06-05.

behavior in the future. Most of the individuals in the database are suspected of no wrongdoing whatsoever. Yet the minimization procedures allow for any information obtained from mining the data to then be used in criminal prosecution. This is an unprecedented use of subpoena information-gathering authority. It amounts to a permanent, ongoing grand jury investigation into all, possible, future criminal acts.

Remarkably, FISC itself, despite the statutory language, has recognized that the information it obtains from the metadata program could not otherwise be collected with any other legal instrument—including a subpoena *duces tecum*. In a secret opinion issued in March 2009 Judge Reggie Walton wrote:

> Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States (U.S.) persons located within the U.S. who are not the subject of any FBI investigation and whose metadata *could not otherwise be legally captured in bulk*, the government proposed stringent minimization procedures that strictly controlled the acquisition, accessing, dissemination, and retention of these records by the NSA and FBI.[42]

Later in the document, he again noted that the information "otherwise could not be legally captured in bulk by the government".[43] This assertion directly contradicts the statutory requirement that the information could otherwise be obtained via subpoena *duces tecum*. It amounts to an admission, by the Court, that the program violated the statute.

What makes the failure of the Court to prevent the illegal program from continuing even more concerning is Judge Walton's explanation of why, even though the information could not legally be obtained in any other way, FISC allowed the government to proceed. He continues,

> Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and includes specific oversight requirements.[44]

In other words, FISC allowed an illegal program to operate because the government (1) promised that it was vital to U.S. national security, and (2) was directed by the court to police its own house by following

[42] In re Production of Tangible Things *From* [REDACTED], Order, No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.
[43] *Id.* at 12.
[44] *Id.*

the minimization procedures. The former is legally insufficient to justify violation of a Congressional statute. The latter highlights the extent to which FISC, precisely because of the size of the collection program in question, has become dependent on the NSA to conduct its own oversight—thus abdicating its responsibilities to the Executive Branch.[45] This further underscores the inapposite nature of the bulk collection program in light of the requirements of grand jury subpoenas, issued in the course of an investigation overseen by the judicial instruments of the state.

[45] *Id.* ("[I]n light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified. . . and that it is being implemented in a manner that protects the privacy interests of U.S. persons.")

"Continued Oversight of the Foreign Intelligence Surveillance Act" Hearing
<u>Senator Franken Questions for the Record</u>

(1) Professor DONOHUE, in August the Office of the Director of National Intelligence announced that it would start annually disclosing to the public the number of orders issued under key surveillance authorities, as well as the number of quote, "targets" affected by these orders. Are these promised disclosures enough? Or are actual changes to the law necessary to achieve greater transparency?

<u>Response</u>:

While welcome, the voluntary disclosure of the number of orders issued under key surveillance authorities, as well as the number of "targets" affected by these orders, is far from adequate. The release of such numbers, as can be seen from the current statistical updates provided by the Department of Justice, may provide some information, but its value is limited. The specific type of information being volunteered, moreover, is dwarfed by the claim that all telephony metadata is relevant to terrorism investigations. Any one order can result in millions of pages of data being released to the National Security Agency ("NSA"), suggesting that over-reliance on the reporting of the number of orders issued can be misleading. Similarly, reporting the number of targets, while contributing some information, fails to deliver meaningful data on the extent to which surveillance authorities are being used. The voluntary provision of such data, in addition, would not be subject to judicial review and could be altered absent Congressional approval, making the offer insufficiently grounded in the law. Actual statutory changes that address the quantitative and qualitative nature of the surveillance programs underway are essential to achieving greater transparency.

The Department of Justice ("DOJ") currently provides Congress with statistical information on the number of applications to the Foreign Intelligence Surveillance Court ("FISC"). This information has value. The numbers reveal that over the first two and a half decades FISC approved nearly every application without any modification.[1] (Between 1979 and 2003, FISC denied only 3 out of 16,450 applications.)[2] Looking more recently, since 2003, FISC has issued a ruling on 18,473 applications for electronic surveillance and/or physical search (2003-2008), and electronic surveillance (2009-2012). Only 11 applications have been denied in whole or part. (See *Fig. 1*) This means that only 0.06 percent of all applications are denied in whole or part. Looking at this data, scholars have observed that the rate of

[1] *See* DAVID S. KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS ch. 12 (2d ed. 2012), at 469. Letter from Attorney General William French Smith to Director, Administrative Office of the U.S. Courts (Apr. 22, 1981, *available at* [illegible] 1980 report) (No orders were entered which modified or denied the
[2] *Laura K.* DONOHUE, THE COST OF COUNTERTERRORISM: POWER, POLITICS AND LIBERTY 232 (2008).

success enjoyed by the government in its applications to FISC is "unparalleled in any other American court."[3]

FISC RULINGS ON ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH (2003-2008) AND ELECTRONIC SURVEILLANCE (2009 – 2012)[4]

Year	# of Applications on which FISC ruled	# Approved	# Modified	# Denied in Part	# Denied in Whole	# w/drawn by Gov't prior to FISC ruling
2003[5]	1,727	1,724	79	0	3[6]	0
2004[7]	1,756[8]	1,756	94	0	0	3
2005[9]	2,072[10]	2,072	61	0	0	2
2006[11]	2,176[12]	2,176	73	1	0	5
2007[13]	2,371	2,370	86	1	3[14]	0
2008[15]	2,082	2,083[16]	2	0	1	0
2009[17]	1,321[18]	1,320	14	1	1	8
2010[19]	1,506[20]	1,506	14	0	0	5
2011[21]	1,674[22]	1,674	30	0	0	2

[3] Theodore W. Ruger, *Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 245 (2007).

[4] Starting in 2009, the Department of Justice began providing the breakdown of the number approved, modified, denied in part, denied in whole, or withdrawn by the government prior to the FISC ruling only for those applications involving electronic communications. Prior to that time, these numbers were combined.

[5] Letter from William E. Moschella, Assistant Attorney Gen., to Mr. L. Ralph Mecham, Dir., Admin. Office of the U. S. Courts (Apr. 30, 2004), *available at* https://www.fas.org/irp/agency/doj/fisa/2003rept.pdf.

[6] An addition application was initially denied but later approved. *Id.*

[7] Letter from Office of Legislative Affairs, U.S. Department of Justice, to The Honorable J. Dennis Hastert, Speaker, U.S. House of Representatives, (Apr. 1, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/2004rept.pdf.

[8] 1758 submitted, 3 of which were withdrawn prior to FISC ruling and 1 of which was resubmitted. *Id.*

[9] Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to The Honorable J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 28, 2006), *available at* https://www.fas.org/irp/agency/doj/fisa/2005rept.html.

[10] 2,074 submitted, 2 of which were withdrawn prior to FISC ruling, and 1 of which was resubmitted. *Id.*

[11] Letter from Richard A. Hertling, Acting Assistant Attorney Gen., to the Honorable Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 27, 2007), *available at* https://www.fas.org/irp/agency/doj/fisa/2006rept.pdf.

[12] 2,181 submitted, 5 of which were withdrawn prior to FISC ruling. *Id.*

[13] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 30, 2008), *available at* https://www.fas.org/irp/agency/doj/fisa/2007rept.pdf.

[14] Discrepancy in the numbers stems in part from holdover applications and denials. Two applications, for instance, filed in CY 2006 were not approved until 2007. *Id.*

[15] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Majority Leader, U.S. Senate (May 14, 2009) *available at* https://www.fas.org/irp/agency/doj/fisa/2008rept.pdf.

[16] Discrepancy in the numbers stems in part from holdover applications and denials. Two applications filed in CY 2007 were not approved until CY 2008).

[17] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to The Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2010), *available at* https://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.

[18] For the first time since 2003, no numbers are available for modifications/denials for the full number of applications submitted (physical search, electronic surveillance, and combined applications). Instead, the report notes that of the 1,376 in total submitted in the former three categories, 1,329 were related to electronic surveillance. It was eight of these applications that were withdrawn, 1 denied in whole, 1 denied in part, and 14 modifications, with 1,320 approved. The number of applications is thus missing the numbers for physical search and physical search combined applications. *Id.*

[19] Letter from Ronald Weich, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Department of Justice, to the Honorable Harry Reid, Majority Leader, U.S. Senate, (Apr. 29, 2011), *available at* https://www.fas.org/irp/agency/doj/fisa/2010rept.pdf.

[20] Total number of electronic surveillance, physical search, and combined applications was 1,579. The report, however, isolates the electronic applications (1,511), and provides breakdowns for modifications, denials, etc., for just that category. Of the total of 1,511, five were withdrawn by the Government prior to FISC ruling. *Id.*

2012[23]	1,788[24]	1,788	40	0	0	1
Totals	***18,473***	***18,469***	***493***	***3***	***8***	***26***

Figure 1

Statistics provided by DOJ similarly demonstrate significant deference extended by FISC to the government with regard to applications under Section 215. From the numbers provided publicly to Congress, it appears that FISC has *never* denied an application for an order under this section. That is, of 751 applications since 2005, all 751 have been granted. (See *Fig. 2*)

ORDERS FOR THE PRODUCTION OF TANGIBLE GOODS

Year	**Number of Applications to FISC under 50 U.S.C. §1862(c)(2)**	**Number of Applications Granted by FISC**
2005[25]	155	155
2006[26]	43	43
2007[27]	6	6
2008[28]	13	13
2009[29]	21	21
2010[30]	96	96
2011[31]	205	205
2012[32]	212	212
Totals	***751***	***751***

Figure 2

These numbers illustrate both the advantage of reporting requirements and the limited value of such information. Crities of the FISC process, for instance, point to the numbers as evidence of the risk of capture presented by in camera, ex parte proceedings. Court supporters, in turn, note that a number of the

[21] Letter from Ronald Weich, Assistant Attorney Gen., to The Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), , *available at* https://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.
[22] Note that there were 1,745 total applications that included electronic surveillance and/or physical searches for foreign intelligence purpose. It appears that approximately 70 of the orders related solely to physical search, since the breakdown for electronic surveillance is only done for the 1,674. Two of the initial orders were withdrawn prior to FISC ruling. *Id.*
[23] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., to the Honorable Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), *available at* https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.
[24] The government made a total of 1,856 applications for electronic surveillance and/or physical searches; of those, 1,789 included requests for electronic surveillance. Of those, one was withdrawn by the Government prior to FISC ruling. *Id.*
[25] Letter from William E. Moschella, Assistant Attorney Gen., to the Honorable Richard B. Cheney, President, United States Senate (Apr. 28, 2006), *available at* http://www.justice.gov/nsd/foia/foia_library/2005fisa-ltr.pdf.
[26] Letter from Richard A. Hertling, Acting Assistant Attorney Gen., to the Honorable Richard B. Cheney, President, United States Senate (Apr. 27, 2007), *available at* http://www.justice.gov/nsd/foia/foia_library/2006fisa-ltr.pdf.
[27] Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., to the Honorable Richard B. Cheney (Apr. 30, 2008), *available at* http://www.justice.gov/nsd/foia/foia_library/2007fisa-ltr.pdf.
[28] Letter from Ronald Weich, Assistant Attorney Gen.l, to the Honorable Joseph R. Biden, Jr., President, United States Senate (May 14, 2009), *available at* http://www.justice.gov/nsd/foia/foia_library/2008fisa-ltr.pdf.
[29] Letter from Ronald Weich, Assistant Attorney Gen., to the Honorable Joseph R. Biden, Jr., President, United States Senate (Apr. 30, 2010), *available at* http://www.justice.gov/nsd/foia/foia_library/2009fisa-ltr.pdf.
[30] Letter from Ronald Weich, Assistant Attorney Gen., Department of Justice, to the Honorable Joseph R. Biden, Jr., President, U.S. Senate(Apr. 29, 2011), *available at* http://www.justice.gov/nsd/foia/foia_library/2010fisa-ltr.pdf.
[31] Letter from Ronald Weich, Assistant Attorney Gen., Department of Justice, to the Honorable Joseph R. Biden, Jr., President, U.S. Senate (Apr. 30, 2012), *available at* http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf.
[32] Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., Department of Justice, , to the Honorable Joseph R. Biden, Jr., President, U.S. Senate(Apr. 30, 2013), *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf.

applications for electronic surveillance or physical search are either modified or withdrawn by the government prior to FISC ruling, suggesting the presence of an informal process whereby FISC provides a check on the Executive. Critics counter by, again, appealing to the numbers. Looking at electronic surveillance and physical search applications, 493 modifications over the past decade still only comes to 2.6% of the total number of applications. (See *Fig. 1*). The numbers further show that only 26 applications have been withdrawn by the government prior to FISC ruling—approximately one tenth of one percent of all applications to the Court. (See *Fig. 1*).

In other words, the numbers raise concern about the role performed by FISC and indicate the presence of some informal process whereby FISC appears to be influencing the contours of applications. They also raise question about the extent of this informal process itself. But without further qualitative information and contextual data, it is extremely difficult to evaluate the information.

The release of statistical information regarding the number of orders approved by FISC would suffer from a similar lack of contextual information and raise concern about the extent to which such information might be misleading. The government argues that all telephony metadata is relevant to terrorism investigations. It also argues that Section 215 orders can be used to obtain massive amounts of data. This means that any *one* order can require telephone service providers to turn over millions of pages of data. Thus, while it would provide more information than is currently conveyed with regard to the number of applications to FISC under 50 U.S.C. §1862(c)(2), provision of this information would still fail to deliver meaningful data on the extent of surveillance programs underway.

Similarly, the provision of the number of individuals targeted by the government would generate more, but still insufficient information. In the process of targeting specific groups or individuals, the government claims the concurrent authority to draw in wide swathes of U.S. persons' information. So what may appear to be a limited number of targets may, in fact, be masking significant surveillance programs.

As a final note of caution, the voluntary provision of such data would be merely a policy adopted by the Executive Branch. Resultantly, it would not be subject to judicial review and it could be altered without any action from—or even notice to—Congress. It is thus an extremely weak way to ensure greater transparency within the Executive Branch. Actual statutory changes that require DOJ to convey both the quantitative and the qualitative nature of the surveillance programs underway are essential for achieving greater transparency.

Responses to Questions for the Record
Submitted October 29, 2013
Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States Senate, Committee on the Judiciary
Hearing on
Continued Oversight of the Foreign Intelligence Surveillance Act
October 2, 2013

I thank the Committee for the opportunity to respond to these Questions for the Record.

Senator Klobuchar's Question

I am very interested in your recommendation that the FISC should have greater in-house technological expertise to assess the government's bulk collection and surveillance requests. I'd like to ask you to flesh this out a bit more.

How would you recommend working technology experts into the current FISC process?

Response to Senator Klobuchar's Question

In the current FISC process, the government is the only party that files papers and argues before the Court. The most natural way to add independent technical expertise would be for the expert to assist the Court. The Court might follow the practice of some ordinary District Courts by retaining a Court-appointed expert, or by appointing a special master who has technical expertise.

If the FISC process is changed to add another party empowered to participate in FISC matters, such as a representative of the public or an advocate for civil liberties, then this party could retain technical experts to assist it in its argument. This expert assistance is important in allowing the independent party to do its job, because the government's argument before the FISC is well-supported by technical experts, and technical claims often play an important role in the government's argument.

If the process is indeed changed to add an independent party, it is important for this party to be able to challenge the government's technical claims. In an ordinary court case, this would occur via discovery, including expert reports, depositions, and cross-examination of experts. Although this full process might not be appropriate for FISC matters, it is important to ensure that the independent party is in a position to get the information it needs to evaluate and challenge technical assertions made by the government.

Finally, the sensitivity of information before the FISC will require that technical experts have the necessary security clearances. Some independent experts already have clearances, but there are relatively few such people who are not already working for or with intelligence agencies. Steps should be taken to make sure that clearance requests can be expedited for technical experts whom the FISC or an independent party want to engage.

Senator Franken's Question

(1) Professor Felten, in your written testimony you stated that "metadata is easy to analyze."

(a) Do you think the intelligence community has the technical ability to give a rough estimate of the number of American citizens and permanent residents whose communications metadata has been collected in their surveillance programs?

(b) Do you think that the intelligence community has the technical ability to give a rough estimate of the number of American citizens and permanent residents whose communications content has been collected in their surveillance programs?

Response to Senator Franken's Question

Yes, the government has the ability to give a rough estimate of the number of American citizens and permanent residents whose (a) metadata and (b) content has been collected.

(a) The intelligence community can give a rough estimate of the number of citizens and permanent residence whose communications *metadata* has been collected. There are several reasonable methods for doing this. Each method gives an estimate that is not exact but is of roughly the correct magnitude.

A first method is to determine the number of U.S. phone numbers that appear in collected metadata records, and then use this information to estimate the number of affected persons. U.S. phone numbers are easily distinguished from non-U.S. numbers by examining the country code and/or area code of the number. Once the number of affected phone numbers is known, this can be used to estimate the number of citizens and permanent residents by making two adjustments, the first to account for the possibility of one person using multiple affected phone numbers, and the second to account for the fact that a small percentage of U.S. phone numbers are owned by people who are neither citizens nor permanent residents.

A second method is to determine the number of distinct customers of each mobile phone carrier whose information is captured. On the assumption that few people have mobile accounts with multiple mobile carriers, this could be used to estimate the total number of affected persons, again correcting for the fact that a small percentage of accounts are owned

by people who are neither citizens nor permanent residents.

A third method, which appears to offer good accuracy if news reports are accurate, is simply to assume that every adult citizen or permanent resident has been on at least one end of a call whose metadata was captured, and therefore to use an estimate equal to the number of adult citizens plus permanent residents.

(b) It is a bit more challenging, but still feasible, for the intelligence community to give a rough estimate of the number of citizens and permanent residents whose communications *content* has been collected.

It is very likely that in all or almost all cases where call content is collected, the metadata about that same call is also collected. If so, then all that remains is to asssemble a database of metadata for calls whose content has been captured, and then to use this metadata to estimate the number of affected citizens and permanent residents. This could be done, for example, by using the first method described above in part (a).

Even if, for some reason, content collection is not accompanied by metadata collection for the same calls, it would be feasible to estimate the number of affected citizens and U.S. persons, using the existing metadata.

This is not meant as an exhaustive list of methods, and there are probably better and more accurate methods than the ones I have described here. The intelligence community employs a great many mathematicians, statisticians, and computer scientists, and prides itself on its ability to extract useful information from large data sets. Surely they are able to provide at least rough estimates of how many Americans are affected by their data collection.

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate

The Honorable Charles Grassley
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
United States House of Representatives

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
United States House of Representatives

September 30, 2013

We the undersigned are writing to ask that the Senate and House Judiciary Committees quickly move forward to consider legislation that would provide 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.

Specifically, we write to voice our strong support for S. 1452, the Surveillance Transparency Act of 2013, and H.R. 3035, the Surveillance Order Reporting Act of 2013, each of which would clarify that companies have the right to publish basic statistics about the government demands for user data that they receive. We urge the Committees to hold hearings on the issue of surveillance transparency as a prelude to the markup of these bills.

Many of the undersigned organizations and companies previously wrote a letter to you and other leaders in Congress and the Administration on July 18th,[1] asking for legislation that would require more comprehensive transparency reporting by the government and allow for more comprehensive transparency reporting by US companies that receive national security–related information requests. We are thankful that Senator Franken, working with eleven cosponsors including Chairman Leahy, and Representative Lofgren, as part of a bipartisan coalition of nine cosponsors including Ranking Member Conyers and Representatives Poe and Chaffetz, were able to so quickly respond to the pressing need for more transparency around the US government's national security surveillance efforts. Such transparency is important not only for the American people, who are entitled to have an informed public debate about the appropriateness of that surveillance, but also for international users of US-based service providers who are concerned about privacy and security.

We very much look forward to working with the sponsors of S. 1452 and H.R. 3035 to ensure that the goals of those pieces of legislation, and the goals stated in our previous letter, are fully aligned. For example, the Senate bill provides for significant public reporting by the government itself, as requested in our previous letter, and we would welcome the addition of such provisions to the House bill. Similarly, as we had previously requested, the House bill provides for reporting by companies on their receipt of National Security Letters (NSLs) as well as requests under the Foreign Intelligence Surveillance Act (FISA), and we would strongly support inclusion of a similar provision regarding NSLs in the Senate bill, consistent with Chairman Leahy's longstanding and much appreciated support for NSL reform.

In conclusion, we are eager to assist your Committees in taking prompt action around these critically important bills, and to share our views as other bills are introduced or move through the Committees. We look forward to working together to achieve passage of legislation that will ensure the level of transparency necessary to appropriately inform the American public and preserve the trust of Internet users around the world.

---

[1] A copy of that letter, updated to reflect additional companies and organizations that have joined the coalition effort since it was first sent, is attached.

Thank you.

Companies & Investors
AOL
Apple Inc.
Automattic Inc. (WordPress.com)
Boston Common Asset Management
CloudFlare
CREDO Mobile
Data Foundry, Inc.
Domini Social Investments LLC
DreamHost
Dropbox
DuckDuckGo
Facebook
Floor64
Foursquare
Golden Frog
Google
LinkedIn
Meetup
Microsoft
Mozilla
Reddit
Personal Democracy Media
SpiderOak
Tumblr
Twilio
Twitter
Union Square Ventures
Yahoo

Nonprofit Organizations & Trade Organizations
Access
AIDS Policy Project
American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
American Society of News Editors
Association of Research Libraries
Brennan Center for Justice at NYU Law School
BSA | The Software Alliance
Competitive Enterprise Institute
Computer & Communications Industry Association
The Constitution Project
Consumer Action
Defending Dissent Foundation
Demand Progress
Digital Liberty Project at Americans for Tax Reform
DownsizeDC.org
Electronic Frontier Foundation
Engine Advocacy
First Amendment Coalition
Foundation for Innovation and Internet Freedom
Freedom House
Freedom of the Press Foundation
Freedom to Read Foundation
Global Network Initiative
Information Technology and Innovation Foundation
The Internet Association
Internet Infrastructure Coalition
Jewish Voice for Peace
Montgomery County Civil Rights Coalition
National Coalition Against Censorship
NetChoice
New America Foundation's Open Technology Institute
New York Tech Meetup
OpenTheGovernment.org
Project On Government Oversight
Public Citizen
Public Knowledge
Reporters without Borders
Reporters Committee for Freedom of the Press
Software & Information Industry Association
TechFreedom
TechNet
WITNESS

"Continued Oversight of the Foreign Intelligence Surveillance Act" Hearing

October 2nd, 2013

Dear Senators Leahy and Grassley:

Thank you for holding the hearing on October 2 regarding oversight of the Foreign Intelligence Surveillance Act (FISA) in light of the disclosures about NSA surveillance and collection of metadata that includes massive amounts of data about American citizens.

The main thing I want to correct is what Senator Feinstein said about the pre 9-11 warning from Director of Central Intelligence George Tenet, Feinstein's referring to the case of the (arrested) "terrorist who wanted to learn to fly without taking off or landing," the problem of "stovepiping" of intelligence that kept agencies from learning that Al Qaeda terrorist Al Midhar had entered California and her conclusion that if more metadata had been collected prior to 9-11, the attacks could have been prevented. With all due respect, Senator Feinstein has it completely wrong! With her factually inaccurate version of pre 9-11 failures, her point was to insist that there be no significant rolling back of the NSA's post 9-11 massive metadata and FISA surveillance programs. But her account is wrong and the truth is that this massive government surveillance is making things worse and even harder for analysts and agents trying to find the needle in the haystack by adding more hay. Agents and analysts are reported to call the non-relevant data collection "white noise" or false leads, etc.

I would be happy to provide more detail but in a nutshell, the main finding of the 9-11 Commission, based upon the earlier findings of the Joint Intelligence Committee's Inquiry (JICI) which Senator Feinstein was a part of and to whom I actually addressed my "whistleblower memo" of May 21, 2002 about the FBI's pre 9-11 failures (and also based upon the Senate Judiciary Committee's investigation which Senators Leahy and Grassley led in the spring-summer of 2002; and the lengthy Department of Justice's Inspector General Investigation of these failures) was that the failure to share information within agencies, between agencies and with the public was a major problem that enabled the Al Qaeda terrorist attacks to occur. Many examples of these failures to share information (including "stove piping") were documented, including the Moussaoui case in Minnesota and the case of the TWO (not one) Qaeda suspects Al Midhar AND Al Hazmi who the CIA had long been following since their Al Qaeda-related meeting monitored by the CIA in Kuala Lumpur. The CIA learned of Hazmi and Midhar's entry into California but failed to notify the FBI in a timely manner, not until a few weeks before 9-11. As you will recall Moussaoui later convicted of conspiring with the 9-11 hijackers, was arrested in Minnesota on August 16, 2001, suspected of terrorism connected to Bin Laden and thereafter the FBI Headquarters supervisors failed to share this info with the proper DOJ Office to seek a FISA Order for searching of Moussaoui's belongings despite 60 to 70 detailed requests via telephone, email and written draft declaration such that the FBI case agent later testified at Moussaoui's trial, that this FBIHQ "stovepiping" (or maybe the more accurate term would be "stonewalling") constituted "criminal negligence."

There are many more examples that were adduced and documented of US intelligence agencies already possessing key pieces of information and intelligence including the NSA's interception of conversations between terrorist hijackers and planners that were intercepted before 9-11 about the upcoming attacks that were not translated and understood until after the attacks occurred. The excuse by main officials for why they did not share or act upon the key information they already possessed--and in some cases, did not even read--until after 9-11 was that "intelligence is like a firehose and you can't get a sip from a firehose." In other words, officials' excuse for not even reading key intelligence memos, let alone properly sharing and disseminating such information or acting upon it, was that there was already too much intelligence being acquired before 9-11. Related to the "firehose" excuse for why the existing intelligence data was not read, shared or acted upon is that the claim it was impossible to make sense of it, to prioritize the importance of data, and "to connect the dots" when there is so much.

Senators Leahy and Grassley may recall that the Senate Judiciary Committee (at which I testified on June 6, 2002) later uncovered the fact that the FBI's National Security Law Unit Chief failed to read the detailed, written draft declarations submitted by Minnesota FBI agents in the Moussaoui case but simply relied upon a short verbal briefing. A couple years ago, former New York Times reporter Phil Shenon (also author of the book "The Commission" about the 9-11 Commission) discovered another "terrible missed chance" involving a prior written memo to then FBI Director Louis Freeh written in April 2001 explicitly warning of upcoming terrorist attacks by Osama Bin Laden's group and that Bin Laden was "heavily entwined" with the Chechen leader Ibn Al Khattab. However, several of the high level FBI executives who this April 2001 memo was addressed to by name, later denied having read it. And the information linking Al Khattab to Bin Laden was precisely the reason FBIHQ supervisors failed to appreciate the foreign power connection (for which they later were faulted). The FBI Supervisors were held at fault for failing to recognize the foreign power connection but their own supervisor claimed he had not read this April 2001 memo and therefore had not shared it with them.

DCI George Tenet, who Feinstein stated had passionately warned her intelligence committee of upcoming attacks during the summer of 2001 was himself briefed about the arrest of terrorist suspect Moussaoui in Minnesota as an "Islamic fundamentalist who learns to fly" on August 23 or 24, 2001, yet he could not really explain to the 9-11 Commission why he took no action. It's never been determined if DCI Tenet warned the President or anyone else of this information he received almost three weeks before 9-11.

In conclusion, in all due fairness, Senator Feinstein is dead wrong that the 9-11 attacks occurred as a result of not possessing the NSA and other surveillance programs that now collect massive amounts of metadata and other information about individuals, including American citizens, who are not suspicious. US intelligence officials did not read, share or act upon the key pieces of info they already had. And their excuse then was that they were getting too much data to even be able to read, or intelligently share or act upon this intelligence.

I would be happy to provide further details if you are interested.

Coleen Rowley, retired FBI agent and former FBI Minneapolis Division Legal Counsel, Apple Valley, MN

○