NOVEMBER 20, 2014

PREPARED REMARKS

BEFORE EUROPEAN MEMBER STATES DATA PROTECTION AUTHORITIES

BY MS. REBECCA J. RICHARDS

DIRECTOR, CIVIL LIBERTIES AND PRIVACY OFFICE,

NATIONAL SECURITY AGENCY

It is truly an honor and privilege to be here with you today. This is my first public engagement with an international group, and I am happy to have the opportunity for a conversation with a group of international privacy experts. I would also like to thank you for taking time from your busy schedules and offer special thanks to my friends with the International Association of Privacy Professionals for arranging this opportunity. As you may have heard, the National Security Agency has been in the news a few times this past year. So today I thought it might be interesting to discuss what civil liberties and privacy interests the National Security Agency seeks to protect and how we are currently doing so.

I came to this job about nine months ago but for the last fifteen years, I have been working in the area of privacy in both the private sector and government. I am honored to have been selected to serve as NSA's first Civil Liberties and Privacy Officer.

This is an exciting time to be a member of the civil liberties and privacy profession. Our international privacy community is growing and evolving. The same is true for the United States privacy community. I believe we have an opportunity to help inform the debate as the United States continues to reshape its expectations for and limitations on, intelligence community activities. Changes in the nature of the threat to our national security, alongside the rapid advances in technology, make my job both interesting and challenging. Advancements in technology, whether it is big data, data aggregation, or the Internet of Things, raise novel challenges beyond government surveillance and even beyond the government. These advancements go to the heart of how we and the world around us view and manage our own individual privacy. Technology provides us with both opportunities and challenges, but ultimately we must guide and shape its use to ensure the fundamental rights we hold dear as a global society. Today, I would like to describe NSA's civil liberties and privacy programs past, present, and some thoughts for the future.

Historical Aspects of Civil Liberties and Privacy at NSA

Part of NSA's mission is to obtain foreign intelligence worth knowing in response to requirements and priorities validated and levied upon us by the Executive Branch. These intelligence requirements include counterterrorism, but also include helping to identify and stop the spread of nuclear, chemical, and biological weapons and helping to stop cyber attacks. Additionally, NSA works directly with and supports our troops and our allies by providing foreign intelligence for military operations abroad.

While the part of NSA's mission I've described is called Signals Intelligence or SIGINT, the other major portion of our mission is called Information Assurance. Although the Information Assurance mission is not the main topic for today, NSA also has the responsibility to protect national security systems to prevent others from obtaining U.S. government secrets and sensitive information.

As we consider NSA's civil liberties and privacy programs over the last sixty-two years, it is important to think about how the threat, technological, and societal landscape in which NSA conducts its SIGINT mission has changed.

(1) *The threat has changed.* NSA previously operated in the Cold War era when the focus of collection for foreign intelligence was directed at nation-states, structured military units, and foreign intelligence services. While these threats remain from nation-states, they now also come from non-state actors, including terrorists operating in small groups or as individuals. This transition requires intelligence professionals to look at more, smaller, and decentralized targets to protect their nation.

(2) *The technology has changed.* NSA previously operated in an environment where the communications between foreign intelligence targets were frequently conducted over separate, government owned and operated communications channels and equipment. In such cases they were easier to identify and isolate. Now foreign target communications are interspersed with ordinary commercial and personal communications. They flow over the same wires and air waves and are routed through multiple points all over the world. Additionally, the sheer volume and ability to analyze and manipulate big data, which has occurred as a result of significant advances in information technology, can expose information of a personal nature that may not have been previously discoverable and may not be of any foreign intelligence interest.

(3) *How society thinks about civil liberties and privacy has changed.* We have come a long (and positive) distance in thinking through what ought to be private. Personal identifiable information was not a mainstream issue 25 years ago the way it is today. In reaction to technology and business practices that can organize data, quickly provide data to others, or create new uses for data already acquired, we've begun to reconsider what information is available about ourselves through privacy policies and, in some cases, specific legislation.

Historical Civil Liberties and Privacy Framework

NSA's civil liberties and privacy protections have historically been driven primarily by U.S. Constitutional 4th Amendment analysis – the touchstone of which is whether a particular search is reasonable under the particular circumstances. NSA has always applied this analysis, which examines the degree to which an action intrudes on individual privacy, to activities conducted under its primary authorities, namely, Executive Order (E.O.) 12333 and the Foreign Intelligence Surveillance Act (FISA). NSA's privacy protection programs implemented this calculus by analyzing where and how data was collected and the status of the individual or entity being targeted. NSA has consistently conducted extensive legal analysis as it considers new types of collection answering these types of questions.

NSA continues to address these interests through a strong compliance program. The compliance program is designed to provide reasonable assurances that NSA is following its legal and policy restrictions placed on collection, processing, analysis, production, and dissemination of U.S. person information. Many compliance activities are embedded into our technology and systems. Procedures are approved by the United States Attorney General and, for certain authorities such as FISA, these procedures are also reviewed and approved by the Foreign Intelligence Surveillance Court after adoption by the United States Attorney General. Long before I arrived, NSA had organizations, training, policies, procedures, internal and external oversight activities, and a strong compliance program to manage these mandates and procedures. Privacy protections include activities to delete data, limit the time data can be retained, and to put tools in place to reduce the likelihood that information on a U.S. person will be obtained. In instances where U.S. person information is related to the foreign intelligence requirements, identifying personal information is masked or minimized before relevant foreign intelligence may be disseminated to authorized and appropriately cleared personnel outside of NSA.

Evolving Our Civil Liberties and Privacy Framework

The current framework is aligned with how NSA is governed by the U.S. Constitution, Executive Order 12333, FISA, and their associated updates or amendments. As I have learned more about NSA and its compliance regime, it became clear that while this is certainly one way to address privacy concerns, it is somewhat different from how privacy concerns are addressed outside of NSA. Over the last fifteen years our Congress has passed a variety of laws to protect privacy in other parts of government and in the commercial sector. These laws and policies focus more on the *nature* and *use* of the data itself not *where it was collected* or *the citizenship status of the individual*.

With the explosion of the Internet and global communications, resulting in everyone using the same communications infrastructure, and a new Presidential policy for SIGINT that broadens the privacy protections beyond U.S. persons to include ordinary persons of all nationalities, I believe

we have an opportunity to bring together NSA's current civil liberties and privacy analysis with a broader approach to privacy and civil liberties. This new approach is a step in the right direction to support the President's Presidential Policy Directive (PPD-28) "Signals Intelligence Activities" mandate to recognize that "our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in handling their personal information."

Incorporating the Protections of PPD-28

The President issued this new policy on January 17, 2014 to ensure that the United States signals intelligence program operates in recognition of this changed landscape. Specifically, our President directed us to extend, to the maximum extent feasible, comparable privacy protections afforded to U.S. persons to ordinary persons of all nationalities. We are working hard to do just that.

Last month, the Office of the Director of National Intelligence, the organization that is responsible for coordinating the activities of the U.S. Intelligence Community, made public its interim report to provide an update regarding the implementation of PPD-28. The status report, entitled "Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28" is available to you online (icontherecord.tumblr.com) and provides additional guidance for elements of the intelligence community to translate principles from PPD-28 into procedures and practices. Specifically, PPD-28 and the Status Report call on the intelligence community to provide the following protections, among others. These words hold weight and represent the values and principles we hold dear. I wanted to share ten major points with specific language that may be of interest to you. They set the tone and tenor for our continued implementation:

1. Ensure that privacy and civil liberties are integral considerations in the planning of SIGINT activities.
2. Ensuring that, "the United States [does] not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes."
3. Limit the use of signals intelligence collected in bulk only "for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cyber security threats; (5) threats to U.S. or allied Armed Forces or other

U.S. or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes."

4. Ensure that retention and dissemination standards for U.S. person information under E.O. 12333 are also applied, where feasible, to all personal information in signals intelligence, regardless of nationality.
5. Clarify that the intelligence community will not retain or disseminate information as "foreign intelligence" solely because the information relates to a foreign person.
6. Develop procedures to ensure that unevaluated SIGINT is not retained for more than five years, unless the DNI determines, after carefully evaluating appropriate civil liberties and privacy concerns, that continued retention is in the national security interests of the United States.
7. Reinforce and strengthen internal handling of privacy and civil liberties complaints.
8. Review training to ensure the workforce understands the responsibility to protect personal information, regardless of nationality. Successful completion of this training must be a prerequisite for accessing persona information in unevaluated SIGINT.
9. Develop oversight and compliance programs to ensure adherence to PPD-28 and agency procedures, which could include auditing and periodic reviews by appropriate oversight and compliance officials of the practices for protecting personal information contained in SIGINT and the agencies' compliance with those procedures.
10. Publicly release, to the extent consistent with classification requirements, the procedures developed pursuant to PPD-28.

Based on this very clear direction from the President of the United States, NSA is developing its "Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of SIGINT Information and Data Containing Personal Information of Non-United States Persons." These set of rules will help us put into practice the principles of PPD-28. We are still working through some very detailed implementation to make sure we get them right. We owe them to the President and January, just a couple months from now. And, as part of our efforts to improve communications and transparency, we will make this implementation plan available to the public, including the international community. We hope they will be considered as steps toward building increased trust and confidence.

The Civil Liberties and Privacy Assessment

Implementing PPD-28's mandate is critical, but we are doing more. As NSA's first Civil Liberties and Privacy Officer, I am working to address a broader set of civil liberties and privacy interests. That is why I am testing a new civil liberties and privacy assessment process that expands NSA's views to include considerations of frameworks that the private sector and non-intelligence elements of government use to assess civil liberties and privacy. To make sure we get it right, we are testing this approach for a variety of mission activities and we hope to evolve

to incorporate a more scientific approach to the assessments. We expect testing to continue during the next year.

For example, for the first time in its history, NSA is using the Fair Information Practice Principles (FIPPs) as a framework for considering civil liberties and privacy risks. The FIPPs have come in many variations over the last forty years, but they are commonly employed within the U.S. government as the following eight principles: transparency, individual participation, purpose specification, data minimization, use limitation, security, and accountability and auditing.

While the traditional NSA civil liberties and privacy questions center on the citizenship and location of NSA's foreign intelligence targets, as well as the collection techniques that will be employed to acquire a target's communications, FIPPs- related questions boil down to "follow the data." Data-centric perspectives mean privacy officials ask a different set of questions: What data is being collected and how will it be used? As we continue to test how we may adapt the FIPPs framework to NSA mission operations, we are beginning to ask additional questions that start with what data is being collected and for what specific purpose. Still in its early stages, we have designed an initial template and during the next year we will refine the questions and processes to ensure we are building a repeatable, meaningful, and helpful process to identify and mitigate civil liberties and privacy risks.

A critical part of the assessment process is to make sure we are not merely checking off boxes, but fundamentally weighing the risks associated with an activity to form a holistic value proposition. In essence, we are asking, "Should NSA conduct a given activity given its civil liberties and privacy risks?"

There are several broad civil liberties and privacy considerations that I think about when I consider new or existing programs at NSA, including: (1) how intrusive is the program to the individual (e.g., what type of data is being collected?), (2) how broad is the program (e.g., am I obtaining data about more people than my intended foreign intelligence target?), and (3) are the stated use and future uses appropriate given the type of data collected?

We ask questions to ensure that our protections evolve and adapt to this new landscape. As we consider how NSA conducts its mission to protect the country, we will continue to ask questions and provide safeguards to protect the legitimate civil liberties and privacy interests of ordinary individuals.

Providing Greater Transparency

In addition to evaluating specific activities internally for civil liberties and privacy, we recognize NSA must provide greater transparency to the public, including our international community. This is a central challenge for an Intelligence Agency – both at the individual level, and more

broadly for public communications. I will continue to advocate for the individual through my systematic civil liberties and privacy assessment processes and through my continuing commitment to share information about NSA activities with the public.

Transparency generally means organizations should be as open as possible about their activities and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information. NSA cannot provide the same level of information as in other parts of the government or private sector, because it risks losing access to foreign intelligence by tipping off adversaries. Instead, NSA provides a great deal of information to its overseers from all three branches of government.

Although NSA has the responsibility to maintain secrecy regarding many aspects of what we do, we are increasing our communications with the public. To date, I have published two reports based on specific NSA authorities using the FIPPs as the model for analysis of existing civil liberties and privacy protections. You may find the reports and other information on my NSA public website. I also meet with civil liberties and privacy experts in and out of government and overseers to better understand their concerns.

Recently, the Agency released more information into the public domain in response to specific requests and declassification of historical documents. NSA's senior leadership, including our Director, Admiral Mike Rogers, recognizes the need to inform the public about NSA's mission, effectiveness, and structure. We are doing so through public speaking engagements and discussions with academics and thought leaders, and we are similarly interested in conversations with the international community on these topics. Additional information has been shared with the public about laws, directives, authorities, and policies that govern NSA activities and associated compliance and oversight framework.

Blending the Art and Science of Privacy

Part of the conversation I would like to have today is how we might consider how to advance the discussion and research regarding the protection of civil liberties and privacy. NSA has many technical experts, computer scientists and mathematicians. We would like to work with other agencies and outside privacy advocates to craft a privacy technology and research agenda that we can use to support NSA's efforts, as well for others with similar interests to consider.

Protecting privacy and civil liberties to date is more art than science. We have privacy policies that are written to cover a variety of technologies, but we generally do not have technologies that identify privacy risks.

In order to move such research forward, I believe we need a broad spectrum of expertise working together to truly understand policy, legal, technical, and ultimately ethical perspectives, both in the United States and among our allies. Today the science of privacy has made notable strides

that include developing technology and tools that promote privacy such as unique encryption capabilities, digital rights management, and trustworthy computing. Great work in the private sector and academia is also being developed on coding privacy policies such that technology supports only specific uses.

Civil liberties and privacy protections need to blend the art and science of privacy if we are going to harness the potential of technology and incorporate our core values in this Era of Big Data.

Yet despite significant progress, basic privacy principles, founded in a strong scientific basis, have proven elusive. If we can better understand what constitutes personal information and how such information is used, we believe it will be possible to help determine whether we can develop more practical approaches to evaluate the inherent privacy risk to the individual.

To that end, we are beginning to explore a scientific approach towards a true Responsible Use Framework. Our initial thoughts include development of five sequential building blocks:

1. **Categorize Personal Information.** As a first step, we would like to determine if it is possible to identify and categorize different possible types of personal information. For example, one category could include biographic information, such as a name or address. Another category could include biometric information. Yet another category could include contextual information about an individual, such as transactional information about an individual's activities. If we can understand these various categories, it may then be possible to identify relative risks and thus understand the privacy risk of given category of personal information. This would lay the groundwork from which follow-on work would build.

2. **Categorize Uses of Personal Information.** Second, we would like to determine if it is possible to identify and categorize different types of uses of personal information. Similar to what I just discussed above, if it is possible to categorize basic uses of personal information, it may also be possible to identify relative risks of use and consequently, the risk of a particular type of use.

3. **Design a Process to Understand the Inherent Privacy Risk and Use of Personal Information.** Third, if it is possible to develop a categorization of both personal information and uses of the personal information, it should then be possible to develop a scientific process to assess risk. This process could evaluate the risk of the use of individual types of personal information for different purposes as well as aggregated uses of personal information.

4. **Enhanced Privacy Impact Assessments**. These previous three building blocks in hand, it should be possible to apply the established methodology to develop repeatable and

scalable assessments and help implement the specific FIPPs of purpose specification and use limitation more concretely. Here, the Art of Privacy blends with the Science of Privacy; the judgment of experts must always be part of these solutions with more scientific methods assisting to identify and remediate risks.

5. **Move toward a Responsible Use Framework.** Lastly, a Responsible Use Framework holds data collectors and users accountable for how they manage data and any harm it causes. Building a technical means based on principled scientific methodologies to support the identification of civil liberties and privacy risks can help us better protect civil liberties and privacy in a fluid world of big data. Disciplined data tagging, aided by analytics and metrics that track the movement and use of data, is also of utmost importance for identifying and mitigating risks. These activities, combined with a strong compliance program, provide a holistic approach to building civil liberties and privacy protections into the infrastructure of the cloud and an enterprise's mission systems and architecture.

Success is dependent upon input from a variety of disciplines ranging from technologists, social scientists, privacy and civil liberties experts, ethicists, attorneys, and computer scientists, to name a few. We would welcome the opportunity to discuss this in more detail and greater technical depth at a later time.

Conclusion

Again, I would like to thank you for this opportunity to outline how NSA is addressing privacy today and our path for the future. We will continue to develop and refine a multifaceted approach to strengthen the privacy protections at NSA. We believe that the advancement of the science of privacy, blended with the art of privacy has a potential to benefit how NSA considers civil liberties and privacy within its mission activities and we believe it could benefit others. I look forward to learning more about your views.