

THE BROOKINGS INSTITUTION

FALK AUDITORIUM

U.S. INTELLIGENCE COMMUNITY SURVEILLANCE
ONE YEAR AFTER PRESIDENT OBAMA'S ADDRESS

Washington, D.C.

Wednesday, February 4, 2015

Moderator:

CAMERON F. KERRY
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow
Governance Studies
The Brookings Institution

Featured Speaker:

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

* * * * *

ANDERSON COURT REPORTING
706 Duke Street, Suite 100
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

P R O C E E D I N G S

MR. KERRY: Good afternoon and welcome to the Brookings Institution, both those of you who are here and those of you who are watching on the webcast. I'm Cameron Kerry; I'm the Ann R. and Andrew H. Tisch Visiting Fellow here at the Brookings Institution and it's my pleasure not only to welcome all of you, but to welcome Bob Litt today.

Before I introduce Bob let me remind you to please silence your cell phones. You don't need to turn them off because we encourage you to tweet on these proceedings and you can use the #ODNI.

So this is not the first time that Bob has come to this platform at the Brookings Institution. He was one of the early confirmees in the Obama administration, part of the National Security team, and has been there now for more than five years at ODNI. I recall when I was part of the administration and the Snowden stories broke reaching out to Bob almost first thing to say that I thought as part of the response it was important to put as much out there in the public as possible to address what the real scope of surveillance is, and also to make clear what some of the measures that were being taken to limit that surveillance to provide oversight. And I recall Bob responding, "I'm trying." Well, for now the 18 months or more since then he has been in the middle of that response. And he came to Brookings in the summer of 2013 within less than two months after those stories began and began to lay out some of the facts, some of the administration's response, and it was really the first real substantive response on these issues. So we sort of book end some of that today. Since Bob was here in July of 2013 a lot has happened and he'll certainly describe some of that. But a year ago after the President himself and his administration and his cabinet were deeply engaged in these issues the President went to the Justice Department to announce steps being taken to

limit the Section 215 program, to strengthen some of the oversights on the Section 702(a), email collection, and also to announce that U.S. signals, intelligence activities must include appropriate safeguards for the personal information of individuals regardless of the nationality of the individual, to whom the information pertains, or where the individual resides, to extend to non U.S. persons equivalent protections to those for U.S. persons. Last fall the new Vice President for the Digital Single Market in the European Union, Vice President Andrus Ansip, told the Parliament that this was a remarkable speech, a really strong political statement; that we've waited for that kind of statement during the last 10 years, but we did not get that kind of statement from the United States. But now there is a clear political guideline and we will see whether Americans are able to make this guideline, this principle, a reality.

So I'm pleased now to invite Bob to come and tell us about what has been done to implement the President's policy declaration in Presidential Policy Directive 28 in his surveillance speech, and what has been done to make the principles a reality. Bob, welcome back. (Applause)

MR. LITT: Thank you for that nice introduction, Cam. As Cam said a year and a half ago in July 2013 I gave a speech here; it was called Privacy, Technology, and National Security. The speech was just about a month after the classified documents that Edward Snowden had stolen began appearing in the press, at a time when people in the United States and around the world were raising questions about the legality and the wisdom of our signals intelligence activities.

My speech had several purposes. First, I wanted to set out the legal framework under which we conduct signals intelligence and the extent of oversight of that activity by all branches of government. Second, I wanted to explain how we protect both privacy and national security in a changing technology and security environment, and in

particular how we protect privacy through robust restrictions on the use we can make of the data we collect. And, third, I wanted to demystify and correct misapprehensions about the two programs that had been the subject of the leaks, and to commit the intelligence community to greater transparency going forward.

I began that speech by noting the huge amount of private information that we all expose today through social media, electronic commerce, and so on, but I acknowledged that giving the government access to that same kind of information worries us a lot more, with good reason because of what the government has the power to do with that information. So I suggested that we should address that problem directly. And in fact I said we can and we do protect both privacy and national security by a regime that puts limits not only on collection, but also restricts access to and use of the data we collect based on factors such as the sensitivity of the data, the volume of the collection, how it was collected, and the reason for which it was collected. And it backs up those restrictions with technological and human controls and auditing. And this approach has been largely effective. The information that has come out in the year and a half since my speech, both licitly and illicitly has validated the statement I made then. While there have been technological challenges and human error in our current signals intelligence activities there has been no systematic abuse or misuse akin to the very real illegalities and abuses of the 1960s and 1970s.

Well, you may have noticed that my speech did not entirely put the public concerns to rest. Questions have continued to be asked and we have continued to try to address them. And as Cam mentioned just over a year ago President Obama gave a speech about surveillance reform and issued Presidential Policy Directive 28, or PPD-28.

The pPresident reaffirmed the critical importance of signals intelligence activity to protect our national security and that of our allies against terrorism and other threats, but he took

note of the concerns that had been raised and he directed a number of reforms to -- and I'm quoting here -- "Give the American people greater confidence that their rights are being protected even as our intelligence and law enforcement agencies maintain the tools they need to keep us safe" as well as to provide "ordinary citizens in other countries confidence that the United States respects their privacy too."

The intelligence community has spent the year since the President's speech implementing the reforms he set out as well as many of the recommendations of the Privacy and Civil Liberties Oversight Board, or PCLOB, and the President's review group on intelligence and communications technology. And I just note in passing that last week the PCLOB issued a report finding that we have in fact made substantial progress toward implementing the great majority of its recommendations. We've also consulted with privacy groups, industry, Congress, and foreign partners. In particular we have a robust ongoing dialogue with our European allies and partners about privacy and data protection. We participated in a wide variety of public events at which reform proposals have been discussed and debated. And yesterday the Office of the Director of National Intelligence released a report detailing the concrete steps that we've taken so far along with the actual agency policies that implement some of those reforms.

What I'd like to do today is drill down a little bit on what we've done in the last year, and in particular explain how what we've done is responsive to some of the concerns that had been raised about our surveillance activities. I want to begin by laying out some premises that I think are commonly agreed on and that should frame how we think about signals intelligence.

The first is that we still need to conduct signals intelligence. As the President said in his speech last year, the challenges posed by threats like terrorism and proliferation and cyber attacks are not going away anytime soon. If anything as

recent events show, they are growing. Signals intelligence activities play an indispensable role in how we learn about and protect against these threats. Second, to be effective our signals intelligence activities have to take account of the changing technological and communications environment. Fifty years ago we could more easily isolate the communications of our target. The paradigm of electronic surveillance back then was two alligator clips on the target's telephone line. Today digital communications are all mingled together and traverse the globe. The communications of our adversaries are not separate and easily identified streams, but a part of irrelevant conversations and that creates new challenges for us. Third, it's critical to keep in mind that signals intelligence like all foreign intelligence is fundamentally different from electronic surveillance for law enforcement purposes. In a typical law enforcement context a crime has been or is about to be committed and the goal is to gather evidence about that particular crime. Intelligence on the other hand is often an effort to find out what is going to happen so that we can prevent it from happening, or simply to keep policy makers informed. This means that we cannot limit our signals intelligence activities only to targeted collection against specific individuals who we've already identified. We have to try to uncover threats or adversaries of which we may as yet be unaware, such as hackers seeking to penetrate our systems, or potential terrorists, or people supplying nuclear materials to proliferators. Or we may simply be seeking information to support the nation's political leadership in the service of other foreign policy interests. Fourth, we can also agree that in part because of the considerations I've just articulated signals intelligence activities can present special challenges to privacy and civil liberties. The capacity to listen in on private conversations or to read online communications if not properly limited and constrained could impinge on legitimate privacy interests or could be misused for improper purposes. Finally, as the President also said, "For our intelligence

community to be effective over the long haul we must maintain the trust of the American people and people around the world."

So although we must continue to conduct signals intelligence activities to protect our national security and those of others we need to do so in a way that is consistent with our values, that treats all people with dignity and respect, that takes account of the concerns that people have with the potential intrusiveness of these activities, and that ultimately provides reassurance to the public that they are conducted within appropriate limits and oversight.

So with these premises let me address some of the concerns that people have raised about our signals intelligence activities. I want to first start with the issue of transparency, both because it's something I care about deeply and because our commitment to transparency is what enables me to explain the other changes I want to talk about today. One of the biggest challenges that we faced over the last year and a half is that to a great extent our intelligence activities have to be kept secret. The public does not know everything that's done in its name and that has to be so. If we reveal too much about our intelligence activities we will compromise the capability of those activities to protect the nation. And I want to reiterate what I've said before, there have been significant benefits from the recent public debate, but the leaks have unquestionably caused damage to our national security, damage whose full extent we will not know for years. We've seen public posting clearly talking about the disclosures. One example is an extremist who advised others to stop using a particular communications platform because the company that provided that platform which had been discussed in the leaked documents was, "Part of NSA." So as I said we're not going to know for a long time how much damage we've suffered, but we have suffered damage. And yet the intelligence community, from the Director of National Intelligence on down recognizes

that with secrecy inevitably come both suspicion and the possibility of abuse. I and many others firmly believe that there would have been less public outcry from the leaks of the last year and a half if we had been more transparent about our activities beforehand. In fact as we've been able to release more information I think it's helped to allay some of the misimpressions people have had about what we do. And so we have committed ourselves to disclosing more information about our signals intelligence activities when the public interest in disclosure outweighs the risk to national security. Some examples, we've declassified thousands of pages of court filings, opinions, procedures, compliance reports, congressional notifications, and other documents. We've released summary statistics about our use of surveillance authorities, and we've authorized providers to release aggregate information as well. Representatives of the intelligence community have appeared and spoken in numerous public forums such as this one. We've also changed the way we disclose information to enable greater access by establishing a tumbler account where we post declassified documents, official statements, and other materials. It's called IC on the Record. Finally, we've developed and issued principles of transparency to apply to all of our intelligence activities going forward.

The process of transparency is never going to move as quickly as we would like. Public interest declassification requires a meticulous review to ensure that we don't inadvertently release information that needs to remain classified, and we have limited resources to devote to that task. The same people who review documents for this kind of discretionary declassification also have to review thousands of documents implicated by FOIA requests with judicial deadlines, and all this on top of their day job of actually working to keep us safe. Nonetheless we recognize the importance of transparency and are committed to continue it.

In general our efforts of transparency have focused and will continue to

focus on enhancing the public's overall understanding of the intelligence community's mission and how we accomplish that mission while continuing to protect specific targets of surveillance, specific means by which we conduct surveillance, specific partnerships, specific intelligence we gather. It's particularly important that we give the public greater insight into the laws and policies that we operate under and how we interpret those authorities, into the limits we impose on our activities, and into our oversight and compliance regime. I hope that our continuing efforts of transparency will demonstrate to the American people and the rest of the world that our signals intelligence activities are not arbitrary and are conducted responsibly and pursuant to law.

Now one persistent but mistaken charge in the wake of the leaks has been that our signals intelligence activity is overly broad, that it's not adequately overseen, and it is subject to abuse; that in short NSA collects whatever it wants. This is and always has been a myth. But in addition to greater transparency about what we do we've taken a number of concrete steps to reassure the public that we conduct signals intelligence activity only within the scope of our legal authorities and applicable policy limits. To begin with, in PPD-28 the President set out a number of important general principles that govern all of our signals intelligence activities. The collection of signals intelligence must be authorized by statute or presidential authorization and must be conducted in accordance with the Constitution and the law. Privacy and civil liberties must be integral considerations in planning signals intelligence activity. Signals intelligence will be collected only when there is a valid foreign intelligence or counter intelligence purpose. We will not conduct signals intelligence activities for the purpose of suppressing criticism or dissent. We will not use signals intelligence to disadvantage people based on their ethnicity, race, gender, sexual orientation, or religion. We will not use signals intelligence to afford a competitive commercial advantage to U.S. companies

and business sectors. And our signals intelligence activity must always be as tailored as feasible, taking into account the availability of other sources of information.

In addition to these general principles the President directed that we set up processes to ensure that we adhere to them and that we have appropriate policy review of our signals intelligence collection. I want to spend a little time talking about what these processes are, how it is that we try to ensure that signals intelligence is collected only in appropriate circumstances. And you will forgive me if I get down a little bit into the weeds on this because I think it's important for people to understand.

To begin with neither NSA nor any intelligence agency decides on its own what to collect. Each year the highest priorities for our foreign intelligence collection are set by the President after an extensive and formal interagency process. And as a result of PPD-28 going forward the rest of our intelligence priorities are also reviewed and approved through a high level interagency process. As a result overall this process will ensure that all of our intelligence priorities are set by senior policy makers who are in the best position to identify our foreign intelligence requirements and that those policy makers take into account not only the potential value of intelligence collection, but also the risks of that collection, including the risks to privacy, national economic interests, and foreign relations. Now the DNI, the Director of National Intelligence, then translates these priorities into a document called the National Intelligence Priorities Framework, or the NIPF. Our intelligence community directive about the NIPF, which is ICD 204 and incorporates the requirements of PPD-28 is publicly available on our website. The NIPF itself is classified, but much of what's in the NIPF is reflected annually in the DNI's unclassified Worldwide Threat Assessment. But the priorities that are set in the NIPF are at a fairly high level of generality, like the pursuit of nuclear and ballistic capabilities by particular foreign adversaries, the effects of drug cartel corruption in a particular country,

human rights abuses in identified countries. And these priorities apply not just to signals intelligence, but to all our intelligence activities. So how do the priorities that are set in the NIPF get translated into actual signals collection activities?

The organization that's responsible for doing this is called the National Signals Intelligence Committee, or SIGCOM. We have to have an acronym for everything -- it's the SIGCOM. It operates under the auspices of the Director of the National Security Agency who's designated by Executive Order 12333 as what we call the Functional Manager for Signals Intelligence, responsible for overseeing and coordinating signals intelligence activity across the intelligence community under the oversight of the Secretary of Defense and the DNI. The SIGCOM has representatives from all elements of the intelligence community, and as we fully implement PPD-28 we'll also have full representation from other departments and agencies with a policy interest in signals intelligence.

All departments and agencies that are consumers of signals intelligence submit their request for collection to the SIGCOM. The SIGCOM then reviews these requests, ensures that they are consistent with the NIPF, and assigns them priorities using criteria such as can SIGINT provide useful information in this case. Perhaps imagery or human sources would be better or more cost effective sources to address this particular requirement. How critical is the information need? Generally if it's a high priority in the NIPF it will be a high SIGINT priority. What type of SIGINT could we direct to collect this information? We collect different kinds of signals intelligence. There's what we commonly think of which is communications intelligence, but there's also collection against foreign weapons systems which is called FISINT, and there's other foreign electronic collection which we call ELINT. Is the collection as tailored as feasible or should there be time focus or other limitations on it? And our signals intelligence

requirements also require explicit consideration of other factors. Is the target of collection or the methodology used to collect particularly sensitive? If so it will require review by senior policy makers. Will the collection present an unwarranted risk to privacy and civil liberties regardless of nationality, and should there be additional dissemination and retention safeguards to the information we collect in order to protect privacy or national security interests?

So at the end of the SIGCOM process a limited number of trained NSA personnel take the priorities that the SIGCOM has validated and research and identify specific selection terms, such as telephone numbers or email addresses that are expected to be able to collect foreign intelligence responsive to these priorities. Any selector has to be reviewed and approved by two persons before it's entered into NSA's collection system. Even then, however, whether and when collection takes place will obviously depend on additional consideration such as the availability of appropriate collection resources. And of course when collection is conducted pursuant to the Foreign Intelligence Surveillance Act we have to apply additional restrictions approved by the Court.

So that's the process by which we ensure that signals intelligence collection targets reflect valid and important foreign intelligence needs. But as is typically the case with our signals intelligence activities we don't simply set rules and processes at the front end, but we have mechanisms to ensure that we are complying with those rules and processes. Cabinet officials are required to validate the SIGINT requirements every year. NSA checks the targets that they're collecting against throughout the collection process to determine if they are in fact providing valuable intelligence responsive to the priorities, and they'll stop collection against targets that are not. In addition all selection terms are reviewed annually by supervisors. Based on a recommendation by the

President's Review Group, the DNI has established a new mechanism to monitor the collection and dissemination of signals intelligence that is particularly sensitive because of the nature of the target or the means of collection to ensure that it is consistent with determinations of policy makers. And finally ODNI annually reviews the IC's allocation of resources against the NIPF priorities and against the intelligence mission as a whole. This review includes assessment of the values of all types of intelligence collection, including SIGINT, and looks both backwards, how successful have we been at achieving the goals that we set, and forward, what are we going to need in the future. And this process overall helps ensure that our SIGINT resources are applied only to the most important national intelligence priorities.

The point I want to make with this perhaps excessively detailed description is that the intelligence community does not decide on its own what conversations to listen to, nor does it try to collect everything. Its activities are focused on priorities set by policy makers through a process that involves input from across the government, and that is overseen within the government both by ODNI and the Department of Defense, and through extensive processes within NSA. The processes put in place by PPD-28, which are described in the report we issued yesterday, have further strengthened this oversight to ensure that our signals intelligence activities are conducted for appropriate foreign intelligence purposes and with full consideration of the risks of collection as well as the benefits.

Now one of the principle concerns that has been raised both here and abroad is with bulk collection. Bulk collection is not the same thing as bulky collection. Even a narrowly targeted collection program can collect a great deal of data; rather bulk collection as we use it generally refers to collection that is not targeted by the use of terms such as a person's phone number or email address. We do bulk collection for a

number of reasons, although like all of our intelligence activities bulk collection always must be for a valid foreign intelligence or counter intelligence purpose. In some circumstances, for example, it may not be technically possible to target a specific person or selector. In other circumstances we need to have a pool of data to review as circumstances arise, data which might otherwise not be available because it would have been deleted or overwritten. One of the things we use metadata for, for example, is to help identify targets for more intrusive surveillance. But because bulk collection is not targeted it often involves the collection of information that ultimately is not of foreign intelligence value, along with information that is, and it's therefore important that we regulate it appropriately.

We've taken a number of steps to provide appropriate and transparent limits on our bulk collection activities. First, agency procedures governing signals intelligence now explicitly provide that collection should be targeted rather than bulk whenever practicable. Second, the President in PPD-28 required that when we do collect signals intelligence in bulk we can only use it for one of six enumerated purposes, which I can paraphrase as countering espionage and other threats from foreign powers, counter terrorism, counter proliferation, cyber security, protecting our forces, and combating transnational criminal threats. We cannot take information collected in bulk and troll through it for any reason we please. We have to be able to confirm that we are using it for one of the six specified purposes. Agencies that have access to signals intelligence collected in bulk have incorporated these limitations in procedures governing their use of signals intelligence, which we released yesterday. This is not a meaningless step. It means that violations of those restrictions are subject to oversight, and significant violations have to be reported to the DNI. Third, in PPD-28 the President directed my boss, the DNI, to study whether there were software based solutions that could eliminate

the need for bulk collection. The DNI commissioned a study from the National Academy of Sciences which was conducted by a team of independent experts; they issued their report a few weeks ago and it is publicly available. Summarizing it they concluded that to the extent the goal of bulk collection is as I said a moment ago to enable us to look backwards when we discover new facts, for example to see if a terrorist who is arrested overseas has ever been in contact with people in the United States. There are no software-based solutions today that could accomplish that goal, but that we could explore ways to use technology to provide more effective limits and controls on the uses we make of bulk data, and to more effectively target our collection. And I will return to technology toward the end of my remarks.

To be clear, the National Academy of Sciences' report doesn't purport to settle whether bulk collection is a good idea or whether it's valuable. It simply concludes that present technology does not allow other less intrusive ways of accomplishing the same goals that we can achieve today with bulk collection.

Finally, with respect to bulk collection, the President directed specific steps to address concerns about the bulk collection of telephone metadata pursuant to FISA Court Order under Section 215 of the USA Patriot Act. You will recall that this was the program that was set up to fix a gap identified in the wake of 9/11, to provide a tool that can enable us to identify a potential terrorist, confederates of foreign terrorists. I won't explain in detail this program and the extensive controls it operates under because by now most of you are familiar with it. There's a wealth of information available about it at IC on the Record. Some have claimed that this program is illegal or unconstitutional although the vast majority of judges who have considered it to date have determined that's lawful. People have also claimed that the program is useless because they say it's never stopped a terrorist plot. Well, we have provided examples where the program has

proved valuable. I don't happen to think that the number of plots foiled is the only metric to assess its value. It's more like an insurance policy which provides valuable protection even though you may never file a claim. And because the program involves only metadata about communications and is subject to very strict limitations and controls the privacy concerns that it raises while not nonexistent by any means, are far less substantial than they would be if we were collecting the full content of those communications.

Even so the president recognized the public concerns about this program and ordered that several steps be taken immediately to limit it. In particular, except in emergency situations, NSA must now obtain the FISA Court's advance agreement that there is a reasonable, articulable suspicion that a number being used to query the database is associated with a specific foreign terrorist organization. And the results than an analysts get back from a query are not limited to numbers in direct contact with the query numbers and numbers in contact with those numbers, what we call two hops instead of three as it used to be. Longer term as you know the president directed us to find a way to preserve the essential capabilities of the program without having the government hold the metadata in bulk. In furtherance of this direction we worked extensively with Congress on a bipartisan basis and with privacy and civil liberties groups on the USA Freedom Act. This was not a perfect bill. It went further than some proponents of national security would wish, and it did not go as far as some advocacy groups would wish. But it was the product of a series of compromise and if enacted it would have accomplished the president's goal. It would have prohibited bulk protection under Section 215 and other authorities, but it also would have authorized a new mechanism that based on the telecommunications providers' current practice in retaining telephone metadata would have preserved the essential capabilities of the existing

program. Having invested a great deal of time in those negotiations I was personally disappointed that the Senate failed by two votes to advance the bill. And with Section 215 sun-setting on June 1 of this year I hope that Congress acts expeditiously to pass the USA Freedom Act or another bill that accomplishes the president's goal.

Another set of concerns that people raised centered around the other program that was leaked, collection under Section 702 of the Foreign Intelligence Surveillance Act. Section 702 enables us to target non-U.S. persons located outside of the United States for foreign intelligence purposes with the compelled assistance of domestic communication service providers. Contrary to what some people claim this is not bulk collection. All of the collection is based on selectors such as telephone numbers or email addresses that we have reason to believe are being used by non U.S. persons abroad to communicate or receive foreign intelligence information. Again there's ample information about this program and how it operates on IC on the Record. Unlike the bulk telephone metadata program no one really disagrees that this program is an effective and important source of foreign intelligence information. Rather, the concerns about this statute, at least within the United States, have to do with the fact that even when we are targeting non U.S. persons we are inevitably going to collect the communications of some U.S. persons, either because they're talking to our foreign targets, or in some limited circumstances because we cannot technically separate the communications we're looking for from others. This is called incidental collection because we aren't targeting the U.S. person. And I want to stress that when Congress passed Section 702 it fully understood that this kind of incidental collection was going to occur. Some of this incidental collection may prove to be useful and important foreign intelligence information. To pick the most obvious example, if a foreign terrorist who we're targeting under Section 702 is giving instructions to a confederate in the United States, we need to be able to

identify this communication and follow up, even if we weren't targeting the U.S. person herself. But people have asked, and they are legitimate questions, what are we allowed to do with communications that aren't of foreign intelligence value but may be for example evidence of a crime, and to what extent should we be allowed to rummage through the database of communications we collect to look for communications of U.S. persons. Part of the problem was that the general public didn't even know what the rules governing our activities under Section 702 were. And so we have declassified and released yesterday the procedures for minimizing the collection, retention, and dissemination of U.S. persons under Section 702 of the CIA, FBI, and the NSA.

But to address these concerns further the pPresident in his speech directed the Attorney General and the DNI to "institute reforms that place additional restriction on government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702. And we're doing that. First, as the PCLOB recommended, agencies have new restrictions on their ability to look through 702 collections for information about U.S. persons. The agency's various rules are described in the report we issued yesterday and their procedures.

It's important to note that different agencies in the intelligence community have been charged by Congress and the pPresident with focusing on different intelligence activities. For example, NSA focuses on signals intelligence, CIA primarily collects human intelligence, and the FBI has a domestic law enforcement focus. Because the agencies' missions are different their internal governance and their IT systems have developed differently from one another. And so the specifics of their procedures differ from one another, but all of the procedures will ensure that information about U.S. persons incidentally collected pursuant to Section 702 is only made available

to analysts and agents when it's appropriate. We've also reaffirmed that intelligence agencies must delete communications that we acquire under Section 702 that are to, from, or about U.S. persons if those communications are determined to lack foreign intelligence value. And we strengthened oversight of that requirement. Finally, the government will use information acquired under Section 702 as evidence in a criminal case only in cases related to national security or for certain other enumerated serious crimes, and only when the Attorney General approves. And in that respect I just want to note that this morning's press reports that the Director of National Intelligence's General Counsel told reporters yesterday that we hadn't devised the list of crimes yet. The General Counsel for the Director of National Intelligence forgot that in fact we had. And so today I want to say that in fact the list of crimes other than national security crimes for which we can use Section 702 information about U.S. persons is crimes involving death, kidnapping, substantial bodily harm, conduct that is a specified offense against a minor as defined in a particular statute, incapacitation or destruction of critical infrastructure, cyber security, transnational crimes, or human trafficking. Other than those crimes we cannot use Section 702 information about an American in a case against that American. In short we have taken concrete steps to ensure that there are limits on our ability to identify and use information about U.S. persons that we incidentally collect pursuant to Section 702.

But a refrain that we often hear from our foreign partners is that our rules are focused only on protecting Americans and that we ignore the legitimate privacy interests of other persons around the world. The fact that we have strong protections for the rights of our citizens is hardly surprising and I am not going to apologize for it. Indeed the legal regimes of most if not all countries afford greater protection to their own citizens of residence than to foreigners outside of the country. Nonetheless it has never been

true that the intelligence community had a sort of open season to spy on foreigners around the world. We've always been required to limit our collection to valid intelligence purposes as I set out above. However, the president recognized that given the power and scope of our signals intelligence activities, we need to do more to reassure the world that we treat "All persons with dignity and respect regardless of their nationality and where they might reside", and that we provide appropriate protections for the "legitimate privacy interests of all persons in the handling of their personal information."

And so PPD-28 contains Section 4 which I happen to think is an extraordinarily significant step because it requires that we have express limits on the retention and dissemination of personal information about non U.S. persons collected by signals intelligence comparable to the limits that we have for U.S. persons. These rules are incorporated into agency procedures that we released yesterday and into another publicly available document, Intelligence Community Directive 203 which governs analytic standards in reporting.

With respect to retention we now have explicit rules that require that personal information about non U.S. persons that we collect through SIGINT must generally be deleted after five years unless comparable information about a U.S. person would be retained. And we've likewise prohibited the dissemination of personal information about non U.S. persons unless comparable information about U.S. persons could be disseminated. In particular -- and this is a very significant point -- SIGINT information about the routine activities of foreign persons is not considered foreign intelligence that could be disseminated by virtue of that fact alone unless it's otherwise responsive to an authorized foreign intelligence requirement.

And I want to stop and highlight that point because in the many discussions that I've had over the last year and a half with our foreign partners about our

signals intelligence activity, I've repeatedly made the point that we only collect and retain and disseminate information about foreign persons when it's valid foreign intelligence information. And they have come back at me and pointed out that the definition of foreign intelligence that we have in Executive Order 12333 includes information about "The capabilities, intentions, or activities of foreign persons." And so then they've said well that really provides no limitation at all because if it's about a foreign person it's considered foreign intelligence. And so the new procedures address this concern by making clear that just because an intelligence community officer has signals intelligence information about a foreign person does not mean that she can disseminate this as foreign intelligence unless there is some other basis to consider it valid foreign intelligence information responsive to one of the priorities that we set up before. In short for the first time our nation has instituted express and transparent requirements to take account of the privacy of persons who are not our citizens or residents in how we conduct some of our intelligence activities. These new protections are I think a demonstration of our nation's enduring commitment to respecting the personal privacy and human dignity of citizens of all countries.

There's much more that we've done over the last year, but I'm running short of time if indeed I haven't run over already. The administration has endorsed changes to the operation of the Foreign Intelligence Surveillance Court that were contained in the USA Freedom Act, not because the Court is a rubber stamp as some have charged. The documents that we have released over the last year and a half should make clear that it's not, but in order to reassure the public. These include creation of a panel of lawyers who can advocate for privacy interests in appropriate cases, and continued declassification and release of significant Court opinions. We're taking steps to limit the length of time that secrecy can be imposed on recipients of national security

letters. We're continuing to implement rules to protect intelligence community whistle blowers who report through proper channels. These steps are discussed more fully in the materials we released yesterday.

So where do we go from here. The pP President has directed that we report again in one year and we will do so. In the interim we will continue to implement the reforms that the pP President directed in PPD-28 and his speech. We'll declassify and release more information, we'll continue to institutionalize transparency, and we'll continue our public dialogue and dialogue with our foreign partners on these issues. We'll work with Congress to secure passage of the USA Freedom Act or something like that. And I hope that we'll be able to work together with industry to help us find better solutions to protect both privacy and national security.

One of the many ways in which Snowden's leaks have damaged our national security is by driving a wedge between government and providers and technology companies so that some companies that formerly recognized that protecting our nation was a valuable and important public service they could perform now feel compelled to stand in opposition... I don't happen to think that's healthy because I think that American companies have a huge amount to contribute to how we protect both privacy and national security. When people talk about technology in surveillance they tend to talk about either how technology has enabled the intelligence community to do all sorts of scary things, or on the other hand how technology can help protect us from all the scary things that the intelligence community can do.

There's a third role that technology can play, however, and that's to provide protections and restrictions on the national security apparatus that can provide assurance to Americans and people around the world that we are respecting the appropriate limits on intelligence activities while still protecting national security. This is

where the genius and the capabilities of America's technology companies could provide us invaluable assistance. And in this regard I'd like to point back to the National Academy of Sciences' report that I mentioned earlier. The last section of that report identifies a number of areas where they say technology could help us target signals intelligence collection more effectively, or could provide more robust transparent and effective protections for privacy, including enforceable limitations on the use of the data we collect. One particular challenge they mentioned is the spread of encryption. And in my view this is an important area where we should look to the private sector to provide solutions. I should emphasize here by the way that I'm speaking only for myself. Encryption is a critical tool to protect privacy, to facilitate commerce, and to provide security. And the United States government supports its widespread use. At the same time, the widespread of encryption that cannot be decrypted when we have the lawful authority to do so risks allowing criminals, terrorists, hackers, and other threats to avoid detection. As President Obama recently said, "If we get into a situation in which the technologies do not allow us at all to track someone that we're confident is a terrorist, that's a problem." I'm not a cryptographer, but I am an optimist. I believe that if our businesses, our scientists, and our academics put their mind to it they will find a solution that does not compromise the integrity of encryption technology, but that enables both encryption to protect privacy and decryption under lawful authority to protect national security.

And so with that final plea for assistance let me stop and take your questions, or take Cam's questions, or whatever is next on the agenda. Thank you.

(Applause)

MR. KERRY: Thank you. You warned me that this was going to be a lengthy speech.

MR. LITT: And I fulfilled my promise.

MR. KERRY: There's a lot to cover. I am still digesting all of the material that was released at 9:00 a.m. yesterday. You mentioned IC on the Record. Just to clarify that's a website?

MR. LITT: It's a tumbler website. A year and a half ago I had no idea what a tumbler was; but it's where we post the documents that we're releasing, speeches. There will probably be a link to this before the close of business today.

MR. KERRY: Great. And keep your eyes on Lawfare. There will be some digesting and summaries of what was put out. I want to come back to the issue of protection of foreign persons. And it does strike me that if you go back in history to sort of the first great wave of disclosures about surveillance, the domestic surveillance of Martin Luther King, of anti war activists, including by the way the current Secretary of State that --

MR. LITT: Friend of yours?

MR. KERRY: -- that sort of -- the response was to establish the basic FISA framework that we're now revisiting today, and cabin surveillance of U.S. persons, but to provide far more latitude internationally and that is and has been the international system. But we're now in a globalized world, we are in a world in which the speed and volume of the collection and analysis of information is beyond anything that was imagined at the time of FISA, and we're now addressing that. There are still some open issues. One is in the materials that was put out is the issue of redress for foreign citizens, their rights under the Federal Privacy Act. Another has been the sort of debate about articulating limits on foreign intelligence collection with people in the European side saying that we want a statement that will limit it to what is necessary and proportionate. That's the European legal framework. Under our legal framework and in the Fourth

Amendment the standard is reasonableness. I see this in some sense a debate about legal semantics. But how does PPD-28, the standard sort of been put into place address those questions?

MR. LITT: Well, in no particular order, one of the things obviously is that the degree to which we are transparent now about what we were doing I think now provides more insight into our signals collection activities than virtually any other country in the world affords into their collection activities. I think that the limitations on retention and dissemination of personal information about non U.S. persons address that. I think a significant point to mention is the requirement of PPD-28 that signals intelligence activity be as tailored as feasible taking into account the availability of other means of acquiring the same information and the risks of the collection. You mentioned the necessary and proportionate standard. That's a standard under European law. I don't think we can be expected to conduct our intelligence activities in accord with the European law anymore than we would expect Europeans to conduct their activities in accord with our law. At the same time as you noted I think there's a great deal of congruence between the concept of necessary and proportionate that underlie European law and the Fourth Amendment requirements and the principles that have been articulated in PPD-28. So I do think that there should be some comfort taken by this stage of the game that we're not in fact randomly roaming around listening to communications of burgers, finding out what they're going to have for lunch, but that we're doing appropriate foreign intelligence collection.

MR. KERRY: So we're running short on time so I do want to turn it to the audience, but one more question before we do that. So the existing authority of Section 215 expires in June. What happens if that sun sets?

MR. LITT: Good question. The President said that he wants to have a mechanism that preserves the essential capabilities of the bulk collection program that

we have now without the bulk collection. There's a proposal up there that would accomplish that and I'm hopeful that we will get that passed. If it sun sets, if it goes away, the program will end. We'll also lose other authorities that are important under the same section which have nothing to do with bulk collection whatsoever. So at this point we're still far enough away that I think we're not doing extensive contingency planning other than trying to map out the legislative way to get something passed that will accomplish the President's goals.

MR. KERRY: Questions. Over here.

MR. ROSS: Thank you so much. I'm Andreas Ross with the German newspaper *Frankfurter Allgemeine Zeitung*, so this is going to be even more about what those Europeans are asking you. Could you address would -- you already mentioned the question of redress accords for non U.S. persons, but also the question of selectors, whether for a Visa surveillance to be targeted, what kind of selectors can be used? You mentioned email addresses and phone numbers, but it seems to be the case that much more general selectors have also been used. Are any changed envisioned?

And if I may, looking forward after the Paris attacks there's obviously a whole new debate about exchange of information with the European partners. If you could go into specifics as to what is being searched and to what extent that might be tied to questions about the Visa waiver program as is being discussed in the Hill?

MR. LITT: There's a whole bunch packed into that. I'm not sure I'll be able to answer all of it. I will tell you that I'm not going to talk about specific information that we're exchanging with our foreign partners; that falls the wrong side of the line for me. I will say that before and after Paris we have a very, very robust intelligence relationship with many European countries in which I think they benefit extensively from our intelligence capabilities and the information we share with them.

On the issue of judicial redress, which Cam mentioned, the issue here is that the Privacy Act which Congress passed specifically applies only to United States persons; does not give any rights to non Americans. We are working on legislation right now that we are -- we're working on this with members of Congress -- I hope to see something introduced soon that will provide for certain categories of data, it will provide individuals who are not Americans the right to come into our Courts and seek judicial redress either to correct inaccurate information or for a willful improper disclosure. As I said I'm hopeful that we'll see that sometime in the next few weeks; that will actually be introduced in Congress. And we've been discussing this with representatives of the EU as well.

Your third point about selectors, I don't think it is correct that selectors under Section 702 are broad in the way that you suggest. I think that in general they are all very specific identifiers.

MR. KERRY: The gentleman in the back there had his hand up almost before we sat down here.

MR. BENNETT: I'm Brian Bennett from the *Los Angeles Times*. Thanks a lot for speaking about this publicly and answering questions. I wanted to talk about what's been called the so-called back door for collecting electronic data on U.S. citizens. And this is the queries of the 702 data. And my question is why a regular warrant or an emergency authorization considered too cumbersome for querying 702 data for U.S. persons?

MR. LITT: So I guess I'd start by saying that I think that's the wrong question. I think the right question is under what circumstances should the U.S. government be barred from reviewing information that it has lawfully collected. There are very few such circumstances. If your barber happens to be the target of a wire tap, we

don't need a warrant to find out if you're collected under that. We can just go in and look at it. If your barber happens to be an informant wearing a wire and talks with you, we don't need a warrant to search for your communications. If your barber's computer gets confiscated, we don't need a warrant to look at -- or he abandons it, we don't need a warrant to look at it for information about you. Generally speaking the rule is that if we lawfully acquire information we can search it. We actually restrict ourselves more than that in this case and I articulated some of the rules that we've put into place to ensure that we don't just randomly look through this information, but we do it only when there's a valid purpose for doing so. And they're a little complicated so I'll probably screw them up if I try to articulate them here, but they're in the materials that we released yesterday.

MR. BENNETT: I think what's at issue here is exactly what you've been addressing today which is the public trust, and there's been a presumption that the U.S. government in a criminal investigation or others doesn't query information about U.S. citizens unless there have been another set of eyes on it, either through a regular warrant or an emergency authorization and that doesn't seem to be the case on the settlement of two queries.

MR. LITT: I actually don't think that's right. I think that what's happened here is there has been a confusion of two concepts. One is when we're allowed to target somebody for collection and, yes, in that case we do need to have a warrant to do it. The other is when we collect information what can we do with it. And I promise you that the FBI has information that it's collected over the years in criminal cases and it does not need a warrant every time it goes back and reviews its files for information. So as I said I don't think the premise of your question is correct. I think there's been an effort to try to characterize what's going on here as a back door search, but I just don't think that's an accurate characterization at all.

MR. KERRY: Ben Wittes, "Mr. Lawfare."

MR. WITTES: Thanks for coming, Bob. You articulated I think for the first time a new set of limitations on the use of 702 data in criminal cases and you specified categories of crimes in which it would be permissible. I'm wondering (a) how big a change in practice does that require given the breadth of some of those categories, and (b) are you aware of any cases that have been brought criminally in the past that under the new policy the information would not have been able to be used?

MR. LITT: So it occurs to me by the way that when I gave that list of crimes people should understand that that is the list of crimes other than crimes with national security implications. So there are basically two buckets.

There have always been very strong practical considerations against the use of intelligence-derived information in criminal cases because if you use the intelligence information a criminal case you have to expose the capability, you have to litigate it, and it's something we always prefer to do. So there have always been pretty severe constraints against doing so and as a result of that there have been very, very few cases in which -- I don't know that there is any case in which information actually collected under Section 702 has been used. And I think there have not been even that many cases in which information derived from collection under 702 has been used. What this does ensure is that going forward now that the 702 program is public and some of those constraints will be lesser, we're only going to use it in the most serious kind of cases. For example, routine drug cases are not on there, white collar cases are not on there. There's a whole host of activities that are not included and I think generally speaking people would agree that the list we had is a list of serious crimes.

SPEAKER: I'm a student at American University. And I was just wondering due to the current political makeup of our Congress if you think that the

President's goals will actually materialize in legislation in Congress, and if not are there other security goals that you think will materialize in legislation?

MR. LITT: Well the last part is kind of a broad question so I'll just focus on the first part. I'm hopeful. It's still early on; we haven't really had an opportunity to engage with the Congress yet. Senator Leahy hasn't reintroduced his bill yet, but I am hopeful that we will be able to secure the votes necessary to move this bill or something that is close to it.

MR. MARKS: Joe Marks from POLITICO. Two quick things. One, you said that if there isn't legislation to renew 215 that the program will expire. There's been some talk that there might be ways to continue it in some way without that. Does this mean that the government will not take advantage of those?

And then second, on encryption you seem to suggest that this is something that businesses and the government can work together on fixing. It seems as if -- I mean that doesn't take account of the real difference between government's goal of gathering data and businesses' need to get customers abroad. And can you talk about that and has there been some discussion with the telecom community about this?

MR. LITT: So, on your first point as I said I don't think we've thought a lot about contingency plans. I think that there's obviously -- I don't think I'm revealing any deep secrets here -- there's obviously a somewhat more substantial political hurdle in saying yes Congress, we know you didn't reauthorize this but we're going to go ahead and do it anyway under this authority. I'm hopeful we never have to confront those issues.

On your second point I think you've made precisely the point that I was trying to make which is to say I don't think the interest should be imposed. Frankly I think that people around the world should be comfortable with the concept of a process that

gives them privacy and yet allows the government to protect them when it has the lawful authority to do so. I'm not talking about something that would sort of be an ability to sort of break open anybody's communication, but something that says okay, you can encrypt this, you can send this secure, but if we have lawful authority we have the ability to decrypt it. We're not the only country that wants that. Other countries have the same concerns and I think that this is something where I am concerned that the position that's being asserted is sort of an all or nothing thing. Either you have full encryption that nobody can break or you have no encryption whatsoever. As I said I'm not a cryptographer. I just have to believe that there's a middle ground there where we can provide people privacy reassurances and yet be able to protect them as well.

MR. RIDOUT: Tim Ridout from the German Marshall Fund. Thanks, Bob, for the talk. You mentioned institutionalizing transparency mechanisms, and just to get to your point earlier I agree that if there had been more transparency before the public outcry would have been much less, but as technologies change they create new possibilities as we've seen things we couldn't even have imagined even 15 years ago. So what institutional mechanisms are we working on so that when we sort of reach a new era of technology, whatever you want to call it, that we have these public debates about how to use these tools responsibly? Thanks.

MR. LITT: That's a good question. One of the things we did yesterday was we released the Principle of Transparency that the DNI has issued for across the intelligence community, and we are working on ways to sort of set up processes to implement them.

The specific question of what you do about future technologies is a tricky one because it implicates both sides of the transparency line that I was talking about. On the one hand to the extent that what you're talking about is new authorities, new

generalized capabilities, you're right, there needs to be a debate about that. On the other hand if you're talking about something which if you disclose it you lose it that creates a problem. Historically the way we've dealt with that in this country, the way we've sort of tried to balance the need for secrecy and privacy is through the oversight mechanisms of the intelligence committees in Congress who sort of serve as proxies for the people. And the fact of the matter is the intelligence committees knew everything that's come out in leaks here. All of these programs were known to them. In fact they were more broadly known within the Congress. And I think that there are going to be certain things which are going to have to be kept at the level of the intelligence committees and I think we all recognize that strong and vigorous oversight from those committees is really essential to try to recreate public trust.

MR. KERRY: A couple of more questions. In the back.

SPEAKER: Thank you very much. I'm Duran Fausa reporter of *El Pais*, a newspaper from Spain. I wanted to ask you a year after the President's speech if it has completely ended the monitoring of foreign leaders from countries that are allies and close partners of the U.S.? A *New York Times* article yesterday suggested that the programs in Mexico and Brazil have continued. If you could give me a bit of details on this. Thank you.

MR. LITT: So I'm not going to comment on any specific collection activities that may or may not be occurring. We did have an extensive process to review our collection and we have removed some prior targets for collection against whom we no longer collect. But in terms of more specifics than that, that gets to the kind of thing that I don't feel comfortable talking about.

SPEAKER: First, Bob, thank you for coming. My name is Harbrusch Goff; I'm with the American Bar Association. First, thank you for coming and doing this.

One of the things you mentioned is that you as a group would support FISA Court reform in some sense. Could you articulate what you at this point would like to see in that reform?

MR. LITT: Well, I think we supported the USA Freedom Act. And as I said there was a provision in there to have a panel of outside lawyers who would be available to the FISA Court to help advocate for privacy and appropriate cases. I think there was a provision for a greater transparency about FISA Court opinions. As I recall those are the two principle areas of Court reform that were in the USA Freedom Act and I think those would be appropriate.

MR. KERRY: We have time for one more question. You're the lucky question.

MR. STROBEL: Warren Strobel with Reuters. Bob, thanks for doing this. You mentioned earlier in your remarks about the possible benefits of transparency beforehand, and I take it you meant before the Snowden disclosures. I've been told there was actually a rather vigorous debate about whether to explain to the American people what was being done under Section 215. I'm just wondering if you can talk a little bit about that. I mean what happened? Was it deemed just too politically hard to do, did the NSA put its foot down, did it just not happen?

MR. LITT: So a short answer to that is no. I generally don't like to talk about internal deliberations and so I won't.

MR. STROBEL: So there was a debate?

MR. LITT: I don't talk about such matters.

MR. KERRY: There was one other gentleman. That was a short one. Any takers for the last one? Over here.

MR. ROSEMONT: Thanks very much. Hugo Rosemont from Kings

College, London. A grateful European for the greater protections. Thank you. And also just to ask about the public-private cooperation you mentioned and the difficulties around that and if I understood correctly some frustration personally potentially about that. I mean to what extent should there be more structure around this relationship? How can this relationship actually develop?

MR. LITT: That's a very good question. And it's a similar question to what your leaders have been raising as well. I think we just have to find ways to engage with them. I think there has to be a recognition of where do we have common interests, how can we move those forward, and I think there has to be -- I think we have to try to be transparent about it to the extent we can.

MR. KERRY: Well, Bob, I want to thank you for book ending this debate with your July 2013 appearance and then coming here today, and for all of the work that has gone into this.

MR. LITT: Thanks for hosting this, Cam.

MR. KERRY: And thank you all for coming.

(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