THE BROOKINGS INSTITUTION

SAUL/ZILKHA ROOMS

PRIVACY, TECHNOLOGY AND NATIONAL SECURITY:

AN OVERVIEW OF INTELLIGENCE COLLECTION

Washington, D.C.

Friday, July 19, 2013

PARTICIPANTS:

Introduction and Moderator:

WELLS C. BENNETT
National Security Law Fellow
The Brookings Institution

Keynote Speaker:

ROBERT S. LITT
General Counsel
Office of the Director of National Intelligence

* * * * *

P R O C E E D I N G S

MR. BENNETT: Good morning. Welcome to Brookings. My name is Wells Bennett. I'm a fellow in national security law here and managing editor of the *Lawfare* blog, a blog dedicated, we hope, to the non-ideological and rigorous discussion of national security law issues. That means we have followed a certain story that has been in the news lately. It's the story that I suspect brought all of you here and also brought our speaker today, Bob Litt, the General Counsel to the Office of the Director of National Intelligence.

By this, of course, I mean the recent revelations about certain intelligence activities our government, chiefly surveillance conducted pursuant to the Foreign Intelligence Surveillance Act, or FISA, that I think it's fair to say has generated some controversy about the legality, about the effectiveness and the wisdom of these surveillance activities.

There are also some pretty serious questions about privacy as we live now in an era in which vast swathes of our personal data are pushed out into the cloud to third parties. We're going to hear about that, I suspect, in great detail -- about privacy issues -- also oversight; executive, judicial, and congressional, from Bob in just a moment.

As for his biography, Bob, as I mentioned, is the General Counsel at the DNI, a post he has served since 2009. Prior to that, he was a partner in a no-name law firm here in D.C. called Arnold and Porter. I suppose I should mention that Bob and I overlap there, and working with him, in some respects, got me into this racket. We collaborated on a piece that was edited by Ben Wittes, a senior fellow here. By doing that I started working with Ben, writing for his blog, and then by doing that, I became a

fellow here. So, in some indirect way, I suppose, Bob, I have you to thank or to blame for my current job.

In any case, prior to Arnold and Porter, Bob served in senior positions in the Justice Department as deputy assistant attorney general in the Criminal Division and as the PADAG or principal associate deputy attorney general. I believe I have that right. He began his legal career as a law clerk to Judge Edward Weinfeld in the Southern District of New York, and also as a clerk for Justice Potter Stewart of the United States Supreme Court. He is a graduate of Harvard University and of Yale Law School. Please help me welcome Bob to Brookings. (Applause)

MR. LITT: So, thank you, Wells. I want to thank Wells and Brookings for hosting this speech, and I want to thank all of you for coming. I do just want to note that the *Lawfare* blog is a terrific source of balanced commentary on this. It's something I try to check in on periodically. And I want to apologize in advance for the length of this speech because I have a lot to cover. I hope I don't get into Fidel Castro territory. (Laughter)

I wish that I were here in happier times for the intelligence community. The last several weeks have seen a series of reckless disclosure of classified information about intelligence activities. These disclosures threaten to cause long-lasting and perhaps irreversible harm to our ability to identify and respond to the many threats facing our nation, and because the disclosures were made by people who did not fully understand what they were talking about, they were sensationalized, and they've led to misleading and mistaken impressions. I hope to be able to correct some of those misimpressions today.

My speech today, as Wells mentioned, is prompted by disclosures about two programs that collect valuable intelligence that has been used to protect our nation

and its allays; one of the bulk collection of telephony metadata, and the other is the so-called PRISM Program.

Some people claim that the disclosures about these programs were a form of whistle blowing, but I want to be clear about this. These programs were not illegal. They are authorized by Congress, and they're carefully overseen by the Congressional Intelligence and Judiciary Committees. They are conducted with the approval of the Foreign Intelligence Surveillance Court and under that court's supervision and they are subject to extensive court-ordered oversight in the Executive branch. In short, all three branches of government knew about these programs, approved them, and helped ensure that they operated in compliance with the law. Only time will tell us the extent of the damage caused by the unlawful disclosure of these lawful programs.

Never the less, I appreciate that it is not enough for me to stand here and simply assert that our activities are consistent with the letter of the law. The activities of our government must always reflect and reinforce our core democratic values. Those of us who work in the intelligence profession share these values including the importance of privacy. After all, we're all citizens of the United States as well.

But security and privacy are not zero-sum. We have an obligation to give full meaning to both; to protect security while, at the same time, protecting privacy and other constitutional rights. Although our values are enduring however, the manner in which our activities reflect those values necessarily has to change to adapt to changing technology, societal expectations, and norms. And so, we in the intelligence community are constantly evaluating and improving the safeguards that we have in place to protect privacy while at the same time ensuring that we can carry on our mission of protecting national security. And that's going to be the focus of my speech this morning.

I want to do three things. First, I want to discuss and lay out very briefly the laws that govern intelligence collection. Second, I want to talk about the impact of changing technology and the corresponding need to adapt how we protect privacy on those collection activities. And third, I want to bring these two strands together and explain how some of these laws and technology changes play out in practice; how we structure the intelligence community's collection activities under FISA in a way that remains faithful to our democratic values.

So, I want to begin by discussing in very general terms the legal framework that governs intelligence collection activities, and it is a bedrock concept that those activities are bound by the rule of law. This is a topic that others have well-addressed, including the general counsels of the Central Intelligence Agency and the National Security Agency in speeches they've given, and so, I'll make this brief.

We begin with the Constitution. Article 2 makes the President the Commander in Chief, and gives him extensive responsibility for the conduct of foreign affairs. The ability to collect foreign intelligence derives from that Constitutional source. The First Amendment protects freedom of speech and association, and the Fourth Amendment protects unreasonable searches and seizures, and I want to specifically make a few points about the Fourth Amendment. First, under established Supreme Court rulings, a person has no legally recognized expectation of privacy in information that he or she voluntarily gives to a third party, so obtaining those records from that third party is not a search as to the person. I'll return to this point in a moment.

Second, the Fourth Amendment generally does not apply to foreigners outside of the United States. And third, the Supreme Court has said that the reasonableness under the Fourth Amendment of searches without a warrant depends on

balancing "the intrusion on the individual's Fourth Amendment interests against the search's promotion of legitimate governmental interests." So, that's the Constitution.

There are also a variety of statutes governing our collection activities. First, the National Security Act and a number of laws related to specific agencies such as the Central Intelligence Agency Act or the National Security Agency Act limit what agencies can do so that, for example, the CIA is prohibited from domestic law-enforcement activities.

We're also governed by laws such as the Electronic Communications Privacy Act, the Privacy Act, and in particular for today, the Foreign Intelligence Surveillance Act, or FISA. FISA was passed by Congress in 1978 and was significantly amended in 2001 and 2008. It regulates electronic surveillance and other activities carried out for foreign intelligence purposes, and I'll talk a lot more about FISA later on.

There's one final important source of legal restrictions on intelligence activities, and that's Executive Order 12333. This order, which is the founding charter of the intelligence community, provides additional limits on what intelligence agencies can do. It defines each agency's responsibilities and authorities, and one particular provision of EO 12333 is very significant. It's Section 2.3, and it provides that elements of the intelligence community, and I'm quoting here with some ellipses. Elements of the intelligence community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures approved by the Attorney General after consultation with the director of National Intelligence.

These procedures have to be consistent with the agency's lawful authorities. The procedures also have to establish strict limits on collecting, retaining, or disseminating information about U.S. persons unless that information is of foreign-

intelligence value or in certain other circumstances spelled out in the order such as to protect against the threat to life.

These so-called “U.S. person rules” are basic to the operation of the intelligence community. They’re among the first things that our employees are trained on, and they are the core of our institutional culture. And it’s not surprising that our legal regime provides special rules for activities directed at United States persons. So far as I know, and I’m not an expert in this, but so far as I know, every nation in the world recognizes legal distinctions between its citizens and non-citizens, but as I hope to make clear this morning, our intelligence collection procedures also provide protection for the privacy rights of non-citizens.

Now I want to turn to the impact of changing technology on privacy. Prior to the end of the 19th century, you really would find very little discussion about a “right to privacy.” In the absence of mass media, photography, and other technologies of the industrial age, the most serious invasions of privacy were generally the result of gossip or peeping toms.

Indeed, in the 1890 article that first articulated the idea of a legal right to privacy, Louis Brandeis and Samuel Warren explicitly grounded that idea on changing technology, and I’m going to read a quote from the article. “Recent inventions in business methods” -- this is 1890, remember -- “recent inventions in business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley calls ‘the right to be let alone.’ Instantaneous photographs in newspaper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house top.”

Well, today, 120-plus years later, as a result of the way digital technology has developed, each of us shares massive amounts of information about ourselves with third parties. Sometimes this is obvious as when we post pictures on social media or transmit our credit card numbers to buy products online. Other times it's less obvious as when telephone companies store records listing every call we make. All in all, however, there is little doubt that the amount of data that each of us provides to strangers every day would astonish Brandeis and Warren, let alone Jefferson and Madison.

And this leads me to what I consider to be the key question. Why is it that people are willing to expose large quantities of information to private parties, but don't want the government to have that same information? Why, for example, don't we care very much if the telephone company keeps records of all of our phone calls, but we feel very differently about the prospect of the same information going to NSA?

This actually is not a very difficult question to answer. We care because of what the government could do with the information. Unlike a phone company, the government has the power to audit our tax returns, to prosecute and imprison us, to grant or deny licenses to do business, and many other things. And so, there's an entirely understandable concern that the government might abuse this power.

I don't mean to say that private companies don't also have a lot of power over us. Indeed, the growth of corporate privacy policies and the strong public reaction to the inadvertent release or commercial use of personal information by those companies reinforces my belief that our primary privacy concern today is less with who has information than what they can and do with it. But there is no question that the government, because of its powers, is properly viewed in a different light.

On the other hand, just as consumers around the world make extensive use of modern technology so, too, do potential hostile foreign governments and foreign

terrorist organizations and others. Indeed, we know that terrorists and weapons proliferators are using global-information networks to conduct research, to communicate, and to plan attacks.

Information that can help us identify and prevent terrorist attacks or other threats to our security is often hiding in plain sight among the vast amounts of information flowing around the globe, and the new technology means that the intelligence community must continue to find new ways to locate and analyze foreign intelligence information. We need to be able to do more than connect the dots when we find them. We need to be able to find the right dots in the first place.

While one approach to protecting privacy in this context would be to limit the intelligence community to targeted, focused queries looking for specific information about identified individuals based on probable cause. But from a national security prospective, this would not be sufficient.

The business of foreign intelligence has always been fundamentally different from the business of criminal investigation. Rather than attempting to solve crimes that have happened already, we're trying to find out what is going to happen before it happens. We may, for example, have only fragmentary information about someone who's plotting a terrorist attack and need to get more information to find him and stop him. We may get information that's useless to us without a store of data to match it against, such as when we get the telephone number of a terrorist and want to find out who he's been in contact with. Or we may learn about a plot that we were previously unaware of, causing us to revisit old information and find connections that we didn't notice before; connections that we would never know about if we hadn't collected the information originally and kept it for some period of time.

We worry all the time about what we're missing in our daily effort to protect the nation and our allies. So, on the one hand you have vast amounts of data that contain intelligence needed to protect us not only from terrorism but from threats such as cyber-attacks, weapons of mass destruction, and good old fashioned espionage. And on the other hand, giving the intelligence community access to this information has obvious privacy implications.

We achieve both security and privacy protection in this context in large part by a framework that establishes appropriate controls over what the government can do with the information it lawfully collects, and appropriate oversight to ensure that it respects those controls. These protections depend on a variety of factors such as the type of information we collect, where we collect it, the scope of the collection, and the use the government intends to make of the information. In this way we can allow the intelligence community to acquire necessary foreign intelligence while providing privacy protections directed at the use of that information that take account of modern technology.

In showing this morning that this approach is, in fact, the way our system deals with intelligence collection, I'll use FISA as an example for a couple of reasons. First, because FISA is an important mechanism through which Congress has legislated in the area of foreign intelligence activities. Second, because it covers a wide range of activities and involves all three sources of law I mentioned earlier; Constitutional, statutory, and executive. And third, because several previously classified examples of what we do under FISA have recently been declassified, and I know people want to learn more about them.

I don't mean to suggest by this that FISA is the only way we collect foreign intelligence, but it's important to know that by virtue of Executive Order 12333, all

of the collection activities of our intelligence agencies have to be directed at the acquisition of foreign intelligence or counter-intelligence.

Our nation's intelligence priorities are set annually through an inter-agency process. The leaders of the country tell the intelligence community what information they need in the service of the nation, its citizens, and its interests, and we collect information in support of those priorities.

I want to emphasize that the United States is a democratic nation, takes seriously this requirement that intelligence collection activities have a valid intelligence purpose. We do not use our foreign intelligence capabilities to steal the trade secrets of foreign companies in order to give American companies a competitive advantage. We do not indiscriminately sweep up and store the contents of the communications of Americans or the citizenry of any country. We do not use our intelligence collection capabilities for the purpose of repressing the citizens of any country because of their political, religious, or other beliefs. We do collect meta-data; information about communications more broadly than we collect the actual content of communications, but that's because it's less intrusive than collecting content and, in fact, can provide us information that helps us more narrowly focus our collection of content on appropriate foreign intelligence targets. But it's simply is not true that the United States government is listening to everything said by the citizens of any country.

So let me now turn to FISA. I'm going to talk about three provisions of that law; traditional FISA orders, the FISA business records provision, and Section 702. These provisions are relating to the acquisition of different kinds of information and provide limits on how it can be collected, require procedures restricting what we can do with the information we collect, and how long we can keep it, and impose oversight to ensure that those rules are followed. This sets up a coherent regime in which protections

are afforded at the front end when information is collected, in the middle when that information is reviewed and used, and at the back end through oversight, all working together to protect both national security and privacy.

The rules vary depending on factors such as the type of information being collected and, in particular, whether or not we're collecting the content of communications, the nature of the person or persons being targeted, and how narrowly or broadly focused the collection is. They are not identical in every respect to the rules that govern criminal investigations, but I hope to persuade you that they are reasonable and appropriate in the very different context of foreign intelligence.

So, let's begin by talking about traditional FISA collection. Prior to the passage of FISA in 1978, the collection of foreign intelligence was essentially unregulated by statutory law. It was viewed as a core function of the Executive branch. In fact, when the criminal wiretap provisions were originally enacted in 1968, Congress put a provision in there expressly stating that these provisions "did not limit the Constitutional power of the President to obtain foreign intelligence information deemed essential to the national security of the United States." However, 10 years later, as a result of the abuses revealed by the Church and Pike Committees, Congress did decide to impose a judicial aspect on some aspects of electronic surveillance for foreign intelligence purposes. This is what is now codified in Title 1 of FISA, sometimes referred to as traditional FISA. FISA, as most of you know by now, established a special court, the Foreign Intelligence Surveillance Court, to hear applications by the government to conduct electronic surveillance for foreign intelligence purposes. Because traditional FISA surveillance involves acquiring the content of communications, it's intrusive, implicating recognized privacy interests, and because it can be directed at individuals

inside the United States including American citizens, it directly implicates the Fourth Amendment.

In FISA, Congress required that to get a traditional FISA electronic surveillance order, the government must establish probable cause to believe that the target of surveillance is a foreign power or an agent of a foreign power, a probable cause standard that's derived from the standard used for wiretaps in criminal cases. And if the target is the United States person, he or she cannot be deemed an agent of a foreign power based solely on activity protected by the First Amendment. You cannot be the subject of surveillance merely because of what you believe or think. Marco Rubio moment. (Laughter)

Moreover, by law, the use of information collected under traditional FISA must be subject to minimization procedures, and that's a concept that's key throughout FISA. Minimization procedures are procedures that are approved by the FISA court that must be, and again, I'm quoting from the FISA statute here, "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention and prohibit the dissemination of non-publicly available information concerning un-consenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

For example, minimization procedures generally prohibit disseminating the identity of any U.S. person unless the identity itself is necessary to understand the foreign intelligence or is evidence of a crime. Now, the reference in the statute to the purpose and technique of the particular surveillance is important. Minimization procedures can and do differ depending on the purpose of the surveillance and the technique used to implement it. These tailored minimization procedures are an important way in which we do provide appropriate protections for privacy.

So, let me explain in general terms how traditional FISA works in practice. Let's say that the FBI suspects someone inside the United States of being a spy or a terrorist, and they want to conduct electronic surveillance of that person. While there are some exceptions spelled out in the law such as in the case of an emergency, as a general rule the government has to present an application to the FISA court establishing probable cause to believe that that person is an agent of a foreign power according to the statutory definition. That application, by the way, is reviewed at several levels within both the FBI and the Department of Justice before it's even submitted to the court.

Now, if the surveillance is approved, the target may have a conversation with a U.S. person that has nothing to do with the foreign intelligence purpose of the surveillance such as talking to a neighbor about a dinner party. Under the minimization procedures an analyst who listens to a conversation involving a U.S. person that has no foreign intelligence value generally cannot share it or disseminate it unless it's evidence of a crime. And even if the conversation does have foreign intelligence value, let's say it's a terrorist talking to a confederate, that information may only be disseminated to someone with an appropriate need to know the information pursuant to his or her legally authorized mission.

In other words and summing up on this, electronic surveillance under FISA's Title 1 implicates the well-recognized privacy interests in the contents of communications, and is subject to corresponding protections for that privacy interest in terms of the requirements that it be narrowly targeted and have a substantial factual basis approved by the court and in terms of the limitations imposed on the use of that information.

Now let me turn to the second activity which is the collection of business records. After FISA was passed, it became apparent that it left some significant gaps in our intelligence collection capabilities. In particular, while the government had the power in a criminal investigation to compel the production of records with a grand jury subpoena, it lacked similar authority in foreign intelligence investigations.

So, a provision was added in 1998 to provide such authority, and it was amended by Section 215 of the USA Patriot Act which was passed shortly after 9/11, and that's why this provision is generally referred to as Section 215. It allows us to apply to the FISA court for an order requiring the production of documents or other tangible things when they're relevant to an authorized national security investigation. Records can be obtained only if they're the type of records that could be obtained pursuant to a grand jury subpoena or other court process; in other words, where there's no statutory or other protection that would prevent the use of a grand jury subpoena to obtain them.

In some respects, this process is, in fact, more restrictive than a grand jury subpoena. A grand jury subpoena is issued by a prosecutor without any prior judicial review, whereas under the FISA business records provision we have to get court approval. Moreover, as with traditional FISA, records obtained pursuant to the FISA business records are subject to court-approved minimization procedures that limit the retention and dissemination of information about U.S. persons, and while there are other protections that adhere in grand jury subpoena information, this one does not apply.

Now, of course, the FISA business records provision has been in the news recently because of one particular use of that provision. The FISA court has repeatedly approved orders directing several telecommunications companies to produce certain categories of telephone metadata such as making the call, the number being called, and the time, date, and duration of the call. It's important to emphasize, as we do

every time we talk about this, that under this program we do not get the contents of any conversation. We do not get the identity of any party to the conversation, and we do not get any cell site or GPS locational information.

This limited scope of what we collect has important legal consequences. As I mentioned earlier, the Supreme Court has held that if you have voluntarily provided this kind of information to third parties, you have no reasonable expectation of privacy in that information. All of the metadata that we get under this program is information that the telecommunications companies obtain and keep for their own business purposes. As a result, the government can get this information without a warrant consistent with the Fourth Amendment.

None the less, I recognize that there's a difference between getting metadata about one telephone number and getting it in bulk. From a legal point of view, Section 215 only allows us to get records if they are relevant to a national security investigation, and from a privacy perspective, people worry that, for example, the government could apply data mining techniques to a bulk data set and learn new personal facts about them even when the underlying set of records is not subject to a reasonable expectation of privacy for Fourth Amendment purposes. I do want to make clear, however, that as I'll explain in a minute, we're not allowed to do that sort of analysis of these records, and we don't do it. On the other hand, this information is clearly useful from an intelligence perspective. It can help identify links between terrorists overseas and their potential confederates in the United States.

It's important to understand the problem that this program was intended to solve. Many will recall that one of the criticisms made by the 9/11 Commission was that we were unable to locate the connection between a hijacker who was in California and an Al Qaeda safe house in Yemen. Although NSA had collected the conversations

from the Yemeni side, they had no way to determine that the other end of those communications was in the United States and hence to identify the homeland connection. This collection program is designed to help us find those connections.

In order to do that, however, we need to be able to access the records of telephone calls possibly going back many years, and we don't know in advance which calls those are going to be. However, telephone companies have no legal obligation to keep this kind of information, and they generally destroy it after a period of time that they determine based on their own business purposes. Moreover, the different telephone companies have separate data sets in different formats which make analysis of possible terrorist calls involving several providers considerably slower and more cumbersome. That could be a significant problem in a fast-moving investigation where speed and agility are critical such as the plot to bomb New York City subways in 2009.

So, the way we fill this intelligence gap while at the same time protecting privacy illustrates the approach I outlined earlier. From a subscriber's point of view, as I said before, the difference between a telephone company keeping records of his phone calls and the intelligence community keeping the same records is what the government could do with the records. That's an entirely legitimate concern, and we deal with it by limiting what the intelligence community is allowed to do with the records; limitations that are specifically approved by the FISA court.

First, we put this information in secure databases. Second, the only intelligence purpose for which this information can be used is counter-terrorism. Third, we only allow a limited number of specially-trained analysts to search these databases. Fourth, even those analysts are allowed to search the database only when they have a reasonable and articulable suspicion that a particular telephone number is associated with particular foreign terrorist organizations that have been identified to the court. The

basis for that reasonable articulable suspicion has to be documented in writing and approved by a supervisor. Fifth, the analysts are allowed to use this information only in a very limited way to map the network of telephone numbers calling other telephone numbers. Sixth, because this database contains only metadata, even if the analyst finds a previously unknown telephone number that warrants further investigation, all she can do is disseminate the telephone number. She doesn't even know whose number it is. Any further investigation relating to that number has to be done pursuant to other lawful means, and in particular, any collection of the contents of communications relating to that number would have to be done using another legal authority such as FISA Title 1. Finally, the information is destroyed after five years.

The net result is that although we collect large volumes of metadata under this program, we only look at a tiny fraction of it and only for a carefully circumscribed purpose; to help us find links between foreign terrorists and people in the United States. The collection has to be broad to be operationally effective, but it's limited to non-content data that has a low-privacy value and is not protected by the Fourth Amendment. It doesn't even identify any individual. Only the narrowest, most important use of this data is permitted. Other uses are prohibited. In this way, we do protect both privacy and national security.

Now, some have questioned how the collection of a large volume of telephone metadata could comply with the statutory requirement that business records obtained be relevant to an authorized investigation. We're working to see what additional information we can declassify about the program including the actual court papers that have been filed, but I can give a broad summary of this legal basis here today.

First, it's important to remember that the authorized investigation that the statute speaks of is an intelligence investigation, not a criminal investigation, and I talked

about the difference between these before. The statute says that an authorized investigation has to be one that's conducted in accordance with guidelines approved by the Attorney General, and those guidelines allow the FBI to conduct an investigation into a foreign-terrorist entity if there is an articulable factual basis that reasonably indicates that the entity may have engaged in international terrorism or other threat to the national security, or may be planning or supporting such conduct.

In other words, we can investigate an organization, not merely an individual or a particular act, if there's a factual basis to believe that that organization is involved in terrorism. And in this case, the government's applications to the FISA court to collect telephony metadata have identified the particular terrorist entities that are the subject of the investigations.

Second, the standard of relevance required by this statute is not the standard that we think of in a civil or criminal trial under the rules of evidence. The courts have recognized that in other contexts, the term "relevance" can import an extremely broad standard. For example, in the grand jury context, the Supreme Court has held that a grand jury subpoena is proper unless "there is no reasonable possibility that the category of materials the government seeks will produce information relevant to the general subject of the grand jury's investigation." And in civil discovery, again the Supreme Court has said that relevance is "construed broadly to encompass any matter that bears on or that reasonably could lead to other matter that could bear on any issue that is or may be in the case."

So, in each of these contexts, the meaning of "relevance" is sufficiently broad to allow for subpoenas or requests for information that encompass large volumes of information in order to locate within those records a smaller subset of material that will be directly pertinent to actually used in furtherance of the investigation or the case. In

other words, the requester is not limited to obtaining only those records that he or she can specifically identify as potentially incriminating or pertinent to establishing liability because in order to identify such records, it's often necessary to collect a much broader set of records that might potentially bear fruit by leading to specific materials that could bear on the issue.

When it passed the business records provision, Congress made clear that it had in mind broad concepts of relevance such as these, and the telephony-metadata collection program meets this broad relevance standard because, as I explained earlier, the effectiveness of the queries allowed by the court under the strict limitations of this program, the queries that are based on reasonable and articulable suspicion. The effectiveness of these queries depends on collecting and maintaining the data against which the narrowly focused queries can be made. As in the grand jury and civil discovery contexts, the concept of relevance is broad enough to allow for the collection of information beyond that which ultimately turns out to be important to a terrorist-related investigation. While the scope of the collection at issue here is broader than might typically be required through a grand jury subpoena or civil discovery request, the basic principle is similar. The information is relevant because you need to have the broader set of records in order to identify within them the information that is actually important to a terrorism investigation when you make that query. And the reasonableness of this collection overall is reinforced by all of the stringent limitations I described above that the court imposes to ensure that the data is only used for that approved purpose.

I want to repeat that the conclusion, that the bulk-metadata collection is authorized under Section 215 is not that of the intelligence community alone. Applications to obtain this data have repeatedly been approved by numerous judges of

the FISA court, each of whom has determined that the application complies with all legal requirements. And Congress reauthorized Section 215 in 2009 and 2011 after the Intelligence and Judiciary Committees of both houses had been brief on the program, and after information describing the program had been made available to all members of Congress. In short, all three branches of government have determined that this collection is lawful and reasonable in large part because of the substantial protections we provide for the privacy of every person whose telephone number is collected.

The third program I want to talk about is Section 702 which is part of the FISA Amendments Act of 2008. Again, a little history is in order by way of background. Generally speaking, as I said before, Title 1 of FISA, or traditional FISA, governs electronic surveillance conducted within the United States for foreign intelligence purposes.

When FISA was first passed in 1978, Congress did not intend that it would regulate the targeting of foreigners outside of the United States for foreign intelligence purposes. This kind of surveillance was generally carved out of coverage under FISA by the way Congress defined electronic surveillance in the statute.

Most international communications in 1978 took place via satellite, so Congress excluded international radio communications from the definition of electronic surveillance covered by FISA even when the radio waves were intercepted in the United States unless the target of the collection was a U.S. person in the United States. But over time, that technology-base differentiation fell apart.

By the early 21st century, most international communications traveled over fiber optic cables, and thus were no longer international radio communications outside of FISA's reach. At the same time, there was a dramatic increase in the use of the Internet for communications purposes, including by terrorists. As a result, Congress's

original intention was frustrated. We were increasingly required to go to the FISA court to get individual warrants on a case-by-case basis to conduct electronic surveillance of foreigners overseas for foreign intelligence purposes. After 9/11, this burden began to degrade our ability to collect the communications of foreign terrorists.

Section 702 created a new, more streamlined procedure to accomplish this surveillance, and so Section 702 was not, as some have suggested, a de-fanging of the FISA court's traditional authority. Rather, it extended the FISA court's oversight to a kind of surveillance that Congress had originally placed outside of that oversight; a surveillance for foreign intelligence purposes of foreign XXXSIC 00:37:41 XXX overseas, and I want to state that this American regime imposing judicial supervision of a kind of foreign intelligence collection directed at citizens of other countries is a unique limitation that so far as I'm aware again, goes beyond what other countries require of their intelligence services when those services collect against persons who are not their own citizens.

The privacy and Constitutional interests implicated by collection under Section 702 fall between traditional FISA and metadata collection. On the one hand, we are collecting the full content of communications. On the other hand, we're not collecting that information in bulk, and we're only targeting non-U.S. persons outside of the U.S. for valid foreign intelligence purposes. On the other hand, the information involved is unquestionably of great importance for national security.

Collection under Section 702 is one of the most valuable sources of foreign intelligence that we have. So here again, the statutory scheme and the means by which we implement it are designed to allow us to collect this intelligence while providing appropriate protections for privacy. Under the statute, collection under Section 702 does not require individual judicial orders authorizing collection against each target. Instead,

the FISA court approves annual certifications submitted by the Attorney General and the director of National Intelligence that identify categories of foreign intelligence that can be collected subject to court-approved targeting procedures and minimization procedures.

The targeting procedures are designed to ensure that we target someone only if we have a valid foreign intelligence purpose, that we target only non-U.S. persons reasonably believed to be outside the United States, that we do not intercept totally domestic communications, and that we do not target any person outside the United States as a backdoor means of targeting someone inside the United States. These targeting procedures must be reviewed by the court to ensure that they're consistent with the statute and with the Fourth Amendment. In other words, the targeting procedures are a way of minimizing the privacy impact of this collection, both as to Americans and as to non-Americans by limiting the collection to its intended purpose.

Now, the concept of minimization procedure should be familiar to you by this point in my speech. They're the procedures that limit the retention and dissemination of information about U.S. persons. In the course of 702 collection, we may incidentally acquire the communications of Americans even though we're not targeting them. For example, if they talk to non-U.S. persons outside of the United States who are properly targeted for foreign intelligence collection. Some of these communications may be pertinent and some may not be.

But the incidental collection of non-pertinent communications is hardly unique to Section 702. It's common whenever you lawfully collect information whether it's by a criminal wiretap where the target's conversations with his friends or family may be intercepted or when we seize a terrorist's computer or address book, either of which is likely to contain non-pertinent information. In passing 702, Congress specifically

recognized this reality and required us to establish procedures to minimize the impact of this incidental collection on the privacy of persons.

So, how does Section 702 work in practice? As of today, there are certifications for several different categories of foreign intelligence. Let's say that the intelligence community gets information that a terrorist is using a particular e-mail address. NSA analysts take this e-mail address, and they look at the available data to assess whether the e-mail address would be a valid target under the statute in the certification, whether the e-mail address belongs to someone who is not a U.S. person, whether the person with the e-mail address is outside the United States, and whether targeting that e-mail address is likely to lead to the collection of foreign intelligence relevant to the certification. Only if all three of those requirements are met and validated by supervisors will the e-mail address be approved for targeting.

We don't randomly target e-mail addresses or collect all foreign individual's e-mails under Section 702. We target specific accounts because we're looking for foreign intelligence information, and even after a target is approved, the court-approved procedures require NSA to continue to verify that it's targeting decision is valid based on any new information it acquires.

Any communications that we do collect under Section 702 are placed in secure databases, again, with limited access. Trained analysts are allowed to use the data for valid foreign intelligence purposes, but the minimization procedures require that if a review of communication that they determine involves a U.S. person or information about a U.S. person, and they further determine that that communication has no foreign intelligence value and is not evidence of a crime, the communication must be destroyed. And in any case, conversations that are not relevant are destroyed after a maximum of five years. So, under Section F702, we have a regime that involves judicial approval of

procedures that are designed to narrow the focus of the surveillance and the use of the data.

I've outlined three different collection programs under three different provisions of FISA. I think they all reflect the framework I've described. In each case, we protect privacy by a multi-layered system of controls, not only on what we collect but on how we use what we collect; controls that are based on the nature and intrusiveness of the collection, but that take into account the ways in which that collection is useful to protect national security. But we do not simply set out a set of rules and hope that people will follow them.

There are substantial safeguards in place that help ensure that these rules are followed. These safeguards operate at several levels. The first is technological. The same technological revolution that has enabled this kind of intelligence collection and made it so valuable also allows us to place relatively stringent controls on it. For one thing, intelligence agencies can work with providers so that when they do provide us the information we're allowed to acquire under the relevant order, they don't provide additional information as well.

Second, we have secure databases to hold this data to which only trained personnel have access.

Finally, modern information-security techniques allow us to create an audit trail tracking who uses these databases and how so that we have a record that can enable us to identify any possible misuse. And I want to emphasize that there is no indication so far that anyone has defeated those technological controls and improperly gained access to databases containing people's communications. Documents such as the leaked business records secondary order are kept on other NSA databases that do

not contain this kind of collection information, and many more NSA personnel have access to those databases.

We don't rely solely on technology. NSA has an internal compliance officer whose job includes developing processes that al NSA personnel must follow to ensure they comply with the law. In addition, decisions about what telephone numbers we use as a basis for searching the telephone metadata are reviewed first within NSA and then by the Department of Justice. Decisions about targeting under Section 702 are reviewed first within NSA and then by the Department of Justice and by my office, the Office of the Director of National Intelligence, which has a dedicated civil liberties protection officer who actively overseas these programs.

For traditional FISA collection, the Department of Justice regularly conducts reviews to ensure that information collected is used and disseminated in accordance with the court approved minimization procedures. Finally, independent inspectors general also review the operation of these programs.

The point is not that any of these individuals is perfect. It's that you have more and more people from more and more different organizations overseeing the operation of the programs. It becomes less and less likely that unintentional errors will go unnoticed or that anyone will be able to misuse the information.

But there's more. In addition to this oversight by the Executive branch, there's considerable oversight by both the FISA court and the Congress. As I've said, the FISA court has to review and approve the procedures by which we collect intelligence under FISA to ensure that these procedures comply with the statute and the Fourth Amendment.

In addition, any compliance violation, no matter how large or small, has to be reported to the court. Improperly collected information generally must be deleted

subject only to some exceptions set forth in the court's orders, and corrective measures are taken and reported to the court until the court is satisfied.

And I want to correct, once again, the erroneous claim that the FISA is a rubber stamp. Some people assume that because the court approves almost every application, it does not give these applications careful scrutiny. In fact, the exact opposite is true. The judges and their professional staff review every application carefully. They often ask extensive and probing questions, seek additional information from the government or request changes before the application is ultimately approved. Yes, the court does approve the great majority of the applications at the end of this process, but before it does so, the process, its questions and comments, ensure that the application does comply with the law.

Finally, there's the Congress. By law, we're required to keep the Intelligence and Judiciary Committees informed about these programs including detailed reports about their operation and about compliance matters. We regularly engage with the Congress and discuss these authorities as we did this week to provide them information in furtherance of their oversight responsibilities. As I said before, when Congress re-authorized Section 215, and also when they re-authorized Section 702 in 2012, information was made available to every member of Congress by briefings and written materials describing these programs in detail.

In short, or in summary, perhaps, is a better word, the procedures by which we implement collection under FISA are sensible means of accounting for the changing nature of privacy in the information age. They allow the intelligence community to collect information that is important to protect our nation and its allies while protecting privacy by imposing appropriate limits on the use of that information. Much is collected, but access, analysis, and dissemination are subject to stringent controls and procedures.

This same approach making the extent of the nature of controls over the use of information vary depending upon the nature and sensitivity of that information is applied throughout our intelligence collection. Our intelligence collection has helped protect both our nation and its allies from a variety of threats.

We have robust intelligence relationships with many other countries. These relationships go in both directions, but it is important to understand that we cannot use foreign intelligence services to get around the limitations imposed by our laws, and we assume that other countries similarly expect their intelligence services to operate in compliance with their own laws. By working closely with these other countries, we have helped to ensure our common security. For example, while many of the details remain classified, we have provided the Congress a list of 54 cases in which the bulk metadata and Section 702 authorities have provided us information that helped us understand potential terrorist activity and even to disrupt it; from potential bomb attacks to material support for foreign terrorist organizations.

Forty-one of these fifty-four cases involve threats in other countries, including twenty-five in Europe alone. We were able, by virtue of our intelligence collection, to alert officials in these countries to these events and help them fulfill their mission of protecting their nations because of the intelligence capabilities we have.

I believe that our approach to achieving both security and privacy is effective and appropriate. It's been reviewed and approved by all three branches of government. It's consistent with the law and Constitution.

It is however, not the only way that we could regulate intelligence collection. Even before the recent disclosures occurred, the President said that we welcome a discussion about privacy and national security, and we're currently working to declassify more information about our activities to inform that discussion.

In addition, the Privacy and Civil Liberties Oversight Board, which is an independent body established by statute and charged with overseeing our counter-terrorism activities, has announced that it intends to provide the President and Congress a public report on the Section 215 and 702 programs including the collection of bulk metadata. The board met recently with the President who welcomed their review and committed to providing them all the materials that they'll need to fulfill their oversight and advisory function, and we've been doing that. We look forward to continuing to work with the board on this project.

But the discussion about these authorities can and should have taken place without the recent disclosures, which have brought into public view the details of sensitive operations that were previously discussed on a classified basis with the Congress and in particular with the committees that were set up precisely to oversee intelligence operations. The level of detail in the current public debate certainly reflects a departure from the historic public understanding that the sensitive nature of intelligence operations demanded a more limited discussion. Whether or not the value of the exposure of these details outweighs the cost to national security is now a moot point, but as the debate about our surveillance activities goes forward, I hope that my remarks today have helped to provide an appreciation of the efforts that have been made and will continue to be made to ensure that all of our intelligence activities comply with our laws and reflect our values.

Thank you very much. I'll be glad to take some questions now. I do want to caution that much of what we do in this area remains classified for good reason, so I'm not going to be able to talk much about other activities that have not been publicly disclosed or about some of the details even of the activities that we have disclosed. As I

said, we are working to declassify additional information, but until that declassification is made, I'm going to be restricted in what I can say. Thank you very much. (Applause)

MR. BENNETT: I'm going to ask a question or two of Bob before turning it over to the audience. Beyond the classified open foreign point that Bob made, just one more parameter. I suspect we have an audience of the utmost in decorum and politeness, but if you plan to ask Bob to blow the whistle on how the CIA faked the Apollo moon landing or something, I suspect he will politely decline to answer, but I may not be so polite.

But with that out of the way, I guess I have just a few quick questions before we turn it over to the audience, but I think both of them, bearing mostly on 215, but also on some of the other activities you mentioned.

You referred to a long-standing, I guess, wide-ranging buy-in about the Executive Branch's position on the relevance standard. It's been put forward repeatedly, the judges have endorsed it, Congress has endorsed it in various ways. Notwithstanding that, there's been controversy in the public about how this really drives its relevance and in some quarters of Congress as well about essentially disagreeing with that view. I understand that having that buy-in and having those remarks you've made, that puts forth one position, but if there's still that disagreement and some confusion, particularly in the public, why not proceed on the basis of a bulk-collection statute with simply more clear language that it permits this sort of activity?

MR. LITT: That would certainly be one option. You'd have to make sure that it enables the kind of flexibility and operational agility that we need to conduct the collection. We don't think a new statute is necessary. We think we have the authority, but obviously, if Congress thinks a new statute is appropriate for this, Congress can provide that.

MR. BENNETT: I guess on that point as well, you referred to both the opinions. I think the papers underlying that interpretation and the declassification effort, if you're not changing the law, I suppose you're working on the back end as well. And everyone agrees there should be as much declassification as possible, but I think you mentioned the other day in your testimony for the House Judiciary Committee that referred to a comment by one of the judges on the FISA court, Judge Walton, who noted the intertwined nature of a lot of the facts and legal analyses for these, particularly the judicial opinions. Maybe, I can imagine that being true of the government's applications to the court, as well, but that sort of leaves us with this sort of -- wouldn't this be nice? It's going to be really hard, and not necessarily a clearer sense of where the declassification project is and maybe what we might see in the future. I'd just be curious to hear from you about whether you think we can really -- how much progress can really be made in that regard?

MR. LITT: I'm hopeful that we can make a lot of progress. I mean, one of the hurdles to declassification earlier was that the existence of the program was classified, and it's very hard to think about releasing an opinion that says that a particular program is legal if you're not going to disclose what the program is. Now that the program has been declassified, we're going back and we're relooking at these opinions, and I certainly am personally hopeful that we will be able to release court documents that will provide a greater visibility into exactly how these are dealt with.

MR. BENNETT: Do you think that will be more in terms of all of these activities; 702, 215, or do you think that might be more in the telephony-metadata neighborhood, so to speak?

MR. LITT: Well, I think we're looking across the entire spectrum of our activity. I think that, generally speaking, there has been considerably less concern about

the legal rationale for the 702 program than about the bulk-telephony metadata, but we're looking at all of our programs to see what can be declassified to inform the public debate.

MR. BENNETT: Okay, I'll take a few now.

MR. LITT: Oooh.

MR. BENNETT: Wow, that was a -- quite a response. Sir.

SPEAKER: Some quick questions. One, is there any other precedent of sections of the FISA court, which is a secret court, that works closely with the agency which is not subject to review over the legal basis of that? My second is don't foreign spies or intelligence people sort of understand that their phone calls and other communications are going to be intercepted anyway? So, what's the real harm to national security by the Snowden revelations?

MR. BENNETT: So, let me take the first one. It's important to go back to the history that I mentioned. This is not a court that exists to adjudicate disputes between individuals. This is a court that exists to oversee the Executive branch's acquisition of foreign intelligence information. So, the court is unprecedented in that sense. The fact that it's secret is a necessary consequence of the fact that it's overseeing secret activities. There are plenty of court proceedings that take place in secret in a variety of contexts, particularly when they implicate national security.

On your second point, if I can read my handwriting here -- oh, the fact of the matter is that we collect a lot of very valuable information pursuant to these programs. The fact of the matter also is that without going into a lot of detail, our adversaries have noticed these revelations. It's too early to tell yet whether it is going to have an impact, but there's no question that they have sat up and taken notice of specifically what has been released here, and the impact it has on their communications.

MR. BENNETT: Just before I call another person, if you do have any institutional affiliations or some other, please do identify yourself. I know your institutional affiliation. You're Allan, so you can go ahead and ask your question. This is Allan Friedman.

MR. FREIDMAN: Allan Friedman, the Brookings Institution. So first, thank you for your comments and for taking the time today. I wanted to talk about oversight, not just from a legal perspective, but from a policy perspective. You could help us appreciate the process, so as whether it's reported accurately or not, there are reports that say these companies are forced to compel data, and that is, since these are large international companies, that it had an impact on their trade relationships and on international trade discussions. So, there's this sort of broader impact question, and I'm wondering whether there's been a discussion as these programs expand, do you find new ways of gathering valuable intelligence? Is there some input from the American economic community, from the trade community, to understand the impact beyond just the legal questions?

MR. LITT: Well, again, the programs are classified, so we don't generally discuss them. Providers obviously have an opportunity to be heard. And we are always re-assessing is this program sufficiently valuable to continue it in light of the costs, and we're doing that again right now.

MR. BENNETT: Yes, sir. Russ.

MR BOWER: Thank you very much. Raymond Bower with Parr Global. A question in terms of, sort of say, use of the information maybe outside of the intelligence area, for example, in terms of the FCPA enforcement. Is that something that the DOJ can actually come to you and ask for, say, maybe if there is an idea of overseas bribery, can they come and use some of these powers to gain that information? Or if the

services come across that kind of information, can that be shared with the DOJ in terms of, say, enforcement of the FCPA?

MR. LITT: So, generally speaking, as I said, we can't task the collection of information for those purposes, and the Department of Justice can't ask us to collect evidence of that kind of a crime. Terrorism is one thing, but FCPA or other sorts of ordinary criminal activity, we cannot be tasked to collect that. If the intelligence agency uncovers evidence of any crime ranging from sexual abuse to FCPA, they tend to turn that information over to the Department of Justice, but the Department of Justice cannot task the intelligence community to do that.

MR. BENNETT: Shane Harris, I see you right there.

MR. HARRIS: Hi. Shane Harris, the *Foreign Policy* magazine. You said earlier that when NSA analysts are trying to determine whether they can target a particular e-mail address that they attempt to find out if it's a valid target by looking at whether it's send by a U.S. person, and whether that person was outside the U.S. Can you explain technically how they do that because determining those two things just by looking at an e-mail address, I understand is quite technically very difficult, so how do they actually do that?

MR. LITT: So, you're right. It is technically very challenging, and I guess one of the things I'm not at liberty to do is exactly talk about NSA's analytic tradecraft. But they do have a variety of information in databases that they can check. There may be other ways in which you can learn where an e-mail address is located, or whether it's associated with a U.S. person. But the rules require them to check a variety of databases to make that determination based on sort of standard analytic tradecraft.

MR. HARRIS: Just to follow up, are those databases also secured and protected in the same way --

MR. LITT: Well, it depends upon the contents of the database.

MR. HARRIS: Do you know what's in them?

MR. LITT: I don't know what's in every one of NSA's databases, no.

MR. BENNETT: Yes, ma'am.

SPEAKER: Hi, you mentioned with regard to the collection of business records that you don't think individuals have a legitimate expectation of privacy because they've already disclosed their information to a third party, but when so many of these tech companies have a monopoly on the services they provide, and when individuals can't receive those services without agreeing to all the terms, would you consider that meaningful consent as far as providing that information to a third party?

MR. LITT: I guess the relevant issue is not whether I would, but whether the courts would, and the courts do. The seminal cases in this involve things like bank records. Most of us need to have a bank account, and we disclose our bank records to the bank, and a subpoena to the bank can generate those records. Telephone companies used to be a monopoly, and the telephone-calling records were held not to be subject to a reasonable expectation of privacy. It's the same principle.

MR. BENNETT: Sir.

SPEAKER: At least one extraordinary assertion in your speech, and I wanted to make sure I understood it right. My understanding is that among the internal controls is a FISA audit process, and that process is triggered to examine some of these programs to see if they have violated some of these internal controls. It sounded like what you said was that that FISA audit process, these internal controls, have never found an instance where these authorities or those programs have reached beyond those authorities. I think one of the skepticisms about internal controls is that they often, just like internal affairs departments in police departments, may not look as hard as they

should. I mean, I think you could put some of that skepticism to rest if you could tell us, for example, how many FISA audits are done, say, last year, and reaffirm the fact that they have never found any misuse of these authorities in any program.

MR. LITT: So, first of all, I don't think that's what I said. In fact, I said that compliance violations have to be reported, and I think the premise of that is that there have been compliance violations. So, if I said something that led you to the conclusion that I was saying there's never been a violation, that's not what I meant to say.

You use the term FISA audits, but we have different audit regimes for different programs. There's an audit regime that is required for the 215 program. There's an audit regime that's required for the 702 program. There's an audit regime that's required for a Title 1 FISA and so on. I can't sit here and give you exact statistics on this. I just don't know them.

I do know that the Senate Intelligence Committee last year in a -- or the year before -- I can't remember when it was -- they issued a report in connection with the re-authorization of the Section 702 program, and in that report the majority of the Senate Intelligence Committee specifically noted that there has never been, under the 702 program, a finding of a willful violation of the law. There are absolutely occasions where people make mistakes, where there are technological problems that lead to errors, but there's not been a finding of somebody going in and willfully trying to evade the restrictions.

MR. BENNETT: I think timing-wise we've got maybe one more. Man in the front row right here.

MS. JENKS: Hi, I'm Laura Jenks with the *Associated Press*. I'm wondering if you can tell us a little information on how many times, if there have been

times, that some of the providers have objected or challenged some of the court orders to turn over the metadata, and whether it's telephony or some of the Internet records?

MR. LITT: So, I can't because those proceedings are still under seal. I guess there's one court proceeding that has recently been in the news where the FISA court has ordered us to review documents for declassification, and we're in the process of doing that. But in terms of other proceedings before the FISA court, those are still classified. Again, there's a lot of material that we're working on declassifying. We're trying to prioritize things that we think are sort of the greatest public interest, and we're trying to get that, but I can't answer the question.

MR. BENNETT: And I'll give myself maybe the last word. Are those things the highest priority?

MR. LITT: I think that to a certain extent, what's the highest priority is getting out fuller information about the programs about which partial information is already out.

MR. BENNETT: Bob, thank you very much.

MR. LITT: Thank you, Wells. (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or

counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016