Statement for the Record

United States Senate

Committee on the Judiciary

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Carrie F. Cordero

Director of National Security Studies
& Adjunct Professor of Law

Georgetown University Law Center

Introduction

Mr. Chairman, Ranking Member Grassley, members of the Committee, thank you for this opportunity to appear before you again to share my views on the important issue of continued oversight of U.S. Government surveillance activities, including activities conducted under the Foreign Intelligence Surveillance Act (FISA).

I am currently the Director of National Security Studies and an Adjunct Professor of Law at Georgetown University Law Center, where, among other things, I teach a course on Intelligence Reform. The views presented in this statement and at this hearing are my own, and should not be construed to reflect the views of any employer, current or former. This statement was reviewed by the government for classification purposes.

By way of background, prior to joining Georgetown Law in November 2011, I spent my career as a practicing national security lawyer in the Executive Branch. In 2009, I served as Counsel to the Assistant Attorney General for National Security at the United States Department of Justice, where I co-chaired an interagency group created by the Director of National Intelligence (DNI) to improve FISA processes. From 2007-2009, I served in a joint duty capacity as a Senior Associate General Counsel at the Office of the Director of National Intelligence, where I worked behind the scenes on matters relating to the legislative efforts that resulted in the FISA Amendments Act of 2008. Once that law was passed, I was involved in many aspects of implementing the FISA Amendments Act, as well as standing up the internal executive branch interagency oversight structure. Prior to my tour at ODNI, I served for several years as an attorney in the office now called the Office of Intelligence, which is part of the National Security Division at the Department of Justice, and appeared frequently before the Foreign Intelligence Surveillance Court (FISC). I handled both counterterrorism and counterintelligence national security investigations. Later, I became involved in policy matters, including contributing to the development of the Attorney General's Guidelines for FBI Domestic Operations and updated FISA minimization procedures. I also did a short stint as a Special Assistant United States Attorney in the Northern District of Texas. Early in my career, I spent considerable time preparing information that was reported to both the Intelligence and Judiciary Committees of Congress as part of the annual public reports on FISA as well as the comprehensive semi-annual reports on FISA. In short, I am one of a very small handful of attorneys currently outside of government who has direct experience with the operational, legislative, policy, and oversight aspects of FISA, as it was practiced from 2000-2010.

Accordingly, my views are informed by this up-front perspective regarding how the USA PATRIOT Act of 2001, the Intelligence Reform and Terrorism Prevention Act of 2004, and later the FISA Amendments Act of 2008, vastly improved the Intelligence Community's ability to protect the nation from another attack on the scale of September 11th. More recently, I have had the added benefit of having spent the past three years outside of government to reflect, and to engage with the academic community, and to some extent the public, regarding some of the issues this Committee is considering today.

Since the Committee's October 2, 2013 hearing, the legislative debate and public conversation have been influenced by additional events. First, new legislation has been

introduced, in particular, S.1599, the USA FREEDOM Act, a bipartisan bill sponsored by the Chairman; as well as S.1631, the FISA Improvements Act of 2013, the bill put forth by Chairman Feinstein of the Senate Select Committee on Intelligence, who, of course, also serves on this Committee. That bill has been voted out of Committee. Second, the Executive Branch has declassified additional documents that are relevant to the current legislative debate, including but not limited to a FISC opinion on the ongoing telephony metadata program,[1] as well as a FISC opinion regarding the collection of Internet metadata that has since been discontinued.[2] Third, additional unauthorized disclosures of classified information have continued on what seems like at least a weekly basis. A recent example is the December 4, 2013 *Washington Post* story on NSA's collection of international cell site data.[3]

As a result of these and other developments, the conversation has shifted somewhat from where it was in October. I would like to offer a few observations that pick up on these developments. First, I would suggest that the conversation has evolved from objections to specific programs, such as the 215 or 702 collections (although objections do remain, particularly on 215), to a discussion of our cultural understanding and acceptance of foreign intelligence surveillance activities more broadly. Consideration of providing privacy protections to foreigners in the surveillance context, as well as whether to prohibit altogether the use of FISA for so-called "bulk" collection, have become a larger part of the debate. Second, legislative proposals, including S.1599, are coming closer to scaling back national security legal authorities in a way that would take the country backwards by reinstituting legal standards above and beyond what is required in the criminal investigative context. And, third, the path forward on authorized public disclosure in a way that both protects classified information and restores relationships between the private sector and consumers, as well as between the private sector and the U.S. Government, remains a worthy goal, but a significant challenge.

I. Proposals to Scale Back Foreign Intelligence Collection

A. Metadata Collection

Increasingly, the argument against the telephony metadata[4] collection under the business records provision of FISA, as amended by section 215 of the USA PATRIOT Act, focuses on

---

[1] Memorandum Opinion*, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[2] [Redacted], PR/TT [Redacted], Opinion and Order, dated [Redacted], (available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf).

[3] Barton Gellman and Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, December 4, 2013 (http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html).

[4] Footnote 1 in Judge Mary McLaughlin's October 11, 2013 primary order defines "telephony metadata" as:

> "…comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc…), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. 2510(8), or the name, address, or

what I will call the "power of metadata" argument.[5] The argument goes something like this: metadata, that is, the information about our communications (such as dialed digits made in a phone call), can be assembled and analyzed in a way that it previously could not, both due to the way that data is communicated, retained and collected, as well as through tools that are now available to analyze it. Therefore, the argument goes, if the government collects large volumes of Americans' metadata, and then assembles, maps and/or analyzes that information, the government could learn an awful lot about a person, or a group of persons, simply by looking at metadata. Accordingly, metadata is a very powerful tool and there should be limits on the government's collection and use of it.

I doubt most Americans would argue with this proposition. I certainly don't. The problem with this argument made in the context of the debate concerning the current NSA surveillance activities under FISA, and the 215 program in particular, is that the worrisome assemblage of Americans' metadata bears no relation to the existing 215 program under consideration by Congress. According to the information that has been publicly disclosed by the Government, the telephony metadata program under section 215 does collect an enormous volume of Americans' telephone call detail records.[6] The collected information does not appear to include the content of phone calls, names of subscribers, payment information, or location information. The vast majority of the information collected is never viewed by human eyes. It simply sits in a so-called electronic or digital "black box," held by the NSA, and eventually ages off the system. The records are collected under FISA Court order that requires that the data acquired under this program: (i) only be used for counterterrorism purposes; (ii) only be queried by trained, designated personnel and that the queries themselves are approved by a smaller number of designated supervisory personnel; (iii) only be queried according to standards set out in the order; (iv) be destroyed within five years of collection; and (v) be subject to additional handling and processing procedures as directed by the FISC in its order.[7] The Court has said, in a written opinion, that without all of the limits in place, the Court would not have approved the program.[8]

Moreover, current Supreme Court precedent holds that there is no expectation of privacy in our telephone metadata, that is, the numbers we dial or the numbers that dial us. A warrant is not required to obtain this information.[9] Likewise, Supreme Court precedent also still holds that

---

financial information of a subscriber or customer. Furthermore, this Order does not authorize the production of cell site location information (CSLI)." (opinion and order available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[5] I previously described this and a second issue discussed in this statement in a post on *Lawfare* on November 14, 2013 (http://www.lawfareblog.com/2013/11/thoughts-on-two-propositions-the-power-of-metadata-and-providing-privacy-protections-to-foreigners/).

[6] *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-109, dated August 29, 2013, at p.4 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[7] Memorandum Opinion*, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[8] *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-109, dated August 29, 2013, at p.3 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[9] *Smith v. Maryland*, 442 U.S. 735 (1979).

we do not have a reasonable expectation of privacy in records voluntarily turned over to a third party.[10] In the first publicly-released FISC opinion on the 215 program dated August 29, 2013, Judge Claire Eagan, approving continuation of the business records metadata program, offered a straightforward analysis of the law:

> In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such Orders were lawful and required, and the requested Orders were therefore issued.[11]

Since this Committee's October 2, 2013 hearing, the Government has released a new written opinion, by Judge Mary McLaughlin, who had not previously ruled on the 215 program. Judge McLaughlin approved the continuation of the program, and adopted Judge Eagan's previous analysis. In addition, she distinguished *United States v. Jones*,[12] the 2012 case concerning GPS surveillance, stating that "*Jones* involved the acquisition of a different type of information through different means."[13] She went on to state:

> The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, *Smith* remains controlling with respect to the acquisition by the government from service providers of non-content telephony metadata such as the information to be produced in this matter.[14]

In the meantime, current collection activities, based on the FISC opinions and accompanying materials that have been declassified by the government, are consistent with *current* precedent and *existing* interpretations of the laws.

As I noted in my previous statement, with respect to 215 in particular and intelligence programs generally, I believe that they should be regularly reviewed and evaluated to determine whether they continue to be necessary and valuable. It is wholly appropriate to end a collection program that has outlived its usefulness, or perhaps is no longer necessary based on new

---

[10] *United States v. Miller*, 425 U.S. 435 (1976).

[11] *Amended Memorandum Opinion, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-109, dated August 29, 2013, at p.3 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[12] 132 S.Ct. 945 (2012).

[13] Memorandum Opinion*, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013, at p.4 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

[14] Memorandum Opinion*, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, BR 13-158, dated October 11, 2013, at p.5-6 (available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf).

technologies or methods of collecting intelligence that may be more efficient or productive. As we now know publicly from the release of the opinion regarding the now-defunct Internet metadata program, intelligence programs come and go. And so it may be useful for Congress to look beyond the immediate focus on 215, and think more broadly regarding what limits it may or may not want to place on the Intelligence Community in light of as-yet-unforeseen threats or needs.

Some will argue that Congress should outlaw bulk collection under FISA, based on the "power of metadata" argument as well as arguments about our changing expectation of privacy in light of the methods of modern communications. But everyday Americans, or friends in foreign nations, are not the only people using the Internet to communicate. We *all* - - regular people, government leaders, as well as those who pose national security threats such as terrorists, terrorist financiers and facilitators, proliferators of weapons of mass destruction, spies, sophisticated hackers, and cyber intruders - - use the Internet, computers, and smart phones to communicate. And so just as regular people should not be expected to turn off their modern communications and revert to old fashioned modes of communication, neither should the Intelligence Community or law enforcement resort to pen, paper and index cards to conduct national security collection or investigations. It is just as unrealistic to expect citizens to unplug, as it is to expect or require the NSA or FBI to use 20th century collection, analytic or investigative techniques or methods to protect the nation from 21st century threats.

B. Providing Privacy Protections to Foreigners

In light of recent unauthorized disclosures, concerns have also been expressed regarding the NSA's collection targeting or pertaining to foreign persons located outside the United States. Suggestions have been made that U.S. foreign intelligence collection should recognize some sort of privacy right for non-U.S. persons.

In fact, the U.S. Intelligence Community has a recent history of affording Constitutional protections to persons who are not entitled to them. Congress made a deliberate decision with the passage of the FISA Amendments Act of 2008 to end that practice. And for good reason: prior to 2007, the U.S. government was, in fact, going through incredible hoops to acquire certain communications of foreign terrorist targets overseas. Two parallel processes caused this to happen. The first was described in a written statement for the record by the Director of National Intelligence before this Committee in September 2007[15]

> "…[P]rior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a

[15] Statement for the Record of J. Michael McConnell, Director of National Intelligence, Before the Senate Judiciary Committee, September 25, 2007 (available at http://www.dni.gov/files/documents/Newsroom/Testimonies/20070925_testimony.pdf).

> foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests."

In other words, the Intelligence Community, because of the requirements of the FISA statute prior to 2007, found itself in a position where it was seeking individual probable cause-based orders from the FISC to target terrorists overseas. When the government needed to obtain certain communications of a terrorist target, located in, as examples, Pakistan or Yemen, it was preparing a full application to the FISC, with a detailed factual showing providing probable cause that the target was an agent of a foreign power, and obtaining the signatures of a high ranking national security official and the Attorney General, and then submitting that application to the FISC for approval. This extensive process, in addition to being unnecessary from a Constitutional perspective, was a crushing force on the system.

In a separate but somewhat related chain of events and as described in the Senate Select Committee on Intelligence's Report of October 26, 2007,[16] in January 2007, the Attorney General announced that collection that had previously been conducted under the Terrorist Surveillance Program had transitioned to collection authorized by the FISC. The FISC's authorization was based on findings that "'there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist group.'"[17] According to the SSCI report, Congress subsequently received the Administration's proposal to modernize FISA in April 2007. The report went on to state:

> "The Administration's proposal for FISA modernization was comprehensive, and had been coordinated within the Department of Justice and the intelligence community. At the end of May 2007, however, attention was drawn to the FISA Court. When a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information from the Court. In late July, the DNI informed Congress that the decision of the second FISA Court judge had led to the *degraded capabilities in the face of a heightened terrorist threat environment*. The DNI urged the Congress to act prior to the August recess to *eliminate the requirement of a court order to collect foreign intelligence about foreign targets located overseas*."[18] [emphasis added]

As this Committee is aware, in August 2007, Congress enacted the Protect America Act of 2007, the interim law. Next came the FISA Amendments Act of 2008, including the significant section 702, which enabled collection against non-U.S. persons reasonably believed to be outside the

[16] Report 110-209, Senate Select Committee on Intelligence, Foreign Intelligence Surveillance Act of 1978, Amendments Act of 2007, (http://www.intelligence.senate.gov/071025/report.pdf).
[17] *Id*. at p.5.
[18] *Id*. at p. 5-6.

United States to proceed, not under probable cause requirements, but under a Director of National Intelligence and Attorney General approved certification, and under targeting and minimization procedures approved by the FISC. Future considerations of affording Constitutional protections to foreigners outside the United States should take the experiences of this recent history into account.

II. Analysis of Selected Sections of S.1599

I would next like to highlight four components of S.1599. The first three would, in my view, significantly limit the effectiveness of the U.S. Government to conduct foreign intelligence activities to protect the nation from the national security threats of today, and, tomorrow. The fourth is a brief comment on competing proposals to add an adversarial component to the FISA process.

First, sections 101 and 201 would change the legal standards to obtain business records and implement pen register/trap and trace devices by requiring a connection to an agent of a foreign power. The sections also add a "materiality" requirement in addition to relevance. The likely intended effect of these provisions is to eliminate the utility of these provisions for large scale collection, such as the 215 telephony metadata program. But the proposed changes would likely have far more dramatic, and harmful, consequences to more traditional, day-to-day, national security investigations. The standards are currently aligned with investigative authorities in the criminal investigative context, such as subpoenas and pen register/trap and trace surveillance conducted under Title 18. Both of those criminal authorities operate on a relevance standard. By raising the standard to requiring a connection to an agent of a foreign power, these sections would render these investigative techniques nearly useless in the early stages of an investigation, which is precisely when they are most useful. Investigators may never get to determine whether a target rises to the agent of a foreign power standard, if they cannot conduct the less intrusive records request or pen register/trap and trace surveillance as part of an investigation. These changes, if made law, would return us to the days prior to September 11, 2001, when it was harder for an investigator to request records or conduct pen register/trap and trace surveillance in an international terrorism case than it was in an everyday drug or fraud case.

Similarly, section 501 would amend the collection of statutory authorities known as "national security letters" by requiring the requested records to have a connection to an agent of a foreign power. The effect of this provision, if it became law, cannot be understated: it would severely limit the FBI's ability to conduct timely and thorough national security investigations. The criminal investigative counterpart to a national security letter is a subpoena. Subpoenas are issued based on relevance to an investigation. By requiring a nexus to an agent of a foreign power, which is a defined set of terms under FISA, the bill limits the ability of the FBI to request records at early stages of investigation. Moreover, Attorney General Guidelines require that national security letters may only be used in the context of a predicated investigation, which must meet certain factual thresholds and supervisory approvals; national security letters may not be used in an assessment alone.[19] This limiting guideline already imposes a higher bar to

[19] *Attorney General Guidelines for FBI Domestic Operations* (September 29, 2008) (http://www.justice.gov/ag/readingroom/ guidelines.pdf).

obtaining a national security letter than a subpoena for telephone or electronic mail subscriber information, which may be used at the assessment stage.[20]

Second, section 301 would appear to prohibit the Intelligence Community from querying data acquired pursuant to section 702 of FISA to search for U.S. person communications. Under the current minimization procedures approved by the FISC for 702 collection, the NSA may query communications already acquired under section 702 for U.S. person communications.[21] The proposed legislation would only allow the same query to take place if the U.S. person (presumably about whom the query is made) is the "subject of an order" of current surveillance, search or acquisition pursuant to FISA or criminal authorities. In other words, the U.S. person would already have to have been found to be an agent of a foreign power by the FISC, or the target of a criminal wiretap, both of which would require prior judicial approval based on probable cause. (The legislation does include emergency and consent exceptions to the proposed prohibition).

Consider the following hypothetical: this proposal could arguably prohibit the Intelligence Community from querying already lawfully acquired data to search for the methods of communication used by, say, Adam Gadahn, or someone like him. As Members of this Committee are aware, Adam Gadahn is a U.S. citizen who is on the FBI's Most Wanted Terrorist List.[22] He is a known al Qaeda propagandist and is the subject of a pending indictment on charges of providing material support to terrorism, among other charges.[23] Most recently, according to press reports, Gadahn posted an audio speech encouraging militants to attack U.S. interests.[24] Several days later, on December 5, 2013, American teacher Ronald Thomas Smith II was attacked and killed in Benghazi, Libya.[25] Let's assume for a moment that the U.S. Intelligence Community does not currently know what telephone numbers or email addresses Gadahn uses to communicate. (Again, I have no idea whether it does or does not have this information, or whether Gadahn even uses such modes of communication.) In such a case, querying existing, lawfully-acquired 702 data for accounts or identifiers used by Gadahn would be of significant foreign intelligence value. And, the issue is not whether Gadahn could be found to be an agent of a foreign power; under the legislation as drafted, it only matters whether he is, currently, the target of existing collection. If the U.S. Intelligence Community does not know what methods he uses to communicate, then he would not, as a practical matter, be a target of current collection authority, because there would be no number, account or identifier to collect against. In short, the proposed section 301 limitation would prevent the U.S. Intelligence Community of learning exactly the type of information we expect it to discover to protect U.S. interests and Americans from terrorist activity.

---

[20] *Id*.

[21] *See Exhibit B, Minimization Procedures Used By the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, dated October 31, 2011, at p.6 (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf).

[22] http://www.fbi.gov/wanted/wanted_terrorists.

[23] http://www.justice.gov/opa/documents/adam_indictment.pdf.

[24] Associated Press, *U.S. Teacher Shot Dead in Benghazi*, December 5, 2013 (available at http://online.wsj.com/news/articles/SB10001424052702303997604579240163015786696).

[25] *Id*.

This is not to suggest that querying NSA databases for U.S. person information is not sensitive. It is. And it should be done in accordance with meaningful procedures, approvals and oversight. Indeed, according to the now-declassified minimization procedures governing 702 collection, the "use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures[,]" and are subject to oversight by the Department of Justice and the Office of the Direct of National Intelligence.[26] Accordingly, while I do see the issue of NSA queries using U.S. person identifiers to be a legitimate issue for this Committee and/or the Intelligence Committee to conduct oversight of, I would submit that the legislative proposal to prohibit such queries is inappropriately restrictive in the context of the national security mission.

Third, section 302 would appear to limit the way in which NSA uses its collection technologies against valid foreign intelligence targets. Unfortunately, in an effort to limit certain kinds of collection to only those circumstances that would protect against international terrorism or the proliferation of weapons of mass destruction, this provision leaves open the possibility that certain collection techniques would not be available against other valid threats, such as cyber-based threats. For example, a cyber attack directed against U.S. critical infrastructure, perpetrated by or at the direction of a foreign power, would appear not to fall into the exception. Understanding that the intent of this provision is likely intended to make certain collection techniques available only in the most serious of threats, articulating them in the statute itself would leave the Intelligence Community vulnerable to facing operational situations where the law again lags behind the threats and sophistication of hostile actors.

Fourth, section 901 of the bill would add an Office of Special Advocate. I would refer the Committee to my previous statement, in which I discuss why, in my view, a separate office is both unnecessary given the FISC's independent oversight of Executive Branch activities, and would add significant bureaucracy to an already heavily lawyered FISA process. However, given the increasing Congressional and public interest in providing the FISC with the ability to call on outside views in considering novel issues, I would submit that the approach offered in S.1631, which gives the FISC discretion to appoint an *amicus curiae* for either legal or technical advice or views, is less objectionable than establishing a permanent Office of the Special Advocate.

III. Proposals to Enhance Transparency

S.1599 contains a number of transparency provisions directed at both surveillance authorities and national security letters. The legislation approaches the public reporting from two perspectives: what the companies can release, and what the U.S. government should release. In my view, there is substantial value in Congress continuing to work with the Executive Branch and the private sector to rebuild confidence between them, and for the U.S. Government to help the private sector restore confidence with consumers, customers and investors. In 2008, Congress acted in this area by including liability protection in the FISA Amendments Act for companies

[26] *See Exhibit B, Minimization Procedures Used By the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, dated October 31, 2011, at p.6 (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf).

that had voluntarily assisted the government after September 11, 2001, and whose cooperation was subsequently exposed by the significant unauthorized disclosure that took place in 2005.

In my previous statement, I suggested that, in the interests of facilitating transparency while reducing the reactive nature of each authorized public release, Congress could amend the reporting provisions in FISA to provide additional public information—whether it is statistics, declassified legal opinions, summaries of implementation actions or reports on compliance matters—semi-annually, quarterly, or at some other appropriate regular interval. I note that S.1599 contains several reporting provisions that would occur either annually, or quarterly.

With respect to the content of the proposed public reports, I would suggest that further consideration and revision is in order, on several fronts. As a guiding principle, I would suggest that any new public reporting only be mandated by law if Congress is confident that it can reasonably be produced *accurately*. Inaccurate or inconsistent reporting will lead to more questions and less confidence, and may be worse than no reporting at all.

While I would expect that representatives of the Intelligence Community will address concerns with the legislation about disclosing information about targets of surveillance or other data points that may be impossible to produce, I would like to highlight several sections that would benefit from additional consideration:

- Section 601 provides that electronic service providers may report on estimates of demands and requests made and complied with, and estimates of numbers of users or accounts. It may be that the providers and government prefer estimates versus actual numbers, but the proposal does raise some concerns that public reporting from different sources will be inconsistent, which may have the unintended consequence of undermining confidence, not bolstering it. I would also urge caution on releasing numbers of users or accounts affected: if targets use multiple accounts, the number may be misleadingly high.

- Section 601 also proposes to define "surveillance law." Curiously, the section includes the national security letter statutes, which are not surveillance laws, but appears to exclude the federal criminal wiretap law.

- Section 602 proposes that the government disclose numbers of persons "subject to electronic surveillance." If the intent of this proposal is to release how many individuals' communications were collected—either through targeting or incidentally—then it is important to consider the reverse effect on privacy protections that this disclosure would have. Because intelligence analysts only review communications in pursuit of identifying foreign intelligence information, there is a body of collected information that is either never reviewed, or, reviewed but not analyzed, reported, or counted for any statistical purposes. Similarly, minimization procedures would require that analysts not write reports about U.S. persons who may be incidentally collected but whose communications do not appear to be foreign intelligence information. Accordingly, a requirement to report on numbers of persons collected would actually degrade privacy practices: it would require that Intelligence Community personnel look at, read, review, count, keep records

about and report on information that they otherwise would disregard in pursuit of their actual mission of discovering, analyzing and reporting foreign intelligence information.

Conclusion

I thank the Chairman, Ranking Member and Committee Members for providing me with this additional opportunity to share my views on the efforts to reform U.S. Government surveillance activities. Although there is significant public and political pressure to act to reform surveillance activities, I continue to urge the Committee to move cautiously: changes made quickly now will have consequences for the nation's security for years to come. I look forward to continuing to work with the Members and staff of this Committee on these important issues.