STATEMENT OF

APRIL F. DOSS

PARTNER, SAUL EWING, LLP

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
JUDICIARY COMMITTEE

CONCERNING

SECTION 702 OF THE
FOREIGN INTELLIGENCE SURVEILLANCE ACT

MARCH 1, 2017

TESTIMONY OF APRIL F. DOSS
PARTNER, SAUL EWING, LLP
BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
JUDICIARY COMMITTEE
MARCH 1, 2017

Mr. Chairman, Mr. Ranking Member, and Members of the Committee, thank you for the opportunity to testify about Section 702 of the FISA Amendments Act.

My name is April Doss, and I am a partner in the law firm Saul Ewing, LLP, where I chair the firm's Cybersecurity and Privacy practice group. Prior to that, I spent thirteen years at the National Security Agency, and before that, I worked as a public defender, in private practice, and as in-house counsel. The views that I express today are entirely my own and do not represent those of my firm, the National Security Agency, or any other agency or organization. My views are, however, informed by my experience working in the Intelligence Community, and so I will say a few brief words about those qualifications.

Like many other Americans, I recall exactly where I was on September 11, 2001. As I watched the twin towers collapse, I – like so many others – knew that our world had been irrevocably changed. Not long after that, I applied for a position at the National Security Agency (NSA), where I began working in September 2003.

During thirteen years at NSA, I worked in a variety of capacities. I was a senior policy officer for information sharing during the work of the 9/11 Commission and the passage of the Intelligence Reform and Terrorism Prevention Act. I managed counterterrorism programs and served as a foreign liaison officer. I was an intelligence oversight officer and an intelligence oversight program manager for multi-site intelligence operations. I served on the senior management team for new technology development. I also spent six years in the General Counsel's office at NSA. From 2005-2009, I was what we called an "operations" attorney. I provided legal advice to NSA's intelligence collectors, analysts, reporters, and oversight and compliance officers about the requirements of the Foreign Intelligence Surveillance Act (FISA) and other laws and associated procedures, regulations, and policies; I worked closely with counterparts from the Department of Justice; and I served as principal legal advisor on NSA's efforts to develop the new technology capabilities that would be used to carry out those intelligence activities. During that first stint in NSA's Office of General Counsel (OGC), I observed firsthand the ways in which a changing global telecommunications infrastructure had changed the practical impact of the Foreign Intelligence Surveillance Act. I advised NSA personnel on FISA in its traditional form, as well as on the new authorities and restrictions that came with the passage of the Protect America Act (PAA) in 2007 and the FISA Amendments Act (FAA) in 2008. In 2014, I returned to NSA's legal office, where I served as the Associate General Counsel for Intelligence Law. In that capacity, I led the group of several dozen attorneys responsible for giving legal advice on all of NSA's intelligence activities, including NSA's applications to the Foreign Intelligence Surveillance Court (FISC); NSA's use of the

FAA 702 authority; the technical capabilities being used for NSA's intelligence operations; and NSA's civil liberties, privacy, and oversight and compliance programs, including NSA's reporting to internal and external overseers of incidents of non-compliance. Throughout that time, I worked closely with counterparts at other executive branch agencies, including the Department of Justice (DoJ), the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI). I left government service in April, 2016 in order to take my current position.

Because much of the work that I did during those years was classified at the time, and because of my lifetime security obligations as a previous holder of classified information, this testimony has been submitted to the NSA for prepublication review to ensure that there has been no inadvertent inclusion of information that ought to be properly classified. That review, however, does not impact any of the views expressed in this statement, and all views are solely my own.

Having worked at NSA both before and after the passage of the FISA Amendments Act, and having been involved with that authority from a number of perspectives over the years – as a CT program manager, intelligence oversight program manager, technology policy architect, and legal advisor – I can attest to the following observations from my personal experience:

1) In 2008 when the law was passed, the authority was critically needed by the Intelligence Community because of the gaps created by the ways in which technology had changed in the years since the original FISA was passed;

2) The FAA 702 authority strikes an appropriate balance between the government's need for foreign intelligence information and the privacy impacts on individuals, including the impacts resulting from incidental interception of U.S. person communications;

3) The statutory framework incorporates robust oversight requirements and privacy protections;

4) Those protections have been implemented across all three branches of government in meaningful and substantive ways; and

5) The 702 authority has consistently, since its passage in 2008, provided critical intelligence information to the U.S. and its allies that would not have been obtainable in other ways.

1. The Need for the FAA 702 Authority – Then and Now

As this Committee considers whether to support reauthorization of FAA 702, it is worth revisiting the reasons why Congress chose to enact this legislation in 2008, and to renew it in 2012.

As the Committee is aware, prior to the passage of the short-term PAA legislation in 2007 and the FAA in 2008, the Intelligence Community was required to make individualized

showings of probable cause for each application filed under Title I of the FISA. Under the Title I rubric, the government must articulate a specific case demonstrating that there is probable cause to believe each target is a foreign power or an agent of a foreign power, and that each facility – such as an email address or telephone number – is associated with that foreign power or agent of a foreign power.[1] Title I remains the backbone of the overall FISA framework, but it is a poor fit for certain kinds of intelligence challenges, and its utility had been impacted dramatically by changes in the telecommunications environment between 1978, when FISA was passed, and the early 2000s.

In a post-9/11 world, the nature of intelligence targets, the diffuse nature of threats to the U.S., and the challenges of intelligence gathering all made clear that the Title I FISA approach was a poor fit for tackling some of the hardest intelligence problems, such as counterterrorism and countering the proliferation of weapons of mass destruction, that did not directly involve nation-state adversaries. The 21st century had ushered in a new era of communications in which intelligence targets were no longer primarily found talking on landline phones from within government buildings belonging to adversarial nations, nor were they limited to the radio communications of foreign military units that were being used to communicate troop positions or weaponry movements. Instead, diffuse groups such as terrorist networks now using the same commercial telephone and free webmail services that ordinary people around the world were using to stay in touch with family and friends. Terrorists couldn't be counted on to communicate via landline from fixed geographical positions. They didn't have air forces or naval fleets or conventional military bases full of tanks and troop carriers whose movements could be monitored by more traditional means. Instead, they frequently operated from within ordinary communities; they communicated via ordinary commercial means; they took great pains to hide their identities and their communications. In this new era, terrorists' planning for external operations – that is, their planning for attacks outside of the geographic region where they were based – was frequently concealed by a combination of means which made detection and analysis of those communications extraordinarily difficult to carry out through conventional intelligence collection means.[2]

The FISA requirement for individualized warrants meant that the government's capacity to seek intelligence information was necessarily constrained by the resources that would be required to submit an individualized probable cause application for every target of electronic surveillance. Further, the Title I requirement that collection be limited to foreign powers and agents of foreign powers meant that some valuable intelligence information was inaccessible altogether, either because the government did not yet have sufficient information to support a probable cause determination, or because the individual whose communications were being sought was someone who was likely to possess, receive or communicate foreign intelligence information but who did not meet the statutory definition of a foreign power or agent of a foreign

[1] *See generally* 50 U.S.C. §1801-1813.

[2] *See generally*, Hearing before the Senate Select Committee on Intelligence, Sept. 20, 2007, available online at https://www.gpo.gov/fdsys/pkg/CHRG-110jhrg38878/html/CHRG-110jhrg38878.htm ; *see also* Testimony of Kenneth L. Wainstein before the United States Senate Committee on the Judiciary, May 10, 2016, p. 3-5, available online at: https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Wainstein%20Testimony.pdf .

power.[3] Perhaps worst of all, the changes in telecommunications infrastructure between 1978 and the mid-2000s meant that FISA's language – and Congress's intent – had been turned on its head: where Congress's 1978 language required FISC authorization to collect calls from a wire (calls that would most likely have been landline, local calls in the U.S.) but exempted certain radio communications (international calls), the shift to undersea cables for international communications and the installation of cellular infrastructure meant that by 2007, local calls were carried via radio signal and international calls were conveyed on a wire. Because the statutory language had remained the same, there were now circumstances in which FISA applied in ways that were nearly the opposite of its original intent.[4]

In other words, the protections under Title I of the FISA, which had been designed to protect the Fourth Amendment rights associated with U.S. persons' communications, were having an unintended result by the mid-2000s: they were imposing strict statutory restrictions on the collection of information from and about persons who were not entitled to Fourth Amendment rights, and they were simultaneously preventing the government from obtaining important intelligence information that was constitutionally permissible.

These challenges were described in detail in Congressional hearings on the passage of the FAA in 2008, its reauthorization in 2012, and in hearings held by this Committee[5] and by the Senate Judiciary Committee[6] during the last Congress in advance of the current reauthorization discussion.

The result has been the addition to FISA of the current FAA Section 702 framework in which the government is granted the authority to compel communications providers to assist the government in the acquisition of communications that are to, from, or about persons who are expected to possess, communicate, or receive foreign intelligence information. Those processes are carried out through a comprehensive framework in which the Attorney General and Director of National Intelligence certify areas of foreign intelligence to be gathered; the FISC reviews and approves those certifications; the executive branch serves directives on communications

---

[3] *See* Testimony of Matthew G. Olsen before the Senate Committee on the Judiciary, May 10, 2016, p. 7, available online at: https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf

[4] "Because of these changes in technology, communications intended to be excluded from FISA in 1978 were, in fact, frequently included in 2007. This had real consequences. It meant the community in a significant number of cases was required to demonstrate probable cause to a court to collect communications of a foreign intelligence target located overseas." Testimony of Director McConnell before the Senate Select Committee on Intelligence, Sept. 20, 2007, available online at https://www.gpo.gov/fdsys/pkg/CHRG-110jhrg38878/html/CHRG-110jhrg38878.htm .

[5] *See* the Joint Unclassified Statement of Robert S. Litt, General Counsel Office of the Director of National Intelligence; Stuart J. Evans Deputy Assistant Attorney General for Intelligence, National Security Division, Department of Justice; Michael B. Steinbach, Assistant Director Counterterrorism Division, Federal Bureau of Investigation; and Jon Darby, Chief of Analysis and Production, Signals Intelligence Directorate, National Security Agency Before the House Committee on the Judiciary, United States House of Representatives, February 2, 2016, available online at: https://judiciary.house.gov/wp-content/uploads/2016/02/joint-sfr-for-doj-fbi-odni-and-nsa-updated.pdf .

[6] https://www.judiciary.senate.gov/meetings/oversight-and-reauthorization-of-the-fisa-amendments-act-the-balance-between-national-security-privacy-and-civil-liberties

providers; and the intelligence agencies designate and document the individual selectors that meet the detailed criteria required under the statute, certifications, and targeting procedures.[7] The collection is effectuated by two means: 1) through PRISM collection in which electronic communications service providers assist the government in acquiring communications that are to or from targeted selectors, and 2) through "upstream" collection in which telecommunications backbone providers assist the government in acquiring telephony communications to or from a targeted selector and internet transactions that are to, from, or about a targeted selector.[8] The information, once acquired, is handled in accordance with Court-approved minimization procedures that govern the processing, analysis, retention, and dissemination of the data. These minimization procedures are an essential part of the overall set of measures that makes the FAA 702 an appropriately circumscribed program.

2. FAA 702 APPROPRIATELY BALANCES INDIVIDUAL PRIVACY AND NATIONAL SECURITY

The first and most important point to make is that, despite some public misconceptions to the contrary, FAA 702 is a targeted intelligence authority. It is not "bulk" collection. As explained by the independent Privacy and Civil Liberties Oversight Board (PCLOB) in its July, 2014 report, "The statutory scope of Section 702 can be defined as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the 1) targeting of persons who are not United States persons, 2) who are reasonably believed to be located outside the United States, 3) with the compelled assistance of an electronic communication service provider, 4) in order to acquire foreign intelligence information."[9]

In more concrete terms, FAA 702 collection can only be initiated when an analyst is able to articulate, and document, a specific set of facts to meet the statutory and procedural requirements for demonstrating that: 1) a specific "facility" (such as a phone number or email address) 2) is associated with a specific user 3) who is a non-U.S. person 4) who is reasonably believed to be located outside the U.S. and 5) who is likely to possess or communicate foreign intelligence information.[10]

Although a large number of selectors have been targeted under FAA 702, each of those selectors has been tasked for collection because *on an individual, particularized basis* each one of them meets the criteria noted above.[11] "Bulk" collection is different: as explained in

---

[7] *See generally* 50 U.S.C. 1881.

[8] In all cases, PRISM and upstream, the basis for collection is a communications identifier, such as an email address or telephone number. FAA 702 does not authorize, and is not used for, the collection of communications based on key words, names, or generic terms. *See* PCLOB report, p. 33-41.

[9] PCLOB Report, p. 20, citing 50 U.S.C. §1881a(a), 1881a(b)(3), 1881a(g)(2)(A)(vi).

[10] *See* 50 U.S.C. §1881a(a),(b); *see also* Semi-Annual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702, August, 2013, p. A-1- A-2, available online at: https://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf ; *and see* Oversight Summary prepared by Department of Justice and Office of the Director of National Intelligence, Aug. 11, 2016, p. 2, available online at: https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of .

[11] *See* PCLOB Report, p. 103.

"Presidential Policy Directive – Signals Intelligence Activities" (PPD-28), bulk collection is information that is collected without the use of discriminants.[12] This is a critically important difference. As the PCLOB noted in its report, Section 702 does not authorize bulk collection.[13]

Further, once the information has been collected under FAA 702, the information is subject to a significant number of post-collection safeguards that are captured in lengthy, detailed minimization procedures that demonstrate both the care that is taken with the information, and the complexity of the 702 framework.[14] At a high level, the procedural protections include both technical and administrative means. For example, 702 information in stored in restricted-access information systems where the data can be identified as having been collected under, and being subject to, FAA 702 minimization procedures. NSA personnel are only permitted to access the information if they have taken specialized training on those procedures, passed the associated training exam, and have continued to update their training and pass the associated tests on an annual basis. Similar requirements exist for CIA and FBI personnel.[15] Many of these protections are detailed in documents issued by DoJ and ODNI, and I discuss some of these protections in further detail below.

Because of the tailored, documented, and carefully overseen manner in which the front-end collection is carried out, it is neither unlawful nor inappropriate for intelligence analysts to query the collected information using U.S. person identifiers when there is a legitimate basis to do so. Some critics have referred to the ability to query 702 data for U.S. person information as "back door searches." That hyberbolic phrase doesn't help illuminate the true issues – the intelligence benefits or the privacy risks – that are stake. First, it is important to understand how such queries actually happen. As the PCLOB noted in its report, the use of query terms relating to U.S. persons is tightly constrained at both NSA and CIA, which have similar practices; FBI takes a different approach.[16] I'm most familiar with NSA's processes: NSA analysts must obtain prior approval to run U.S. person identifier queries in FAA 702 content; there must be a basis to believe the query is reasonably likely to return foreign intelligence information; all

[12] PPD-28 notes that, "References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)." https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities#_ftn5

[13] PCLOB Report at 103, available online at: https://www.pclob.gov/library/702-Report.pdf .

[14] These procedures have been declassified, with minor redactions, and released for public review. For example, the 2014 procedures include NSA Section 702 Minimization Procedures, available online at: https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf . The FBI Section 702 Minimization Procedures are available online at: https://www.dni.gov/files/documents/0928/2014%20FBI%20702%20Minimization%20Procedures.pdf . The CIA Minimization Procedures are available online at: https://www.dni.gov/files/documents/0928/2014%20CIA%20702%20Minimization%20Procedures.pdf and the NCTC Minimization Procedures are available online at: https://www.dni.gov/files/documents/0928/2014%20NCTC%20702%20Minimization%20Procedures.pdf .

[15] *See* PCLOB Report at p. 53, 127, available online at: https://www.pclob.gov/library/702-Report.pdf.

[16] PCLOB Report at p. 129-131, available online at: https://www.pclob.gov/library/702-Report.pdf.

queries are logged and reviewed after the fact by NSA; and DoJ and ODNI review every U.S. person query run at NSA and CIA, along with the documented justifications for those queries.[17]

As a practical matter, internal agency mechanisms also provide strong protections against abuse. For example, within the NSA intelligence oversight framework, query auditors and intelligence oversight officers play an active role in checking for errors or unauthorized queries. Throughout my time at NSA, I routinely saw analysts self-report if they ran an improper query; auditors actively review and assess query logs for any indication of any improper query; and questionable queries are reported promptly to NSA's internal intelligence oversight officers and organizations for further action, which includes reporting to external overseers.

Writ large, the government has put in place detailed mechanisms to protect individual privacy within the 702 framework, including measures to guard against the overuse or improper use of queries the deliberately search for U.S. person information in Section 702 data.

3. The Statutory Framework Establishes Robust and Effective Oversight Mechanisms

In designing this statute, Congress wisely chose to build in oversight mechanisms involving all three branches of government.

Four committees of Congress have oversight jurisdiction of the government's activities under Section 702: this Committee, the Senate Committee on the Judiciary, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence. The statute requires the Attorney General to provide Congress with a semiannual report assessing the government's compliance with the targeting and minimization procedures of the 702 program, along with additional information regarding compliance with the statutory constraints on targeting.[18] As noted by the PCLOB in its 2014 Report, "In practice, the government provides the four committees all government filings, hearing transcripts, and FISC orders and opinions related to the court's consideration of the Section 702 certifications," along with any reports by agency inspectors general.[19]

The FISC also plays a central and critical role in oversight of the 702 program. Under the requirements of the program's procedures and the rules of the FISC, the government must report compliance incidents either immediately upon recognition or as part of quarterly reporting.[20]

---

[17] Oversight Summary prepared by Department of Justice and Office of the Director of National Intelligence, Aug. 11, 2016, p. 3, 4, available online at: https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of

[18] 50 U.S.C. § 1881b, 1881f, 1881l.

[19] PCLOB Report at 77.

[20] *See* FISC Rules of Procedure, available online at: http://www.fisc.uscourts.gov/rules-procedure Specifically, Rule 13(b), "Disclosure of Non-Compliance" states that, "If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made of: 1) the non-compliance; 2) the facts and circumstances relevant to the non-compliance; 3) any modifications the government has made or proposes to make in how it will implement any authority or approval

These "13(b)" notices contain comprehensive details about the nature of each incident of non-compliance, and are filed promptly and routinely. It is not uncommon for the FISC to ask the government to provide supplemental information, in writing or through in-person briefings, to address any questions that the court may have regarding those incidents. In addition to carrying out this ongoing oversight function, each year, the FISC reviews the government's annual certification package for sufficiency, making independent determinations about whether the proposed certifications meet the necessary standards set forth under the law; whether the targeting and minimization procedures faithfully incorporate all of the restrictions necessary to ensure that they are consistent with the statute and with constitutional requirements; and reviewing the compliance incidents that have taken place over the past year. Each of those compliance incidents will have been previously reported to the FISC, either upon recognition or as part of quarterly reporting. However, the annual certification package provides the FISC with an opportunity to review in total the compliance incidents over the course of a year, to assess whether any trends can be identified or whether there are particular issues that are cause for concern, and to hold the government to account for providing additional information on the nature of those incidents, any steps that might have prevented them from happening, and the details of any remedies that the government may have put in place to correct them or prevent similar occurrences in the future. Further evidence of the FISC's close attention to and careful scrutiny of the government's activities under FAA Section 702 can be found in the court's November 6, 2015 Memorandum Opinion and Order regarding the 2015 FISA Section 702.[21]

It would also be useful to consider here a potential component of oversight that *isn't* currently required by the statute. Members of this Committee, along with others, have asked the government for information regarding the number of U.S. person communications that are collected through the use of the FAA 702 authority. I'd like to offer here some perspective on the practical, policy, and privacy obstacles to making such a count.

As noted above, when the government collects communications under FAA 702, it stores those communications in databases or systems that protect the collected information from unauthorized access, that support queries of the textual information and support the ability to listen to telephonic communications, and that log queries into the systems so that they can be reviewed for lawfulness and consistency with policy. All of these processes are designed around the goal of producing foreign intelligence information, *not* around an intention to look for U.S. person information. Although in theory such searches for U.S. person information could be made, the process of identifying which unknown identifiers are associated with U.S. persons would require the Intelligence Community to deliberately hold and analyze information about U.S. persons, information that it would otherwise have no reason to collect or retain.

Imagine, for a moment, the communications of a non-U.S. person outside the U.S. who is believed to be associated with international terrorism. Further imagine that selectors associated with that person were targeted under Section 702. Once that information has been collected and stored in a database, it can be queried by appropriately cleared and trained analysts. The

---

granted to it by the Court; and 4) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance."

[21] https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

analyst's query will be designed to search for those communications that have intelligence value. As they review those communications, they will almost certainly encounter other identifiers – other emails addresses, phone numbers, and the like – that the tasked selector is in communication with, but that are unfamiliar to the analyst. The analyst would need additional information in order to assess whether those unknown identifiers are being used by people in the U.S., or by U.S. persons anywhere in the world. In some cases, technical information may help assist with the location determination. But technical information generally cannot identify whether the user of an email account happens to be a U.S. person located somewhere else in the world. If the communication itself appears to have no intelligence value, the analyst has little reason to research the possible identity, nationality or location of that identifier.

The minimization procedures anticipate precisely how to address this situation: when an analyst determines that a communication contains information that should be disseminated in an intelligence report, the analyst will assess whether the other identifiers are relevant to the intelligence (in some cases, they are not). If not, the report will be written in a way that omits mention of that identifier. If the identifier is relevant, the analyst will look for any indications that the non-target communicant is a U.S. person or a person in the U.S. If that's the case, then that identifier or user's identity (if known) may be masked in any resulting reports. This approach complies fully with the 702 minimization procedures.

From a policy and privacy perspective, the current approach – in which analysts only research unknown identifiers when they appear likely to be of intelligence interest – is a sound and sensible one that protects privacy, conserves resources, and helps the government focus on the highest intelligence priorities. A requirement to count the number of U.S. person communications that are incidentally acquired under Section 702 would require the Intelligence Community to conduct exhaustive analysis of every unknown identifier in order to determine whether they are being used inside or outside the U.S., and whether their users might be U.S. persons located anywhere in the world. NSA does not – nor should it – collect or maintain comprehensive directories of the communications identifiers used by U.S. persons. However, in order to perform a reliable count of U.S. person communications in 702 collection, the Intelligence Community would have to create and maintain precisely such a database. The very creation of these reference databases would constitute an unnecessary and unwarranted intrusion on the privacy of U.S. persons; without specific statutory authorization, it would likely also be unlawful, since it would be both intrusive and unrelated to any need for foreign intelligence gathering.[22] Further, searching for U.S. person information would require intelligence agencies to divert scarce analyst time and computing resources away from intelligence activities in order to hunt for the communications of U.S. persons whose information is not related to an authorized intelligence need (and whose information would never be looked at by the government but for this requirement). Finally, it is unlikely that knowing the number or percentage of U.S. persons in a particular sample of data would result in increased privacy protections in the future: first, because target sets vary over time, and therefore it isn't clear whether numbers or percentages of incidental collection would be constant over time; and second, because the fundamental challenge remains an intractable one: as long as foreign intelligence targets communicate with

[22] Even with statutory authorization, the creation of such a comprehensive database would raise Constitutional concerns.

U.S. persons, it will not be possible to avoid the incidental collection of those specific communications.[23] The best way to protect the privacy of incidental U.S. person communications is to advise analysts that they should *not* proactively search for communications that lack intelligence value, nor conduct exhaustive research to determine whether the unknown communicants in irrelevant communications might be U.S. persons or persons in the U.S.

A middle-ground approach to this challenge is the most appropriate one. The currently implemented practice, adopted in response to PCLOB recommendations and consistent with the USA FREEDOM Act, of reporting on the number of U.S. person queries and the number of disseminations of nonpublic information relating to U.S. persons[24] are appropriate measures that should be continued. The recommendation to report on instances of U.S. person information when it is found and identified as such is one that will impose additional resource burdens on the government but could be another measured and balanced approach to this problem, particularly if used for sampling or for a limited period of time.[25] However, requiring a proactive search through 702 databases for all information relating to U.S. persons would – because of the information it would require the government to collect and hold and because of the resources that would be diverted – be unreasonably intrusive on privacy and ill-advised.

4. SECTION 702 OVERSIGHT IS IMPLEMENTED IN COMPREHENSIVE, THOROUGH WAYS

In addition to being structurally sound, the oversight mechanisms for FAA 702 function robustly in practice. The intelligence agencies have rigorous internal oversight and compliance programs. DoJ and ODNI are deeply engaged in detailed scrutiny of targeting decisions, queries, minimization, and compliance incidents. The FISC is actively involved in oversight and is extremely well equipped to do so: the life-tenured federal judges who are appointed to serve on the FISC demonstrate independence from the Executive and Legislative branches of government, as well as independence from each other. In addition, FISC judges are ably supported by court advisors who, on the judges' behalf, press the government for additional information that may be relevant or necessary to understanding a particular court filing or compliance incident report. Further, the USA Freedom Act brought with it the mechanism for naming independent attorneys as amicus curiae, available to be called upon to provide briefings to the FISC in its consideration of novel matters. Finally, of course, there is the legislative branch, where this Committee plays a vital role.

---

[23] Here, it's important to remember that incidental collection doesn't sweep in all of the communications of a particular U.S. person. It only picks up those specific instances in which that U.S. person has been in communication with a foreign intelligence target. All other communications of that U.S. person remain unaffected, and uncollected.

[24] *See* Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report, February 5, 2016, Recommendation 9, "Adopt Measures to Document and Publicly Release Information Showing How Frequently the NSA Acquires and Uses Communications of U.S. Persons and People Located in the United States," available online at: https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf .

[25] Tracking indefinitely the instances in which incidental collection is identified as being associated with U.S. persons could, over time, raise new privacy concerns associated with the government's creation and retention of databases of information relating to U.S. persons who are not intelligence targets.

It may be useful to offer additional details about the practical oversight that takes place within the executive branch. These oversight mechanisms have been described in detail in a number of reports[26] as well as an August, 2016 memo issued by DoJ and ODNI.[27] The summary below draws on many of these publically available sources, as well as my own experience with oversight mechanisms for FAA 702.

The joint intelligence oversight reviews conducted by DoJ and ODNI include review of a broad and comprehensive range of detailed documentation regarding the day-to-day implementation of intelligence activities under FAA 702. These include NSA and FBI targeting decisions; reviewing U.S. person identifiers approved by NSA for querying unminimized 702 data; reviewing CIA content queries of unminimized FAA 702 data; reviewing FBI queries of unminimized FAA 702 data; reviewing disseminations of 702 data by NSA, FBI, and CIA; reporting to the FISC and to Congress every instance of non-compliance that is identified; and assessing the Intelligence Community's implementation of appropriate remedial actions to address compliance matters, including purging of non-compliant data and recalling non-compliant disseminations.[28]

At bimonthly visits (often referred to as "60-day reviews"), DoJ and ODNI scour through detailed documentation of targeting decisions, queries, and reporting. NSA prepares exhaustively for these visits, pulling together detailed information on targeting rationales, targeting sheets, query records, and intelligence product reporting. DoJ and ODNI meet with NSA's attorneys and oversight and compliance officers, as well as with analysts and technology personnel as needed in order to answer questions. These 60-day reviews are by no means the only interactions on 702; there are near-daily phone calls, emails, and in-person discussions among NSA, DoJ, and ODNI about current and potential operational and compliance matters, whether those are upcoming reviews, follow-up questions, potential incidents that are being investigated, authorization discussions, or other matters. The dialogue is a robust, continuous, and ongoing one in which DoJ and ODNI both maintain independent professional judgment and distance from the people and organizations they are responsible to oversee. Because the tone of interactions can't be easily captured with metrics, it's hard to convey just how thorough and exhaustive the oversight is, beyond providing this Committee with the observation that I have consistently seen the Department of Justice and ODNI approach their oversight responsibilities with rigor, thorough attention to detail, and a dogged and fully formed intent to ferret out any indication of actual or potential error. Although my direct experience, of course, lies with NSA,

---

[26] Among the most important sources are the PCLOB's "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", July 2, 2014, available online at: https://www.pclob.gov/library/702-Report.pdf and the "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence" and the Office of the Director of National Intelligence's "Assessment of Oversight & Compliance with Targeting Procedures"; these reports are available online at: https://icontherecord.tumblr.com/post/155810963663/release-of-joint-assessments-of-section-702 .

[27] https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of

[28] Oversight Summary prepared by Department of Justice and Office of the Director of National Intelligence, Aug. 11, 2016, available online at: https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of .

I would expect that DoJ and ODNI take a similar approach to their oversight interactions with FBI and CIA.

Equally important to these external checks, the use of the FAA 702 authority takes place within a deeply rooted culture of compliance. Again, my greatest familiarity is with the NSA, where a number of detailed internal procedures are rigorously adhered to in order to support effective compliance with the statute and applicable procedures. For example, NSA analysts review traffic from all newly tasked selectors to ensure it is associated with the intended target. Queries into unminimized data are captured in detailed logs that are audited to look for query errors. And NSA's compliance structure includes having personnel with different backgrounds and areas of focus (such as analysis, technical capabilities, dissemination) spread throughout the organization in order to be able to provide oversight of 702 activities and support to compliance-related questions.[29] The longstanding message that has been reinforced within NSA is that it is a privilege to be entrusted with the responsibility to self-report incidents of non-compliance; that the way to keep that privilege is to be forward-leaning at all times on reporting compliance incidents when they arise; and that if it is unclear whether a particular situation constitutes an incident of non-compliance, to err on the side of over-reporting. Although critics will point to instances in which NSA was slow to recognize that errors had been made, I would respond to those criticisms by pointing out the extraordinary technical complexity involved in executing NSA's missions under its existing authorities. In thirteen years at NSA, I often saw mistakes that resulted from human error that were quickly identified and promptly reported and remediated. I also saw instances in which technical complexity led to errors that hadn't been foreseen; those, too, were reported upon recognition and addressed, but sometimes were harder to identify. However, I did not see people deliberately taking actions that would abuse the trust placed in them in handling this very sensitive data. In other words, my experience was entirely consistent with the PCLOB's finding that, "Although there have been various compliance incidents over the years, many of these incidents have involved technical issues resulting from the complexity of the program, and the Board has not seen any evidence of bad faith or misconduct."[30]

As someone who, today, advises private sector entities on cybersecurity and privacy, I'm well attuned to the fact that among the most important factors in a successful privacy or compliance program are maintaining a culture of compliance, and setting that tone from the top. During my years at NSA, I saw both of those factors as daily and present realities. It's hard to provide metrics or quantitative information to support a statement like this one. After all, the indicia of privacy and compliance programs – policies, procedures, training, and the like – can be present both in environments in which they are fostered, supported, and enhanced by a culture of compliance, and also in organizations in which the compliance program exists in tension with the larger organizational culture. At NSA, I had the opportunity to work in policy, technology, operations, oversight and compliance, foreign relations, and law, and I had the opportunity to work in and visit a number of NSA locations. I was left repeatedly with the same consistent impression: NSA has a workforce that is deeply committed to the principles of the oath they

[29] *See generally* NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, April 16, 2014, available online at: https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_report_on_section_702_program.pdf

[30] PCLOB Report, p. 8.

swore to protect and defend the Constitution; it's a team of people who work hard to understand complex areas of law, policy, regulation, and procedure and how those apply in practical terms to the everyday work that they're doing; and it's an Agency whose staff are dedicated to doing their work in compliance with the law. There have certainly been errors in executing this complex program, but my experience has been consistent with the findings of the PCLOB and others that – over the course of nearly a decade, in a very large Agency – there has been no indication of intentional misuse of the 702 authority.

5. FAA 702 IS A CRITICAL TOOL IN INTELLIGENCE GATHERING

Throughout thirteen years at NSA, I had the opportunity to witness firsthand the critical importance of robust intelligence information in supporting U.S. troops and in detecting terrorist plans and intentions that threatened the safety of the U.S. and its allies. I had a front-line view of these impacts when I managed counterterrorism information sharing programs both before and after the passage of FAA.

Many of those instances are recent and remain classified, and I assume that many of those intelligence successes have been or will be briefed to this Committee in closed session. However, the fact that many details remain classified should not, in my view, cause concern or alarm for privacy advocates or the public at large, for two reasons. First, our democracy has been deliberately structured to empower you, as our elected officials, to stand in the shoes of the constituents whom you represent. Your ability to scrutinize government programs rigorously, inquire about them thoughtfully, and oversee them vigorously are key reasons why the public may, and should, have confidence that this authority is being used as intended and in ways that are consistent with the laws, policies, and principles of our nation. Together with oversight from independent federal judges, overlapping oversight mechanisms within the executive branch, and independent boards and agencies such as the PCLOB, this law has been structured to afford the public a wealth of surrogates who are authorized and empowered to carry out effective oversight on their behalf. Second, while it would be reckless for the government to divulge all of its national security information to the public as a whole, the national security establishment has made significant strides in recognizing the importance of moving towards as much transparency as possible regarding the manner in which national security programs like this one are carried out and overseen. This kind of transparency is an area in which the Intelligence Community clearly fell short in the past; it is also an area in which it has made genuine progress in recent years. Those efforts should be applauded and continued. Indeed some of those transparency requirements are underpinned both by the statute itself, in its requirements for Semi-Annual Assessments and Annual Reviews,[31] and the Intelligence Community's recent practice of declassifying much of the information contained in those documents.[32]

---

[31] 50 U.S.C. §1881(l).

[32] *See, e.g.,* the release on July 21, 2016 of the Tenth, Eleventh, and Twelfth Semi-Annual Joint Assessments, collectively covering the time period from Dec. 1, 2012 through . The Joint Assessment covering December 1, 2012 through May 31, 2013 is online at: https://www.dni.gov/files/documents/10thJA-FINAL_REDACTED.pdf . The Joint Assessment covering June 1, 2013 through November 30, 2013 is online at: https://www.dni.gov/files/documents/11thJA-FINAL_REDACTED.pdf . The Joint Assessment covering Dec. 1, 2013 through May 31, 2014 is online at: https://www.dni.gov/files/documents/12thJA-FINAL_REDACTED.pdf .

In addition to the intelligence successes that remain classified, I would draw the Committee's attention to the unclassified information that has been released regarding the critical importance of this authority in gathering foreign intelligence information. In its 2014 report, the PCLOB noted that:

> "[O]ver a quarter of the NSA's reports concerning international terrorism include information based in whole or in part of 702 collection, and this percentage has increased every year since the statute was enacted. Monitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics. In addition, the program has led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United states and other countries."[33]

In more recent testimony before the Senate Committee on the Judiciary, a number of witnesses have underscored the national security importance of 702 collection. These included Matthew G. Olsen, former director of the National Counterterrorism Center, Kenneth L. Wainstein, and Rachel Brand, at the time a member of the President's Civil Liberties and Oversight Board.[34] In a previous hearing before this committee, government officials from the Office of the Director of National Intelligence, the Department of Justice, the Federal Bureau of Investigation and the National Security Agency all testified to the vitally important nature of the intelligence information that is gathered under Section 702 and that would not be available without this authority.[35]

Having seen firsthand the challenges faced by the Intelligence Community in obtaining critical intelligence information, particularly relating to terrorism, prior to the enactment of FAA 702, as well as the significant foreign intelligence produced through the use of this authority since 2008, there is no doubt in my mind that loss of this authority would have a devastating effect on intelligence gathering, undermining the security of both the U.S. and our allies.

It's my belief, based on my personal experience and professional judgment, that Congress drew the balance of authority and restrictions in the right place when it enacted FAA 702 in 2008 and when it reauthorized it in 2012. As debate proceeds throughout this year on whether to renew this provision, and in what form, I would urge Congress to reauthorize this statute in a

---

[33] PCLOB report at 10, https://www.pclob.gov/library/702-Report.pdf

[34] *See generally*, Olsen statement at 1-7, Wainstein statement at 2-3, Brand statement at 12. All are available online at: https://www.judiciary.senate.gov/meetings/oversight-and-reauthorization-of-the-fisa-amendments-act-the-balance-between-national-security-privacy-and-civil-liberties

[35] Joint Unclassified Statement of Robert S. Litt, General Counsel Office of the Director of National Intelligence; Stuart J. Evans Deputy Assistant Attorney General for Intelligence, National Security Division, Department of Justice; Michael B. Steinbach, Assistant Director Counterterrorism Division, Federal Bureau of Investigation; and Jon Darby, Chief of Analysis and Production, Signals Intelligence Directorate, National Security Agency Before the House Committee on the Judiciary, United States House of Representatives, February 2, 2016, available online at: https://judiciary.house.gov/wp-content/uploads/2016/02/joint-sfr-for-doj-fbi-odni-and-nsa-updated.pdf .

form that adopts the same language as, or that remains fundamentally consistent with, the existing statutory framework.

Thank you once again for the privilege of offering this testimony for your consideration. I look forward to addressing any questions you may have.