National Security Law Journal

Excerpt from Vol. 3, Issue 2 (Spring/Summer 2015)

Cite as:

Robert S. Litt, Remarks, *U.S. Intelligence Community Surveillance One Year After President Obama's Address*, 3 NAT'L SEC. L.J. 210 (2015).

© 2015 *National Security Law Journal*. All rights reserved.

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

REMARKS

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

The Hon. Robert S. Litt*

On February 4, 2015, Mr. Litt delivered remarks on the legal framework under which the Director of National Intelligence conducts signals intelligence.[1] Following is an edited version of his prepared remarks, presented in partnership with the Office of the Director of National Intelligence and the Brookings Institution.

A year and a half ago, in July 2013, I gave a speech here about Privacy, Technology and National Security. It was just about a month after classified documents stolen by Edward Snowden 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 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 extensive oversight of that activity by all three branches of Government.

---

* Second General Counsel of the Office of the Director of National Intelligence, 2009 to present.

[1] A video recording of these remarks is available online through the Brookings Institution at http://www.brookings.edu/events/2015/02/04-intelligence-community-surveillance-litt-kerry.

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.

Third, I wanted to demystify and correct misimpressions 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 by noting the huge amount of private information that we all expose today, through social media, e-commerce, and so on. But I acknowledged that government access to the same information worries us more—with good reason—because of what the government could do with that information. So I suggested we should address that problem directly. And in fact, I said, we can and do protect both privacy and national security by a regime that not only puts limits 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 that backs up those restrictions with technological and human controls and auditing. This approach has largely been effective. The information that has come out since my speech, both licitly and illicitly, has validated my statement 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've continued to address them. In particular, just over a year ago, President Obama gave a speech about surveillance reform, and issued Presidential Policy Directive 28 ("PPD-28"). The President 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 directed a

number of reforms to "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."[2]

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 ("PCLOB") and the President's Review Group on Intelligence and Communications Technologies. And I'd note in passing that the PCLOB last week issued a report finding that we have made substantial progress towards implementing the great majority of its recommendations. We've 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've 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 ("ODNI") released a report detailing the concrete steps we have taken so far, along with the actual agency policies that implement some of those reforms.[3] What I want to do today is drill down on what we have done in the last year, and in particular explain how we have responded to some of the concerns that have been raised in the last year and a half.

Let me begin by laying out some premises that I think are commonly agreed upon and that should frame how we think about signals intelligence. The first is that we still need to conduct signals intelligence activities. 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 any time soon."[4] If anything, as

[2] President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[3] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SIGNALS INTELLIGENCE REFORM (2015) [hereinafter ODNI REPORT], *available at* http://icontherecord.tumblr.com/ppd-28/.
[4] Obama, *supra* note 2.

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 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 are part of an ocean 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 the typical law enforcement context, a crime has been or is being 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 to keep policymakers informed. This means that we cannot limit our signals intelligence activities only to targeted collection against specific individuals whom we have 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 leadership in the service of other important foreign policy interests.

Fourth, we can also agree that—in part because of these considerations—signals intelligence activities can present special challenges to privacy and civil liberties. The capacity to listen in on private conversations or read online communications, if not properly limited and constrained, could impinge upon legitimate privacy interests, and 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."[5] So although we must continue to conduct signals intelligence activities to protect our national security, 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 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.

TRANSPARENCY

I want to start with the issue of transparency, both because it is something I care about deeply and because our commitment to transparency is what enables me to explain the other changes we have made. One of the biggest challenges that we have faced in responding to the events of the past 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 is 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 have said before—while there have been significant benefits from the recent public debate, the leaks have unquestionably caused damage to our national security, damage whose full extent we will not know for years. We have seen public postings clearly referencing the disclosures, such as an extremist who advised others to stop using a particular communications platform because the company that provided it, which had been discussed in the leaked documents, was "part of NSA."

And yet the Intelligence Community, from the Director of National Intelligence ("DNI") on down, recognizes that with secrecy inevitably come both suspicion and the possibility of abuse. I and

[5] Obama, *supra* note 2.

many others in the Intelligence Community 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. Indeed, as we have been able to release more information, it has helped to allay some of the mistaken impressions people have had about our intelligence activities.

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 from disclosure:

- We have declassified thousands of pages of court filings, opinions, procedures, compliance reports, congressional notifications and other documents.

- We have released summary statistics about our use of surveillance authorities, and have authorized providers to release aggregate information as well.

- Representatives of the Intelligence Community have appeared in numerous public forums—such as this one.

- We've also changed the way we disclose information to enable greater public access, by establishing *IContheRecord*, a tumblr account where we post declassified documents, official statements, and other materials.[6]

- Finally, we have developed and issued principles of transparency to apply to our intelligence activities going forward.

The transparency process will never 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 the task. The same people who review documents for discretionary declassification also have to review thousands of documents

[6] IC ON THE RECORD, http://icontherecord.tumblr.com/ (last visited May 15, 2015).

implicated by FOIA requests with judicial deadlines—and all this on top of their "day job" of actually working to keep us safe. But we recognize the importance of this task and are committed to continued greater transparency.

In general, our transparency efforts 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, and specific intelligence we gather. It's particularly important that we give the public greater insight into the laws and policies we operate under and how we interpret those authorities, into the limits we impose upon our activities, and into our oversight and compliance regime. I hope that our efforts at transparency will continue to 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.

LIMITATIONS ON SURVEILLANCE

One persistent but mistaken charge in the wake of the leaks has been that our signals intelligence activity is overly broad, that it is not adequately overseen and is subject to abuse—in short, that NSA "collects whatever it wants." This is and always has been a myth, but in addition to greater transparency we have 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 our signals intelligence activity:

- The collection of signals intelligence must be authorized by statute or Presidential authorization, and must be conducted in accordance with the Constitution and law.

- Privacy and civil liberties must be integral considerations in planning signals intelligence activities.

- Signals intelligence will be collected only when there is a valid foreign intelligence or counterintelligence 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.

- Our signals intelligence activity must always be as tailored as feasible, taking into account the availability of other sources of information.

The President also directed that we set up processes to ensure that we adhere to these restrictions, and that we have appropriate policy review of our signals intelligence collection. I want to spend a little time now talking about what these processes are—how we try to ensure that signals intelligence is only collected in appropriate circumstances. And you'll forgive me if I get a bit down into the weeds on this, but I think this is important for people to understand.

To begin with, neither NSA nor any other intelligence agency decides on its own what to collect. Each year, the President sets the nation's highest priorities for foreign intelligence collection after an extensive, formal interagency process. Moreover, as a result of PPD-28, the rest of our intelligence priorities are now also reviewed and approved through a high-level interagency policy process. Overall, this process ensures that all of our intelligence priorities are set by senior policymakers who are in the best position to identify our foreign intelligence requirements, and that those

policymakers take into account not only the potential value of the intelligence collection but also the risks of that collection, including the risks to privacy, national economic interests, and foreign relations.

The DNI then translates these priorities into the National Intelligence Priorities Framework, or "NIPF." Our Intelligence Community Directive ("ICD") about the NIPF, ICD 204, which incorporates the requirements of PPD-28, is publicly available on our website.[7] And while the NIPF itself is classified, much of it is reflected annually in the DNI's unclassified Worldwide Threat Assessment.

But the priorities in the NIPF are at a fairly high level of generality. They include topics such as the pursuit of nuclear and ballistic missile capabilities by particular foreign adversaries, the effects of drug cartel corruption in Mexico, and human rights abuses in specific countries. And they apply not just to signals intelligence, but to all intelligence activities. So how do the priorities in the NIPF get translated into actual signals intelligence collection?

The organization that is responsible for doing this is called the National Signals Intelligence Committee, or "SIGCOM." (We have acronyms for everything.) It operates under the auspices of the Director of the NSA, who is designated by Executive Order 12333 as what we call the functional manager for signals intelligence, responsible for overseeing and coordinating signals intelligence across the Intelligence Community under the oversight of the Secretary of Defense and the DNI. The SIGCOM has representatives from all elements of the community and, as we fully implement PPD-28, also will have full representation from other departments and agencies with a policy interest in signals intelligence.

All departments and agencies that are consumers of intelligence submit their requests for collection to the SIGCOM. The

[7] *Intelligence Community Directives*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives (last visited May 15, 2015).

SIGCOM reviews those 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 are better or more cost-effective sources of information to address the requirement.

- How critical is this information need? If it is a high priority in the NIPF, it will most often be a high SIGINT priority.

- What type of SIGINT could be used? NSA collects three types of signals intelligence: collection against foreign weapons systems (known as "FISINT"), foreign communications (known as "COMINT"), and other foreign electronic signals such as radar (known as "ELINT").

- Is the collection as tailored as feasible? Should there be time, focus, or other limitations?

And our signals intelligence requirements process also requires explicit consideration of other factors, namely:

- Is the target of the 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 . . .

- Are additional dissemination and retention safeguards necessary to protect privacy or national security interests?

Finally, at the end of the process, a limited number of trained NSA personnel take the priorities validated by the SIGCOM and research and identify specific selection terms, such as telephone numbers or email addresses, that are expected to collect foreign intelligence responsive to these priorities. Any selector must be reviewed and approved by two persons before it is entered into NSA's collection systems. Even then, however, whether and when actual collection takes place will depend in part on additional

considerations such as the availability of appropriate collection resources. And, of course, when collection is conducted pursuant to the Foreign Intelligence Surveillance Act, NSA and other agencies must follow additional restrictions approved by the court.

So that's how 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 just set rules and processes at the front end; we also have mechanisms to ensure that we are complying with those rules and processes.

Cabinet officials are required to validate their SIGINT requirements each year.

NSA checks signals intelligence targets throughout the collection process to determine if they are actually providing valuable foreign intelligence responsive to the priorities, and will stop collection against targets that are not. In addition, all selection terms are reviewed by supervisors annually.

Based on a recommendation from 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 the determinations of policymakers.

Finally, ODNI annually reviews the Intelligence Community's allocation of resources against the NIPF priorities and the intelligence mission as a whole. This review includes assessments of the value of all types of intelligence collection, including SIGINT, and looks both backward—how successful have we been in achieving our goals?—and forward—what will we need in the future?—and helps ensure that our SIGINT resources are applied to the most important national priorities.

The point I want to make with this perhaps excessively detailed description is that the Intelligence Community does not

decide on its own which conversations to listen to, nor does it try to collect everything. Its activities are focused on priorities set by policymakers, through a process that involves input from across the government, and that is overseen both within NSA and by the ODNI and Department of Defense. The processes put in place by PPD-28, which are described in the report we issued yesterday,[8] 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.

BULK COLLECTION

One of the principal 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 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 it must always be for a valid foreign intelligence or counterintelligence purpose. In some circumstances, it may not be technically possible to target a specific person or selector. In other circumstances, we need to have a pool of relevant data to review as circumstances arise, data which might not otherwise be available because, for example, it would have been deleted or overwritten. In particular, we can use metadata that we collect in bulk to help identify targets for more intrusive surveillance. But because bulk collection is not targeted, it often involves the collection of information that is ultimately not of foreign intelligence value along with information that is, and it is 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

[8] ODNI REPORT, *supra* note 3.

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, counterterrorism, counter-proliferation, cybersecurity, protecting our forces, and combating transnational criminal threats. We can't take information collected in bulk and trawl 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 must be reported to the DNI.

Third, in PPD-28, the President directed my boss, the Director of National Intelligence, 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.[9] To summarize, 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 arrested overseas has ever been in contact with people in the United States—there are no software-based solutions available 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 collection. I'll return to technology a bit later in my remarks. To be clear, this report doesn't purport to settle whether bulk collection is a good idea, or whether it is valuable; it simply concludes that present technology doesn't allow other, less intrusive ways of accomplishing the same goals we can achieve with bulk collection.

[9] NAT'L RESEARCH COUNCIL, NAT'L ACADS., BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS (2015), *available at* http://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options.

Finally, 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'll recall that this was the program set up to fix a gap identified in the wake of 9/11, to provide a tool that can identify potential domestic 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, but there is a wealth of information about it available at *IContheRecord*.[10]

Some have claimed that this program is illegal or unconstitutional, though the vast majority of judges who have considered it to date have determined that it is lawful. People have also claimed that the program is useless because they say it's never stopped a terrorist plot. While 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 it; it's more like an insurance policy, which provides valuable protection even though you may never have to file a claim. And because the program involves only metadata about communications and is subject to strict limitations and controls, the privacy concerns that it raises, while not non-existent, are far less substantial than 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 specific foreign terrorist organizations. And the results that an analyst actually gets back from a query are now limited to numbers in direct contact with the query number and numbers in contact with those numbers—what we call "two hops" instead of three, as it used to be.

[10] *Section 215 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD, http://icontherecord.tumblr.com/topics/section-215 (last visited May 15, 2015).

Longer term, the President directed us to find a way to preserve the essential capabilities of this 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 compromises, and if enacted it would have accomplished the President's goal: it would have prohibited bulk collection under Section 215 and several other authorities, while authorizing a new mechanism that—based on 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 this bill, and with Section 215 sunsetting on June 1 of this year, I hope that the Congress acts expeditiously to pass the USA FREEDOM Act or another bill that accomplishes the President's goal.

INCIDENTAL COLLECTION

A second set of concerns 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 communications service providers. Contrary to some claims, this is not bulk collection; all of the collection is based on identifiers, 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 is ample information about this program and how it operates on *IContheRecord*.[11]

[11] *Section 702 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD, http://icontherecord.tumblr.com/topics/section-702 (last visited May 15, 2015).

Unlike the bulk telephone metadata program, no one really disagrees that Section 702 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 U.S. persons, either because U.S. persons are talking to the foreign targets, or, in some limited circumstances, because we cannot technically separate the communications we are looking for from others. This is called "incidental" collection because we aren't targeting the U.S. persons, and I want to emphasize that when Congress passed Section 702 it fully understood that incidental collection would occur.

Some of this incidental collection may be important foreign intelligence information. To pick the most obvious example, if a foreign terrorist who we are targeting under Section 702 is giving instructions to a confederate in the U.S., we need to be able to identify that communication and follow up—even if we weren't targeting the U.S. person herself. But people have asked: 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 know what the rules governing our activities under Section 702 were. And so we have declassified and released the CIA, FBI, and NSA procedures for minimizing the collection, retention, and dissemination of information about U.S. persons under Section 702.

But to address these concerns further, the President in his speech directed the Attorney General and the DNI to "institute reforms that place additional restrictions on government's ability to retain, search, and use in criminal cases, communications between

Americans and foreign citizens incidentally collected under Section 702."[12] We are doing so.

First, as the PCLOB recommended, agencies have new restrictions on their ability to look through 702 collection for information about U.S. persons. The agencies' various rules are described in the report we issued yesterday.[13] It's important to note that different agencies in the Intelligence Community have been charged by Congress and the President with focusing on different intelligence activities. For example, NSA focuses on signals intelligence; CIA collects primarily human intelligence; and FBI has a domestic law enforcement focus. Because these 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 somewhat. But they will all ensure that information about U.S. persons incidentally collected pursuant to Section 702 is only made available to analysts and agents when appropriate.

Second, we have reaffirmed that intelligence agencies must delete communications acquired pursuant to Section 702 that are to, from, or about U.S. persons if the communications are determined to be of no foreign intelligence value, and we have strengthened oversight of this requirement.

Third, the Government will use information acquired under Section 702 as evidence against a person in a criminal case only in cases related to national security or for certain other enumerated serious crimes,[14] and only when the Attorney General approves. In

[12] Obama, *supra* note 2.

[13] ODNI REPORT, *supra* note 3.

[14] In his remarks as delivered, Mr. Litt went on to describe the "enumerated serious crimes" for which the U.S. Government will use information acquired under Section 702 as evidence against a person. Under the new policy, in addition to any other limitations imposed by applicable law, including FISA, any communication to or from, or information about, a U.S. person acquired under Section 702 of FISA shall not be introduced as evidence against that U.S. person in any criminal proceeding except (1) with the prior approval of the Attorney General and (2) in (A) criminal proceedings related to national security (such as terrorism, proliferation, espionage, or cybersecurity) or (B) other prosecutions of crimes involving (i) death; (ii)

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 under Section 702.

PROTECTION FOR NON-U.S. PERSONS

But one refrain that we often hear from some of 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'm not going to apologize for it. Indeed, the legal regimes of most if not all nations afford greater protection to their own citizens or residents than to foreigners abroad. Nonetheless, it was never true that the Intelligence Community had a sort of "open season" to spy on foreigners around the world; we have always been required to limit our activities to valid intelligence purposes, as I outlined 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," [15] and that we provide appropriate protection for the "legitimate privacy interests [of all persons] in the handling of their personal information."[16] And so Section 4 of PPD-28, which I think is an extraordinarily significant step, 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 we have for U.S. persons. These rules are incorporated into the agency procedures that we released yesterday, and into

kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 U.S.C. § 16911; (v) incapacitation or destruction of critical infrastructure as defined in 42 U.S.C. § 5195c(e); (vi) cybersecurity; (vii) transnational crimes; (or (vii) human trafficking.

[15] Obama, *supra* note 2.

[16] *Id.*

another publicly available Intelligence Community Directive, ICD 203, governing analytic standards in reporting.[17]

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 could be retained. And we have likewise prohibited the dissemination of personal information about non-U.S. persons unless comparable information about U.S. persons could be disseminated. In particular, "SIGINT information about the routine activities of a foreign person" would not be considered foreign intelligence that could be disseminated by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement.

This last point in particular is, in my opinion, a big deal. Over the last year and a half, in defending our signals intelligence activity, we have repeatedly said that we protect personal information because we only disseminate valid foreign intelligence information. But many have expressed concerns that our limitations on dissemination are neither transparent nor enforceable. Moreover, people have noted that the definition of "foreign intelligence" includes information about "the capabilities, intentions, or activities of . . . foreign persons," and have therefore questioned whether the foreign intelligence requirement imposed any meaningful limits to protect the privacy of foreign persons. The new procedures address this concern, by making clear that just because an Intelligence Community officer has signals intelligence information about a foreign person doesn't mean she can disseminate it as foreign intelligence, unless there is some other basis to consider it foreign intelligence information.

In short, for the first time, we have instituted express and transparent requirements to take account of the privacy of people outside our nation in how we conduct some of our intelligence activities. These new protections are, I think, a demonstration of our

[17] *See Intelligence Community Directives*, *supra* note 7.

nation's enduring commitment to respecting the personal privacy and human dignity of citizens of all countries.

OTHER ACTIVITIES/GOING FORWARD

There is much more that we have done but I am running short of time. 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 charged—the documents we have released make clear that it is 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 are taking steps to limit the length of time that secrecy that can be imposed on recipients of National Security Letters. We are continuing to implement rules to protect Intelligence Community whistleblowers 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 President has directed that we report again in one year. In the interim, we will continue to implement the reforms that the President directed in PPD-28 and his speech. We will declassify and release more information, we will continue to institutionalize transparency, and we will continue our public dialogue on these issues. We will work with Congress to secure passage of the USA FREEDOM Act or something like it.

And I hope that we will 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 the government and providers and technology companies, so that some companies that formerly recognized that protecting our nation was a valuable and important public service now feel compelled to stand in opposition. I don't think that is 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 and surveillance, they tend to talk either about how technology has enabled the Intelligence Community to do all sorts of scary things, or about how technology can protect you from the scary things that the Intelligence Community can do. But there's a third role that technology can play, and that is to provide protections and restrictions on the national security apparatus that can assure 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 capabilities of American technology companies can provide invaluable assistance.

In this regard, I'd like to point you to the National Academy of Sciences report that I mentioned earlier.[18] The last section of their report identified a number of areas where technology could help us target signals intelligence collection more effectively, and provide more robust, transparent and effective protections for privacy, including enforcing limitations on the use of data we collect. One 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. And I should emphasize that I am speaking for myself here.

Encryption is a critical tool to protect privacy, to facilitate commerce, and to provide security, and the United States supports its use. At the same time, the increasing use of encryption that cannot be decrypted when we have the lawful authority to collect information risks allowing criminals, terrorists, hackers and other threats to escape detection. As President Obama recently said, "[i]f 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."[19] I'm not a cryptographer, but I am an optimist: I believe that if our businesses and academics put their mind to it, they will find a solution that does not compromise the integrity of encryption

[18] NAT'L RESEARCH COUNCIL, *supra* note 9.

[19] President Barack Obama, Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference (Jan. 16, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-.

technology but that enables both encryption to protect privacy and decryption under lawful authority to protect national security.

So with that plea for help, let me stop and take your questions.