Testimony of Rachel L. Brand, Member of the Privacy and Civil Liberties Oversight Board, before the United States Senate Committee on the Judiciary

May 10, 2016

Mr. Chairman, Ranking Member Leahy, and Members of the Committee, thank you for the opportunity to testify today.

Introduction

I am a Member of the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board"), an independent executive branch agency charged with ensuring that the nation's need for strong and effective counterterrorism programs is balanced with protecting privacy and civil liberties.

I appear before the Committee today in my capacity as an individual Member of the Board. Although my testimony discusses the Board's report, I speak for myself and not for the Board.

In 2014, the PCLOB conducted an in-depth study of the NSA's intelligence collection conducted under Section 702 of the Foreign Intelligence Surveillance Act (the "702 program"). Certain details about this program had previously been leaked to the press and then declassified. After concluding its study, the Board published a lengthy public report ("report") explaining the program in detail and analyzing its legality, policy implications, and operational effectiveness.[1] The Board's report became the authoritative source of accurate and complete information about this highly complex intelligence program. The report dispelled a number of mischaracterizations and misperceptions that had pervaded the public debate about the program.

The Board found that:

- Under Section 702, the government engages in *targeted* collection of telephone and internet communications of *non-U.S. persons located abroad* who are likely to communicate information about a court-approved set of *foreign intelligence* topics.
- The 702 program has strict, court-approved targeting and minimization procedures that protect all persons' privacy and provide special protections for U.S. persons.
- It is subject to oversight by all three branches of government.
- It is reasonable under the Fourth Amendment and authorized by Congress.
- It is highly effective as a source of valuable foreign intelligence.

The Board did, however, identify certain aspects of the program – including the fact that some U.S. person communications will be incidentally collected – that have privacy and civil liberties

[1] "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," https://www.pclob.gov/library/702-Report-2.pdf ("Report"). The Board found the NSA and the rest of the Administration to be cooperative in facilitating our review of the program and in providing the necessary information and documentation. They also worked cooperatively with the Board during the pre-publication review process and agreed to declassify additional facts in order to permit a more comprehensive unclassified description of how the program works.

implications. The Board made several policy proposals to alter those aspects of the program. The Administration has since implemented each of these recommendations in whole or part.

It is worth noting that the Board's five independent members unanimously adopted the report's central conclusions, and we were unanimous in almost all of our recommendations for tightening the program's privacy protections.

The 702 program

Background

The Foreign Intelligence Surveillance Act ("FISA") provides the statutory procedure under which the government may collect foreign intelligence inside the United States. When FISA was enacted in 1978, it allowed the government to obtain an order from the Foreign Intelligence Surveillance Court ("FISA Court") to wiretap a foreign power or agent of a foreign power at a location inside the United States. These original provisions of FISA (which are still in effect) require a showing of probable cause that the telephone to be wiretapped is used by a foreign power or agent of a foreign power. Over the years, Congress has amended FISA in a variety of ways, some of which address technological developments since 1978. When enacted, FISA applied to collection in the United States; it was never intended to cover collection of communications of non-U.S. persons outside the United States. FISA's original 1978 text did not account for the current technological environment in which a communication between two individuals located outside the United States might transit through the United States. Section 702, enacted in 2008, was intended in part to address that scenario.[2]

What Section 702 authorizes

Under Section 702, the government may collect (at a point inside the United States) the telephone and internet communications of non-U.S. persons located outside the United States who are likely to communicate foreign intelligence information about certain subjects that have been certified by the Attorney General and Director of National Intelligence ("DNI"). Before the government can collect any data under this program, the FISA Court must approve the "certifications" as well as strict rules for the program known as "targeting procedures" and "minimization procedures."

Limitations on Collection

Section 702 contains several important limitations on collection:

Section 702 is a targeted program. The PCLOB report specifically rebutted the notion that Section 702 authorizes "bulk" collection.[3] Instead, the government must "target" particular non-U.S. persons located abroad. To begin collection, the government must identify a specific

[2] *See* Report at 19-20; *see also* Joint Unclassified Statement of Robert S. Litt, Stuart J. Evans, Michael B. Steinbach, and Jon Darby, Senate Committee on the Judiciary, Briefing on the FISA Amendments Act (March 8, 2016), at 2-3.

[3] *See* Report at 103.

"selector" that is used by the potential target.[4] Collection can only be effectuated by "tasking" this particular "selector."[5] A "selector" must be a specific communications facility such as a telephone number or email address – it cannot be a name, word, or phrase.[6]

Under Section 702, a person cannot be targeted for collection unless the person meets three requirements. Specifically, the person must be:

1) A non-U.S. person. A U.S. person may never be targeted under Section 702.[7]
2) Located outside the United States. No person physically present in the United States – regardless of nationality – may be targeted under Section 702. If a person who was properly targeted while he was located outside the United States later travels to the United States, collection generally must stop.[8]
3) Likely to communicate foreign intelligence information. Section 702 does not permit targeting of every foreign person. The government must believe that a person is likely to communicate foreign intelligence information. More specifically, the person must be likely to communicate information about the subjects that have been certified annually by the Attorney General and DNI with the approval of the FISA Court.[9] Although the exact subjects of 702 certifications remain classified, the PCLOB report noted that they "include information concerning international terrorism and … acquisition of weapons of mass destruction."[10]

Thus, before targeting any person, the government must make both a "foreignness" determination (non-U.S. person located outside the United States)[11] and a "foreign intelligence purpose" determination.[12]

"Reverse targeting" – such as targeting a non-U.S. person outside the United States for the purpose of acquiring the communications of a U.S. person – is specifically prohibited.[13]

---

[4] *See id.* at 42-43.
[5] *Id.* at 32-33.
[6] *See id.*at 33, 111-12.
[7] *See id.* at 43-45*; see also* sec. 702(b)(3), FISA Amendments Act of 2008, 50 U.S.C. 1881a(b)(3). The Board noted that FISA and the FISA Amendments Act define the term "United States person" to include not only U.S. citizens and lawful permanent residents, but also unincorporated associations with a substantial number of U.S. citizens or lawful permanent residents as members, as well as corporations incorporated in the United States. The term does not, however, include either associations or corporations that meet the statute's definition of a "foreign power." Report at 106, n. 466 (citing the FISA definitions of "United States person" at 50 U.S.C. 1801(i) and of "foreign power" at 50 U.S.C. 1801(a)(1)-(3)).
[8] At the time of the Board's report, the NSA was required to "promptly detask[]" a selector if the target was discovered to have traveled into the United States. Report at 49. This aspect of Section 702 was amended by the USA Freedom Act to allow collection to continue, under certain limited circumstances, for up to 72 hours after the non-U.S. person target is believed to have entered the United States. *See* sec. 701(a)(2), USA Freedom Act (P.L. 114-23), codified at 50 USC 1805(f) .
[9] *See* Report at 6, 24-25.
[10] *Id.* at 6.
[11] Report at 23.
[12] *See id.* at 43.
[13] *See id.* at 23.

The statute also prohibits the government from intentionally collecting a communication "as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[14]

Incidental Collection of U.S. Person Communications

The fact that U.S. persons cannot be targeted does not mean that U.S. persons' communications will never be collected under Section 702. For example, if a targeted non-U.S. person located abroad communicates with a U.S. person, then those communications will be collected. This is referred to as "incidental" collection.[15]

Incidental collection is not the same as "inadvertent collection," which is collection by mistake.[16] Rather, incidental collection is inevitable, permitted by the statute, and was anticipated by Congress when Section 702 was enacted. In fact, incidentally collected communications indicating a connection between a terrorist located abroad and someone located inside the United States could be among the most important communications collected under the program.[17]

Nonetheless, incidental collection of U.S. person communications has obvious implications for the privacy and constitutional rights of U.S. persons. Because Congress understood the inevitability of incidental collection and its implications for privacy and other rights, it required the government to operate the program under strict, FISA Court-approved procedures. These procedures contain specific rules limiting the government's treatment and use of information concerning U.S. persons. They are discussed further below.

Two Means of Targeted Collection: PRISM and Upstream Collection

Once a targeted person and a particular "selector" have been identified, communications are collected through two mechanisms. One is referred to as "PRISM," the other as "upstream." Both forms of collection occur with the compelled assistance of service providers.[18]

In PRISM collection, once the agency identifies a certain selector that is used by a targeted person, it sends the selector to an Internet Service Provider ("ISP") that has previously received a written directive compelling the company to provide NSA with the communications to and from identified selectors.[19] The ISP provides communications sent to or from that selector to the government. While the NSA receives all the communications collected through PRISM, the CIA and FBI each receive only a subset.[20]

---

[14] 50 U.S.C. 1881a(b)(4).
[15] *See* Report at 114-15.
[16] *See id.* at 114. If communications are collected by mistake, such as if a U.S. person is erroneously targeted or collection occurs due to a technical malfunction, the collection must cease once the mistake is discovered, and the communications generally must be deleted. *See id.* at 6.
[17] *See id.* at 114-15.
[18] *See id.* at 33.
[19] *See id.*
[20] *See id.* at 7.

In upstream collection, telephone and electronic communications are collected from the telecommunications backbone.[21] As with PRISM collection, upstream collection involves tasking specific selectors associated with targeted non-U.S. persons located outside the United States. For telephone communications, the NSA sends a selector to a company, which is required to provide the government with telephone communications to and from that selector.[22]

Upstream collection of internet communications is done with the compelled assistance of the electronic communications providers that operate the "internet backbone."[23] Tasked selectors are sent to a provider to acquire communications transiting circuits used to facilitate internet communications.[24] To collect transactions associated with tasked selectors from the backbone of the internet, two filters are applied. First, transactions are "filtered to eliminate potential domestic transactions." Second, they are "screened to capture only transactions containing a tasked selector." If a transaction does not pass both these screens, it is not ingested into the NSA's database.[25]

Upstream collection has a higher likelihood than PRISM of collecting some communications that are not to or from targeted individuals and some wholly domestic communications. The first reason for this is so-called "about" collection. In upstream internet collection, the NSA will collect a communication in which a selector appears anywhere, even if the communication is not to or from the selector. For example, in the case of an email, if the selector appeared in the body of an email, not just the "to" or "from" field, that communication would be collected.[26] Thus, "about" collection could encompass some communications between two individuals who are not targets and some purely domestic communications.[27] The NSA uses technical measures, such as IP filters, to acquire '"about" communications without violating the statute's prohibition on knowingly collecting purely domestic communications. These filters are very effective, but not perfect.[28] This issue affects only upstream internet collection – not PRISM collection, and not upstream telephony collection.[29] Upstream collection of internet transactions represents about 9% of 702 internet collection.[30]

One common misconception about upstream collection was that the government used "about" collection to scan the internet backbone for words, themes, or names. The Board found that this is incorrect. Communications are only acquired if they are "about" a tasked "selector," such as a telephone number or email address associated with a targeted person.[31]

---

[21] *See id.* at 7, 35.
[22] *See id.* at 36.
[23] *See id.* at 35-36.
[24] *See id.* at 36-37.
[25] *Id.* at 37.
[26] *See id.* at 36-39.
[27] *See id.*at 38.
[28] *See id.* at 38-39.
[29] For telephone calls, the government acquires only calls "to" or "from" the tasked number. *See id.*at 36.
[30] *See* Report at 33-34 (noting that PRISM collection accounted for 91 percent of 702 collection).
[31] *See id*. at 119.

The Board found that "about" collection is an unavoidable aspect of upstream collection and that NSA could not completely eliminate it without also eliminating collection of a significant portion of communications to and from targets.[32] Although "about" collection occurs through several different technical means (the details of which remain classified) that have greater or lesser privacy implications, the NSA currently cannot eliminate one type of "about" collection without eliminating all of it.[33] The Board concluded that "[e]nding all 'about' collection would require ending even those forms …that the Board regards as appropriate and valuable, and that have very little chance of impacting the privacy of people in the United States….[G]iven a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable."[34] The Board did, however, recommend that the NSA develop technology to allow it to distinguish among forms of "about" collection so that a determination could be made about the appropriateness of each form.[35]

The second reason why some purely domestic communications might be collected upstream (but not in PRISM) is the collection of "multiple communications transactions" ("MCTs"). An MCT is an internet transaction containing multiple discrete communications. If one communication within an MCT is to, from, or about a tasked selector, the whole MCT will be collected.[36] This could result in collection of entirely domestic communications embedded in an MCT. The government has not found a way to filter MCTs to acquire only the discrete communication within the MCT that involves the 702 selector.[37] However, because of an MCT's potential to contain discrete communications that are not to or from a target or are between two points inside the United States, MCTs are subject to rules even stricter than the program's general rules.[38] In 2011, MCTs accounted for about ten percent of upstream collection.[39]

Rules governing collection and use of data under Section 702

Section 702 requires that the agencies adopt two sets of rules designed to ensure that the program complies with the statute and the Fourth Amendment and to minimize the program's privacy impact. These "targeting procedures" and "minimization procedures" must be approved by the FISA Court.[40] These procedures are highly complex, and my testimony touches only on the highlights. They are described in more detail in the Board's report.[41]

---

[32] *Id*. at 10, 35 n. 123, 38, 123.
[33] *See Id*. at 122-23.
[34] *Id*. at 123-24.
[35] *See Id*. at 124, 143-45.
[36] *See id*. at 7, 39-41.
[37] *See id*. at 40-41.
[38] *See id*. at 41, 85-86.
[39] *See id*. at 39.
[40] *See id*. at 26-29.
[41] *See id*. at 41-50 (targeting); 50-55 (minimization).

Targeting Procedures

The targeting process is governed by a detailed set of judicially approved "targeting procedures."[42] A key requirement is that the agencies use "due diligence" before determining that a target is a non-U.S. person located outside the United States. The Board's report corrected a myth that the NSA could assume a target was foreign based on a 51% probability or based on a single piece of information. In fact, if the agency has conflicting information about whether a person is inside the United States or is a U.S. person, that conflict must be resolved before he or she may be targeted.[43] The Board noted that the NSA's foreignness determinations have proved to be very accurate in practice.[44]

Among the other provisions of the NSA's targeting procedures are that the agency "detask" (i.e., stop collection on) selectors used by targeted persons who travel into the United States after being targeted; periodically ensure that it is appropriate to continue to task a selector; and purge (*i.e.*, delete) communications that should not have been collected.[45]

The targeting procedures also require NSA analysts to document the basis for foreignness determinations and foreign intelligence purpose determinations.[46] However, the Board judged the documentation requirement for the foreign intelligence purpose determination to be less rigorous than for the foreign intelligence determination. The Board recommended that analysts document foreign intelligence purpose in more detail to put those determinations on par with the detail required for foreignness determinations.[47] This recommendation has been implemented.[48]

Targeting decisions are subject to "extensive" before- and after-the-fact oversight.[49] Before collection on a particular selector can begin, two different senior NSA analysts must approve it.[50]

---

[42] The NSA is responsible for making targeting decisions. The FBI and CIA may "nominate" a selector to the NSA, but those agencies cannot direct the NSA to target a person or task a selector. That decision ultimately rests with the NSA after application of its targeting guidelines. *See* Report at 42. Selectors nominated by the FBI are subject to additional targeting restrictions; even if the NSA has determined a target to be a non-U.S. person located outside the United States, the FBI must review information available to it to "provide additional assurance" that the user of the tasked selector is a non-U.S. person outside the United States. *Id.* at 47.

[43] *See* Report at 43-44, 117.

[44] *See id.* at 44 (noting that a Justice Department oversight review of one year of foreignness determinations found that 0.4 percent of them were incorrect).

[45] *See id.* at 48-50.

[46] An NSA analyst would document foreignness by citing specific supporting documents and providing a narrative explanation. With respect to the foreign intelligence purpose determination, at the time of the Board's report, analysts were required to conduct an analysis, but documentation would typically consist only of noting the identity of the foreign power about which the target was expected to communicate foreign intelligence and very briefly stating why tasking the particular selector would produce information related to one of the certifications. *See* Report at 45-46.

[47] *See* Board Recommendation 1(b), discussed in Report at 134-37.

[48] *See* 2016 implementation status report at 15 (relating to Board Recommendation 1(b))*; see also* Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Redacted caption, Hogan, J. (Nov. 6, 2015), available at: https://icontherecord.tumblr.com/tagged/section-702.

[49] *See* Report at 8.

[50] *See id.* at 46.

After tasking, the National Security Division of the U.S. Department of Justice ("NSD") reviews every tasking sheet. The Office of the DNI ("ODNI") reviews a sample of them as well.[51]

Minimization procedures

Treatment of communications collected under Section 702 is governed by "minimization procedures" that impose limits on collection, retention, dissemination, and use of communications. They provide special protections for incidentally collected U.S. person communications, but many of their procedures protect U.S. persons and non-U.S. persons alike.[52]

Key provisions include the following. Data acquired under section 702 that has not been reviewed or analyzed by a human being ("raw" or "unminimized" data) is stored in separate databases that may be accessed only by specially trained personnel.[53] Unminimized data held by the NSA and CIA generally must be "purged" (deleted) after five years.[54] Data that should not have been collected, but was collected because of a compliance incident, must be purged.[55] Information derived from Section 702 collection cannot be used in a criminal proceeding without the approval of the Attorney General.[56] If a person's communications collected under Section 702 are used against him in a criminal proceeding, he must be notified.[57] All of those rules protect both U.S. persons and non-U.S. persons. The minimization procedures also include special protections for U.S. persons. For example, in many cases NSA must "mask" the identities of U.S. persons when sharing data collected under Section 702 outside the NSA.[58]

"Queries" (or searches) of data collected under Section 702 are restricted in several ways.[59] Some of these rules protect both U.S. persons and non-U.S. persons. For example, personnel who query 702 databases may only access responsive data if they have the required training and authorization.[60] At the NSA and CIA, queries must be designed to return foreign intelligence.[61]

Queries using a "U.S. person identifier" (a term associated with a U.S. person) at the NSA and CIA are subject to additional limitations, such as approval and documentation requirements.[62] The Board recommended the CIA improve its documentation requirement and that both agencies

---

[51] *See id.* at 70.
[52] *See generally id.* at 50-66.
[53] *See id.* at 53.
[54] *See id.* at 60.
[55] *See id.* at 61.
[56] *See id.* at 64. The FISA definition of "Attorney General" includes an Acting Attorney General, the Deputy Attorney General, and, if designated by the Attorney General, the Assistant Attorney General for National Security. *See* 50 U.S.C. 1801(g).
[57] *See* Report at 64.
[58] This means that the name or identifier would be redacted and replaced with a generic term such as "U.S. person."
[59] A "query" refers to a search of data already collected under 702; it does not refer to additional collection. *See* Report at 55.
[60] *See id.* at 55.
[61] *See id.* at 56, 57.
[62] *See id.* at 56-58, 130, 139-40. As noted above, the CIA receives – and is able to query - only a small portion of the data collected under 702.

flesh out their written guidance on complying with these rules.[63] Some of those recommendations have been implemented, and others are in the process of being implemented.[64]

The FBI's query rules differ from the NSA's and CIA's because of its law enforcement mission. At the FBI, during the course of any investigation, an agent or analyst will typically query the FBI's databases to learn what the agency already knows about a particular person. The FBI's queries do not distinguish between U.S. persons and others because nationality is not relevant to most criminal investigations. Such a "federated" search could query all of the FBI's databases, including one that contains some 702 data (but only from PRISM; the FBI does not receive any upstream data).[65] This is true whether or not the investigation concerns a national security-related crime. However, if 702 data were responsive to a query in a non-national-security investigation, the agent or analyst would be informed that there was responsive data but would not receive the query results unless he or she had been specially trained in handling FISA information. The FBI informed the Board that it is "extremely unlikely" that a query conducted in the investigation of a non-national security crime would return 702 data.[66] The Board recommended that the FBI place "some additional limits" on the FBI's use of 702 data in non-national security criminal matters, with Board Members providing separate views on exactly what those limits should be.[67]

In my view, there are important policy reasons to permit the FBI's queries to include the FISA database. An investigator looking into a non-national security crime such as bank fraud might have no reason to expect a connection between his investigation and 702 information. But if such a connection existed – due to a terror financing link, for example – it could be extremely important for the FBI's national security personnel to be alerted to that connection. The FBI's procedures should not limit queries in a way that would prevent it from discovering these connections. Ensuring information sharing of this type has been central to the government's counter-terrorism efforts since the 9/11 Commission highlighted the information sharing barriers that preceded the attacks of September 11, 2001.

Ensuring that the connection between 702 information and a criminal investigation can be *discovered* is distinct from the question how that information can be *used* afterwards. This distinction is reflected in my and Elisebeth Collins' joint separate statement to the Board's 702 report. We recommended that limitations be placed not on querying, but on viewing or using

---

63 *See id.* at 139-40.

64 *See* 2016 implementation report at 17-18; *see also* Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Redacted caption, Hogan, J. (Nov. 6, 2015), at 24-25, available at: https://icontherecord.tumblr.com/tagged/section-702.

65 *See* Report at 58-60.

66 *See id.* at 56, 58-60.

67 *See id.* at 137-39, Annex A, Annex B. Since publication of the Board's report, the FISA Court, in a proceeding in which it solicited the views of a Court-appointed amicus curiae, approved revised FBI minimization procedures permitting FBI personnel to query 702 data in criminal investigations, holding that this provision of the procedures violated neither the statute nor the Fourth Amendment. *See* Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Redacted caption, Hogan, J. (Nov. 6, 2015), available at: https://icontherecord.tumblr.com/tagged/section-702.

any 702 information that was responsive to a query conducted in a non-national security investigation. Specifically, we suggested that supervisory approval be required for an analyst to view the information and that Attorney General approval be required to use the information in a criminal proceeding such as a search warrant or wiretap application, indictment, or prosecution.[68] As law and policy currently stand, using 702 information in a criminal proceeding requires the approval of the Attorney General.[69] The Justice Department has limited the use of 702 information to criminal cases "with national security implications" or concerning "serious crimes."[70] As noted above, if a person's communications collected under Section 702 are used against him in a criminal proceeding, he must be notified. [71] In addition, the FISA Court now requires the FBI to report to the Court any time FBI personnel view 702 information in response to a query in a non-national security investigation.[72]

Upstream collection is subject to even stricter rules than PRISM.[73] For example, the NSA cannot query upstream data using a U.S. person identifier.[74] Only NSA receives unminimized upstream collection; FBI and CIA do not receive it and cannot query it.[75] The retention period for unminimized communications collected upstream is two years, rather than five.[76] MCTs collected upstream are subject to stricter access controls, and some types of MCTs must be segregated in a separate database. If an MCT is determined to contain a wholly domestic communication, it must be destroyed.[77]

Oversight by all three branches of government

The 702 program is subject to extensive oversight by all three branches of government.

Executive branch oversight

Inside the executive branch, the program is overseen by several offices within the NSA, CIA, and FBI, in addition to the Justice Department.[78] Noncompliance with targeting and minimization procedures must be reported to the Justice Department and ODNI.[79] In addition, NSD and ODNI conduct regular reviews of the agencies' compliance with their minimization

---

[68] *See* Report at 138-39 & Annex B (Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook).
[69] *See* Report at 64.
[70] *See* ODNI Signals Intelligence Reform 2015 Anniversary Report, available at: https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-702; *see also* Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Redacted caption, Hogan, J. (Nov. 6, 2015), at 29-30, n. 28 available at: https://icontherecord.tumblr.com/tagged/section-702.
[71] *See* Report at 64.
[72] *See* Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Redacted caption, Hogan, J. (Nov. 6, 2015), at 44, available at: https://icontherecord.tumblr.com/tagged/section-702.
[73] *See* Report at 41.
[74] *See id.* at 56.
[75] *See id.* at 8, 35, 54.
[76] *See id.* at 60.
[77] *See id.* at 54.
[78] *See id.* at 66-68, 75; *see also supra* at 7.
[79] *See* Report at 68-69.

procedures. Some aspects of this review are very granular. For example, the NSD/ODNI team reviews all of NSA's U.S. person queries.[80]

Judicial approval and oversight

The FISA Court does not approve individual targeting decisions under Section 702. Rather, the FISA Court approves the "certifications" of topics about which information may be collected and approves the program's targeting and minimization procedures.[81] The Court must assess whether the procedures meet statutory requirements and comply with the Fourth Amendment.[82] The FISA Court's rules require the government to inform the Court whenever the government realizes that it made an inaccurate or incomplete statement to the Court. The government must also report to the Court noncompliance with the targeting and minimization procedures.[83] Through these mechanisms, the Court engages in ongoing oversight of the program. The Court may – and does – require changes to the procedures when they are initially proposed or in response to a reported misstatement or compliance incident.[84]

Congressional oversight

In addition to oversight by the FISA Court and the executive branch, a great deal of information about the program's operation is provided to Congress.[85] For example, agencies that collect information under Section 702 must report annually to the House and Senate intelligence and judiciary committees, as well as to the FISA Court, Attorney General, and DNI,[86] about the number of times U.S. person identities were disseminated, the number of U.S. person identities subsequently unmasked, and the number of Section 702 targets later determined to be located in the United States.[87] The FISA Amendments Act of 2008 also requires that the Attorney General report semi-annually to the congressional intelligence and judiciary committees on numerous aspects of the 702 program, including incidents of non-compliance with applicable procedures, directives, and guidance.[88] The USA Freedom Act added several 702-related reporting requirements, including the total number of targets and statistics about the use of U.S. person queries.[89]

The program in practice: Compliance

The Board assessed how the program has operated in practice and was "impressed with the rigor of the government's efforts to ensure that it acquires only those communications it is authorized

---

[80] *See id.* at 72.
[81] *See id.* at 26-27.
[82] *See id.* at 27-28.
[83] *See id.* at 29.
[84] *See* Report at 29-31.
[85] *See id.* at 8.
[86] *See* 50 U.S.C. 1881a(l)(3).
[87] *See* Report at 69-70 74, 76-77; *see also* reporting requirements in 50 U.S.C. 1881a(l)(3)(A)(i)-(iii) (discussed in Report at 69).
[88] *See* Report at 74; 50 U.S.C. 1881f.
[89] *See* P.L. 114-23, Title VI, sec. 602

to collect, and that it targets only those persons it is authorized to target."[90] It noted that the program has experienced a very low rate of compliance incidents[91] and stated that it had seen no evidence of "bad faith or misconduct."[92] When observing the program in operation, I was personally impressed with how seriously agency personnel treat the program's rules.

This is not to downplay the compliance incidents that have occurred. The most significant to date was the government's acquisition of MCTs in upstream collection, which the Court did not understand when it first approved the minimization procedures. After the government brought this issue to the Court's attention in 2011, the Court held that, although collection of MCTs was permissible (and unavoidable), the then-current minimization procedures did not satisfy the statute or the Fourth Amendment because they did not provide adequate protections to ameliorate the impacts of MCT collection.[93] The FISA Court eventually approved a new set of minimization procedures with stricter rules for upstream collection and MCTs in particular. The government purged upstream data that had been collected prior to implementation of the new procedures.[94] Although a serious compliance incident, in my view this episode demonstrates the FISA Court's effectiveness in overseeing the program: the government took seriously its obligation to self-report, and the Court did not hesitate to demand that the program be significantly altered.

Effectiveness

The 702 program is highly valuable as a source of foreign intelligence. There is no question that the program has supplied important foreign intelligence, supporting the government's efforts to combat terrorism and other efforts to protect the national security.[95] The Board reviewed information about how Section 702 is used, including specific examples. It found that information acquired through the program had provided great value under a variety of measures, including playing a "key role in discovering and disrupting specific terrorist plots," allowing the government to identify previously unknown individuals involved in international terrorism, and providing information about terrorists' operations, priorities, strategies, and tactics.[96] At the time the Board's 702 report was published, information acquired through the program was present in "over a quarter of the NSA's reports concerning international terrorism."[97]

---

[90] Report at 103; *see also id.* at 116-17 (noting that the Board was impressed with the "seriousness" with which the agencies attempt to avoid mistakes in targeting).

[91] *See* Report at 77-78 (noting that DOJ and ODNI reviews revealed an incident rate of less than one percent, of which more than half involved instances where the government otherwise complied with the procedures but was late in making a report to NSD and ODNI). The Board also noted that that compliance incidents that have occurred have mainly involved "technical issues resulting from the complexity of the program." *Id.* at 8.

[92] Report at 8; *see also id.* at 11.

[93] *See* Report at 124-26.

[94] *See id.* at 126.

[95] PCLOB's statutory mandate is limited to overseeing the government's actions to combat terrorism. *See* 42 U.S.C. 2000ee(c). Section 702's uses are not limited to counter-terrorism. During the Board's review of the program, the agencies provided the Board with information about Section 702's value not only to counter-terrorism efforts to but to other national security purposes as well.

[96] Report at 10, 104, 107-10.

[97] *See id.* at 10.

Legality

The Board analyzed the legality of the program and unanimously concluded that the program is statutorily authorized.[98] The Board noted that the text of the statute itself "provides the public with transparency into the legal framework for collection and publicly outlines the basic structure of the program."[99]

The Board also addressed whether the 702 program is consistent with the Fourth Amendment. As noted above, the FISA Court does not approve individual targets. Instead, it approves the minimization and targeting procedures and the certifications of foreign intelligence topics on which information can be collected. [100] Although the targets of collection – non-U.S. persons located outside the United States – do not have Fourth Amendment rights, the Fourth Amendment is implicated by the incidental collection of U.S. person communications.[101]

The Board noted that several federal appeals courts have recognized a foreign intelligence exception to the Fourth Amendment's warrant requirement.[102] Several courts have specifically found that exception to apply to the 702 program.[103] Even where a warrant is not required, however, the Fourth Amendment requires searches to be "reasonable." The courts have held that reasonableness is judged on the totality of the circumstances, balancing the intrusion on privacy interests with the strength of the government's interest.[104] Applying this test, the Board found that the "core of this program – acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight…"[105] is reasonable.

The Board went on to opine that certain aspects of the program outside its core came close to the line of reasonableness and that its recommendations would push the program "more comfortably"[106] inside constitutional bounds. The Board did not opine that any of its recommended changes to the program were statutorily or constitutionally required, but presented them as "policy proposals."[107]

PCLOB's recommendations and the Administration's implementation of the recommendations

---

98 *See id*. at 80-86.
99 *Id.* at 82.
100 *See id.* at 26-27.
101 *See id.* at 86-87.
102 *See id.* at 89-90.
103 *See, e.g.*, U.S. v. Hasbajrami, Mem. Op., 2016 WL 1029500 (E.D. NY, Mar. 8, 2016); Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Redacted caption, Hogan, J. (Nov. 6, 2015), available at: https://icontherecord.tumblr.com/tagged/section-702; U.S. v. Mohamud, Criminal No. 3:10–CR–00475–KI–1 (U.S.D.C., D. Or., June 24, 2014), 2014 WL 2866749.
104 *See* Report at 86-97.
105 *Id.* at 88.
106 *Id.*
107 *Id.* at 88, 97.

The Board made several specific recommendations to alter the rules governing the 702 program.[108] None would require an amendment to the statute; all could be implemented by the agencies or the FISA Court under their existing authority.[109] Each of the recommendations has been implemented in whole or part. [110]

In addition to the recommendations already described, I would like to highlight the Board's recommendation for more transparency about the program's impact on U.S. persons. The government has often been asked to inform Congress and the public about how many U.S. persons are affected by Section 702 or how many U.S. person communications have been collected. It is difficult to assess exactly how much the 702 program affects Americans' privacy rights without that information.

The agencies have stated that they cannot produce an accurate number – or even a reliable estimate – of these numbers. They do not know the nationality of every person with whom a target communicates and do not have the resources to investigate that fact for every communication collected. They point out that it may be a greater privacy intrusion to conduct an investigation into every person whose communications are incidentally collected, when many of those communications otherwise would never be reviewed before being deleted from the database at the end of the retention period.[111]

Nevertheless, the Board recognized the importance of providing as much transparency as possible about the 702 program's impact on U.S. persons. The Board identified five categories of information that it believed *could* be calculated. The Board recommended that the NSA annually measure these factors and report them to Congress and (to the extent consistent with national security) to the public.[112] On April 30, the DNI published a "Statistical Transparency Report" that included statistics on two of the Board's recommended measures: the number of U.S. person queries conducted and the number of disseminated intelligence reports that contained U.S. person information. As to the Board's other recommended measures, the NSA has told the Board that it has encountered technical difficulty in making the calculations, but that it is committed to providing further information and will continue to work with the Board on this subject.[113]

---

[108] *See id.* at 11-13 (especially Recommendations 1-3, 5).
[109] *See id.* at 149.
[110] *See* 2015 and 2016 Board implementation reports, available at: https://www.pclob.gov/library.html.
[111] *See* Report at 146-47.
[112] *See id.* The Board's 2016 implementation status report noted that this recommendation is "being implemented." 2016 implementation report at 23.
[113] 2016 implementation report at 25-26.

Senate Committee on the Judiciary

"Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties"

May 10, 2016

Questions for the Record from Chairman Charles E. Grassley

Kenneth Wainstein, Matthew Olsen, and Rachel Brand

1. Section 702 Sunset Provision

As you know, the FISA Amendments Act Reauthorization Act of 2012 reauthorized Title VII, or Section 702, of the FISA Amendments Act until December 31, 2017. As you also know, the Privacy and Civil Liberties Oversight Board ("PCLOB") conducted an extensive review of Section 702 surveillance and its oversight and compliance processes. The PCLOB concluded that the program was authorized by the FISA statute, was constitutional under the Fourth Amendment, and that the information collected under this authority "has been valuable and effective in protecting the nation's security and producing useful foreign intelligence." Following its extensive review, the PCLOB further explained that "the Board has found no evidence of intentional abuse" of the program. And the Section 702 program is subject to a substantial compliance and oversight regime from all three branches of the government, including the U.S. Intelligence Community and Department of justice, as well as Foreign Intelligence Surveillance Court and the congressional intelligence and judiciary committees.

a. Given all of the above, do you believe Title VII of the FISA Amendments Act should be made permanent?

ANSWER: *Yes. I support permanent reauthorization of Section 702 of FISA without amendment. Congress has often enacted a sunset for a new authority and, after the passage of time, permanently reauthorized the authority when Congress determined that it was valuable and incorporated appropriate protections. Congress should follow that model here. Section 702 was enacted eight years ago. Congress has already reauthorized it once without amendment. Experience with the program operated under Section 702 – as explained by the PCLOB Report – shows that it is legal, operates within strict constraints that protect privacy and civil liberties, and is an extremely valuable source of foreign intelligence. Congress should now permanently reauthorize Section 702. Eliminating the sunset would not prevent Congress from amending Section 702 if it became necessary in the future, but no such need has become evident in the first eight years of the 702 program's operation.*

Ken Wainstein, Matthew Olsen, and Rachel Brand

2. U.S. Person Queries and U.S. Persons' Personal Life

In his Prepared Statement, Chairman Medine asserted that U.S. persons' communications incidentally acquired pursuant to Section 702 "can include family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges. U.S. person queries [of that information] are, therefore, capable of revealing a significant slice of an American's personal life."

a. U.S. persons cannot be targeted, or "reverse targeted," for Section 702 collection, correct?

ANSWER: *Correct. Reverse targeting is expressly prohibited by the statute.*

b. Is it accurate to state that the way the government may incidentally acquire U.S. person communications through Section 702 collection is when U.S. persons communicate with a non-U.S. person abroad who has been targeted pursuant to targeting requirements? And those targeting requirements ensure that the non-U.S. person abroad was targeted for a court-authorized foreign intelligence purpose, correct?

ANSWER: *The only persons who may be targeted under Section 702 are non-U.S. persons located outside the United States who are expected to communicate foreign intelligence information concerning a list of topics certified by the FISA Court. These statutory limitations are enforced through strict targeting procedures that must be approved by the FISA Court. This does not mean that no U.S. person's communications will ever be collected; if, for example, a U.S. person communicates with a targeted non-U.S. person located abroad, then those communications will be "incidentally" collected. In the context of "upstream" collection, which accounts for about 9% of Internet collection under Section 702, there are certain circumstances in which a U.S. person communication could be collected where the U.S. person was not necessarily communicating with a target. This occurs because of the technical method for collecting communications from the Internet backbone (by scanning Internet transactions for the "selectors" (such as e-mail addresses) used by targets). If, for example, a target's e-mail address appeared in the body of an email between two non-targets, that email would be collected.*

c. Further, U.S. person communications that are acquired through Section 702 only include those obtained *while* communicating with a valid foreign intelligence target, correct? In other words, just because a U.S. person has communicated with a valid foreign intelligence target on one occasion doesn't mean the U.S. government thereafter has access to any and all of that U.S. person's communications, correct?

ANSWER: *Correct. If a targeted non-U.S. person located abroad communicates with a U.S. person, that communication will be collected. This does not open up all of that U.S. person's communications to collection under Section 702. Section*

702 does not allow the government to use the fact of a U.S. person's communication with a target as a reason to target the U.S. person, nor does it allow "reverse targeting" (targeting a non-U.S. person in order to collect communications with a U.S. person). Under Section 702, the government may only target the communications of specific non-U.S. persons located outside the United States.

d. **To Rachel Brand:** During the PCLOB's review of the Section 702 program, did you ever encounter an instance in which *U.S. person queries* of collected 702 data revealed a "significant slice" of a specific American's personal life?

ANSWER:

No. It is extremely unlikely that a U.S. person query of 702 data could reveal a significant slice of a U.S. person's life. First, it is important to remember that queries are conducted of information that has already been collected under Section 702. Queries do not collect any new data. Second, a U.S. person can never be a target of collection under Section 702. The only U.S. person communications that could respond to a U.S. person query under 702 are those that were incidentally collected because, for example, a U.S. person sent a communication to a targeted non-U.S. person outside the United States. As noted above, the fact that a particular communication to or from a U.S. person was incidentally collected does not mean that all – or even a "significant slice" – of that U.S. person's communications were collected.

The likelihood of a U.S. person query of 702 data revealing a significant slice of a U.S. person's life is especially remote in the context of queries by the FBI. Chairman Medine's written testimony suggested that a U.S. person query at the FBI could "search through years of a U.S. person's communications," leaving the impression that the 702-collected communications held by the FBI could contain the entirety of a particular U.S. person's communications over a period of years. However, as noted above, the FBI can only query the communications it possesses. And the FBI receives only a small subset of the data collected by the NSA under PRISM and receives no information collected upstream. It is almost impossible to imagine that years' worth of any U.S. person's communications would be both incidentally collected and contained within the small subset of 702 PRISM data that is provided to the FBI.

Ken Wainstein, Matthew Olsen, and Rachel Brand

3. Deletion of U.S. Persons' Irrelevant Communications

Also in his Prepared Statement, Chairman Medine explained that "NSA's minimization procedures further require the destruction of irrelevant U.S. person communications . . . only where the communication can be identified as 'clearly' not relevant to the purpose under which it was acquired or containing evidence of a crime," yet he asserted that "[i]n practice, this destruction rarely happens." He also separately asserted in his Prepared Statement that "[i]n theory . . . innocent communications will be deleted by the intelligence agencies. But in practice, as the Board's Section 702 report notes, they rarely are deleted." Finally, in response to a question during the hearing, he stated that some U.S. person information "is never deleted. It sits in the databases for five years or sometimes longer."

a. As the PCLOB's Section 702 report explains, isn't the reason why NSA doesn't immediately delete many U.S. person communications because most U.S. person communications are never analyzed or reviewed by NSA analysts?

ANSWER: *Yes. Communications collected under Section 702 are subject to a five-year retention period. With narrow exceptions, they "age off" NSA's systems – that is, they are automatically deleted – at the end of the retention period unless they are reviewed. This is true for all communications, including U.S. person communications collected incidentally. As the PCLOB's Report explained: "NSA analysts do not review all or even most communications acquired under Section 702 as they arrive at the agency. Instead, those communications often remain in the agency's databases unreviewed until they are retrieved in response to a database query, or until they are deleted upon expiration of their retention period, without ever having been reviewed." (PCLOB Report at 128-29.)*

The program's minimization procedures require that, if a communication is reviewed by an analyst – because it is responsive to a query, for example – and is determined to be a U.S. person communication, it must be deleted if the reviewing analyst determines that it does not contain either foreign intelligence information or evidence of a crime. Chairman Medine and others have pointed out that communications are rarely deleted in response to this requirement. This is not because NSA analysts fail to comply with the rule, but because it is very difficult for an individual analyst to review an individual communication and determine that it is not foreign intelligence. This is because, as the PCLOB Report on Section 702 explained, "communications that appear innocuous at first may later take on deeper significance as more contextual information is learned, and it can be difficult for one analyst to be certain that a communication has no intelligence value to any other analyst." (PCLOB Report at 129.) If an analyst reviews a

communication and does not know whether it constitutes foreign intelligence or evidence of a crime, he or she may leave it in the database for the remainder of the retention period. These communications will still be subject to the retention period and related limitations.

b. And isn't it correct that all U.S. person communications not reviewed or analyzed by the NSA will be aged-off and deleted within defined periods?

ANSWER: *Yes.*

c. **To Rachel Brand:** During the PCLOB's review of the Section 702 program, did you ever encounter a situation in which the NSA did *not* delete an identified U.S. person communication it had (1) reviewed and (2) determined was "innocent" – i.e., "'clearly' not relevant to the purpose under which it was acquired or containing evidence of a crime"?

ANSWER: *No.*