Testimony of Elisebeth B. Collins

Member, Privacy and Civil Liberties Oversight Board

U.S. Senate Committee on the Judiciary

June 27, 2017

Chairman Grassley, Ranking Member Feinstein, and Members of the Committee, thank you for the opportunity to submit testimony regarding the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act.

As an independent, bipartisan agency, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) has two fundamental statutory responsibilities: first, providing advice relating to executive branch actions or efforts to protect the nation from terrorism; and second, providing oversight to such executive branch counterterrorism actions or efforts, a role that entails close attention to implementation of both law and policy.[1]

In our oversight role, the bipartisan five-member Board undertook an extensive study of activities conducted pursuant to Section 702 of the Foreign Intelligence Surveillance Act (the Section 702 Program or Program) and issued a unanimous report in July 2014.[2] The Board unanimously concluded that the Section 702 Program is valuable, statutorily authorized, and, at its core, constitutional. We set forth the legislative foundation for the Program, the implementing procedures governing the operation of the Program, and the extensive oversight structure that accompanies the Program. We also unanimously voted out 10 recommendations, each of which has been implemented or is in the process of being implemented, and none of which required legislation.

I provide this testimony in my individual official capacity, but note that it is consistent with the analysis and conclusions of the Section 702 Report. I have included below a brief description of the Section 702 Program, based on our year-long examination from 2013-2014; our conclusions as to the value of the Section 702 Program; and an explanation of our relevant recommendations and points of emphasis. The testimony below draws heavily from the Board's Report, which continues to be a valuable resource for understanding and assessing the Program.

The Section 702 Program

Section 702 has its roots in the President's Surveillance Program developed in the immediate aftermath of the September 11, 2001 attacks. Under one aspect of that program, which came to be known as the Terrorist Surveillance Program (TSP), the President authorized interception of the contents of international communications from within the United States, outside the already established Foreign Intelligence Surveillance Act (FISA) process. Following disclosures about the TSP by the press in December 2005, the government sought and obtained authorization from the Foreign Intelligence Surveillance Court (FISC) to conduct, under FISA, the collection that had been occurring under the TSP. Later, the government developed a statutory framework specifically designed to authorize this collection program. After the enactment and expiration of a temporary measure, the Protect America Act of 2007, Congress passed the FISA Amendments Act of 2008, which included the new Section 702 of FISA.

[1] 42 U.S.C. § 2000ee(c), (d)(1), (d)(2).
[2] "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).

Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize surveillance targeting of persons who are not U.S. persons and who are reasonably believed to be located outside the United States, with the compelled assistance of electronic communication service providers, in order to acquire foreign intelligence information. U.S. persons may *not* be targeted, and the purpose of collection must be foreign intelligence. The FISC must approve executive branch authorizations to acquire designated foreign intelligence by non-U.S. persons under Section 702, along with procedures governing targeting decisions and the handling of information acquired. The role of the FISC, an independent Article III court, is an essential feature of the oversight structure accompanying the program.

Although U.S. persons may not be targeted under Section 702, U.S. person communications may be acquired in a variety of ways. The primary example is when a U.S. person communicates with a non-U.S. person who has been targeted, resulting in what is known as "incidental" collection. Subject to numerous rules, the government may retain and ultimately use incidentally collected U.S. person communications.

Under Section 702, the Attorney General and Director of National Intelligence make annual certifications authorizing this targeting to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted. There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the "traditional" FISA process under Title I and Title III of the statute. Instead, Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information. The certifications that have been authorized include information concerning international terrorism and other foreign intelligence topics.

Although probable cause is not required for specific targets, the government must develop targeting and minimization procedures that satisfy certain criteria. As part of the FISC's review and approval of the government's annual certifications, the court must approve these procedures and determine that they meet the necessary standards. The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program. Each agency that receives information acquired through the Section 702 program has its own minimization procedures, approved separately by the FISC, and these procedures are now almost entirely available to the public.

Once acquisition has been authorized, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government provides certain "selectors," such as telephone numbers or email addresses, that are associated with surveillance targets and sends those selectors to the providers to begin acquisition.

There are two types of Section 702 acquisition: "PRISM" collection and "upstream" collection. The National Security Agency (NSA) receives all data acquired through both means, and the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) each receive only a select portion of PRISM (and no "upstream") collection. PRISM collection does not include the acquisition of phone calls. Although "upstream" collection occurs with the compelled assistance of providers that control the telecommunications "backbone" over which telephone and Internet communications transit, the collection is still targeted.

<u>PCLOB's Section 702 Analysis</u>

The Board engaged in a close and rigorous examination of the Section 702 program, with particular attention to the adequacy of privacy and civil liberties protections, in accordance with the Board's authorizing statute. PCLOB is a general oversight body for the executive branch's counterterrorism activities; we are not a compliance body for any specific element of the Intelligence Community. PCLOB conducts "external" oversight – as opposed to Intelligence Community agencies' internal compliance offices, legal offices, and inspectors general. We operate independently both of Administration policy and of every element of the Intelligence Community.

From that independent perspective, the Board conducted both a legal and policy analysis of the Section 702 program. We unanimously concluded that the program is statutorily authorized and constitutional, although certain features of the program push it close to the limits of Fourth Amendment reasonableness. Specifically, we raised and addressed concerns about incidental U.S person collection, so-called "abouts" collection, and the use of U.S. person identifiers as query terms.

In terms of operation, the Board unanimously concluded that the program has a limited scope—in other words, it does not authorize or result in "bulk" collection. Instead, it authorizes the government only to engage in *targeted* collection of telephone and internet communications of *non*-U.S. persons *located abroad* who are likely to communicate information about court-approved *foreign intelligence* topics. Despite the Section 702 Program's explicit limits and the extensive description of the program in our Report, misconceptions remain about the program. To be clear, Section 702 does not permit: (1) "bulk" collection; (2) non-targeted collection; (3) non-FISC approved collection; or (4) U.S. person targeting.

The Board also focused intensively on the judicially-approved targeting and minimization procedures governing the operation of the program, noting the special protections afforded to U.S. persons, and making recommendations designed to tighten certain aspects of the procedures.

Finally, we considered the extensive and layered oversight that accompanies the Section 702 program. Oversight occurs in all three branches of government and can only be described as rigorous. Congress conducts oversight on a routine basis and through periodic consideration of reauthorization; the FISC must consider and approve key aspects of the program's design and operation; and the executive branch features layered inter- and intra-agency oversight.

Each agency's adherence to its targeting and minimization procedures is subject to extensive oversight within the executive branch, including internal oversight within individual agencies as well as regular reviews conducted by the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI). This oversight framework is critical to the Board's overall conclusions of lawfulness and reasonableness. When managing a large program like the Section 702 program, no analyst, machine, process, or methodology is fool-proof. Although we identified no instances of deliberate abuse, there is always the possibility of human error or technological error, as with any complex program. A robust oversight structure with built-in, systematic redundancies can detect and remedy those errors and prevent their recurrence.

Value of Section 702

The Board spent significant time understanding the value of Section 702, particularly in comparison to more traditional FISA authority. Section 702 allows the government to acquire a greater range of foreign intelligence than it otherwise would be able to obtain, and it provides a degree of flexibility not offered by comparable surveillance authorities. Because the oversight mandate of the Board extends only to those measures taken to protect the nation from terrorism, the Board's focus in the report was limited to the counterterrorism value of the Section 702 program, although we were made aware of the value of the program for additional foreign intelligence purposes.

Section 702 enables the government to acquire the contents of international telephone and Internet communications in pursuit of foreign intelligence. While this ability is to some degree provided by other legal authorities, particularly "traditional" FISA, Section 702 offers advantages over these other authorities.

In order to conduct electronic surveillance under "traditional" FISA (i.e., Title I and Title III), the government must persuade the FISC, under a standard of probable cause, that an individual it seeks to target for surveillance is an agent of a foreign power, and that the telephone number or other communications facility it seeks to monitor is used, or is about to be used, by a foreign power or one of its agents. In addition, a high-level executive branch official must certify (with a supporting statement of facts) that a significant purpose of the surveillance is to obtain foreign intelligence and that the information sought cannot reasonably be obtained through normal investigative techniques. To meet these requirements and satisfy the probable cause standard, the Intelligence Community must gather facts, DOJ must draft a detailed FISC application, the accuracy of the facts in the application must be confirmed, the senior government official's certification must be prepared, the Attorney General must approve the application, and the application must be submitted to the FISC, which must review it, determine if the pertinent standards are met, and, if so, grant the request. These steps consume significant time and resources. In practice, FISA applications are lengthy and the process frequently takes weeks from beginning to final approval. This system is deliberately rigorous because it was designed to provide a check on the government's surveillance of U.S. persons and other people located in the United States.

Section 702 imposes significantly fewer limits on the government because it allows targeting only of non–U.S. persons located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted. Rather than approving or denying individual targeting requests, the FISC authorizes the surveillance program as a whole, approving the certification in which the government identifies the types of foreign intelligence information sought and the procedures the government uses to target people and handle the information it obtains. Targets of surveillance need not be agents of foreign powers; instead, the government may target any non-U.S. person overseas whom it reasonably believes has or is likely to communicate designated types of foreign intelligence. The government need not have probable cause for this belief, or for its belief that the target uses the particular selector, such as a telephone number or email address, to be monitored. There is no requirement that the information sought cannot be acquired through normal investigative techniques.

These differences allow the government to target a much wider range of foreign individuals who possess relevant foreign intelligence than was possible under "traditional" FISA. For instance, people who might have knowledge about a suspected terrorist can be targeted even if those people are not themselves involved in terrorism or any illegitimate activity.

In addition to expanding the pool of potential surveillance targets, the Section 702 program also enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISC for each targeting decision. As a result of these two factors, the number of people who can feasibly be targeted is significantly greater under the Section 702 program than under the traditional FISA process.

The streamlined framework in which the program operates has proven valuable in a number of ways in the government's efforts to combat terrorism. It has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

While many of these success stories are classified and cannot be discussed here today, there are some statistics and examples that the Board mentioned in its report that can be shared. One such statistic is that roughly one quarter of the NSA reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. These reports are used by the recipient agencies and departments for a variety of purposes, including to inform senior leaders in government and for operational planning. And, one example of the tangible value of the Section 702 Program involves the surveillance of an email address by an extremist based in Yemen. Through that surveillance, the agency discovered a connection between that extremist and an unknown person in Kansas City, Missouri.

The NSA passed this information to the FBI, which identified the unknown person, Khalid Ouazzani, and subsequently discovered that he had connections to U.S. based Al Qaeda associates, who had previously been part of an abandoned early stage plot to bomb the New York Stock Exchange. All of these individuals eventually pled guilty to providing and attempting to provide material support to Al Qaeda.

PCLOB has received information about other instances in which the Section 702 program has played a role in counterterrorism efforts. In approximately 20 cases that we reviewed, surveillance conducted under the Section 702 program was used in support of an already existing counterterrorism investigation, while in approximately 30 cases, program information was the initial catalyst that identified previously unknown terrorist operatives and/or plots. A rough count of these cases identifies well over 100 arrests on terrorism-related offenses. In other cases that did not lead to disruption of a plot or apprehension of conspirators, the Section 702 program appears to have been used to provide warnings about a continuing threat or to assist in investigations that remain ongoing.

PCLOB Recommendations

In light of our legal and policy analysis, and bearing in mind the value of the Section 702 program, the Board made 10 recommendations, several of which addressed issues that continue to be the subject of debate today.

- U.S. Person Information

The Board conducted a constitutional and policy analysis of the potential for collection of U.S. person information and queries with U.S. person identifiers. These issues raise considerable privacy implications, which we grappled with in our Report and recommendations.

Under the Section 702 framework, the government may not target a U.S. person for surveillance. The Section 702 program also includes a prohibition on "reverse targeting," which means that an intelligence agency may not target a non-U.S. person outside the United States if the government's real purpose is, in fact, to collect information about a person who is in the United States or who is a U.S. person – which might occur if a U.S. person is found to be in touch with the non-U.S. person target located abroad. We are aware of two incidents of reverse targeting, both of which were identified and corrected.

However, as noted above, communications of a U.S. person may be incidentally collected in some instances. For example, a U.S. person communication may be collected if the U.S. person is in communication with a non-U.S. person target. This incidental collection does not mean that the U.S. person was targeted under the Section 702 Program, but it does raise significant privacy concerns.

If incidentally collected, the applicable judicially-approved "minimization" rules govern the retention and dissemination of the information, including when a U.S. person's identity would be included in disseminated intelligence reports (only if the identity would be needed in order to understand the import of the foreign target's communications or if the U.S. person's identity is relevant to evidence of a crime).

In addition, an analyst with the required training and authorization may *query* databases containing unminimized Section 702-acquired information using approved U.S. person identifiers. Such queries of data lawfully acquired pursuant to Section 702 do not involve any new collection, and subsequent dissemination or use of such information is subject to specific additional procedures and safeguards.

When assessing the very real privacy implications of incidental collection and U.S. person queries, we took very seriously the findings of previous commissions, including the 9/11 Commission[3] and the Ft. Hood inquiry,[4] that the government cannot afford to have walls between its national security and criminal investigations, or gaps in the ability of agents and analysts to access lawfully collected information. Moreover, queries using U.S. person identifiers may be the least intrusive means to determine whether a U.S. person has a previously unknown connection to a target, or is perhaps a potential victim.

Fundamentally, we recommended greater clarity and tighter documentation in the applicable minimization and implementing procedures for conducting U.S. person queries, given the very real privacy concerns that this practice implicates. As discussed below, we also recommended that the NSA develop metrics for assessing the amount of incidental collection that occurs.

- "About" Collection

In its review, the Board noted that some forms of "about" collection present novel and difficult issues regarding the balance between privacy and national security. An "about" communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Based on our review, the Board determined that because of the way that the NSA conducted upstream collection, and the limits of its then-current technology, it could not eliminate "about" collection without also eliminating a significant portion of the "to/from" communications that it was seeking. At the same time, the Board identified "abouts" as a driver of incidental U.S. person collection. The Board recommended that the NSA work to develop technology that would enable it to identify and distinguish among the types of "about" collection and if this was not technologically feasible then the NSA should try to segregate all "about" communications after collection.

[3] National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. Washington, D.C. 2004. *Available at* https://www.9-11commission.gov/report/911Report.pdf.
[4] A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack, United States Senate Committee on Homeland Security and Governmental Affairs, February 3, 2011, https://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHoodReport.pdf.

The Board also believed that once these technological mechanisms were in place then it was an appropriate time to have a policy discussion about whether or not the privacy impacts of particular types of "about" collection justify treating those types of communications differently.

Recently, the NSA disclosed a significant compliance incident related to "abouts" collection and has halted that type of collection. In my personal view, ceasing "abouts" collection unless and until the NSA can ensure compliance with applicable minimization procedures was both necessary and appropriate.

- Accountability and Transparency

Throughout its report, the Board stressed the importance of providing accountability and transparency to the public with Section 702 data, consistent with national security. While it respects the government's need to protect its operational methods and practices, the Board also recognizes that transparency enables accountability to the public that the government serves.

One key recommendation to improve accountability and transparency with Section 702 was to provide a better understanding of the procedures that govern the acquisition, use, retention, and dissemination of information collected. The Board strongly advised that the government declassify and make available to the public – without jeopardizing national security – versions of the FBI, CIA, and NSA minimization procedures. This was one method by which the Board felt the government could demonstrate the lengths at which it goes to protect the rights of Americans while gathering valuable foreign intelligence information, and that recommendation has been implemented.

The Board also recommended that the government implement measures to provide insight about the extent to which the NSA acquires and utilizes U.S. person communication under the Section 702 program. Although the government has stated that it is very difficult to determine an exact count of U.S. person queries under Section 702, the Board's recommendation as to quantifying incidental U.S. person information stands.

The Intelligence Community has implemented all 10 recommendations in whole or in part; additional information as to implementation is publicly available reports the Board issued in 2015 and 2016.

Section 702 and Reauthorization

The Board's report and recommendations are consistent with what has been called a "clean" reauthorization of Section 702. We made serious recommendations, each of which we thought necessary to address privacy and civil liberties protections, but none of which required legislation. Each of these recommendations has been (or is being) implemented. I am aware of no information that has surfaced since the Board's 2014 Report that suggests that the Board's key findings would not be as valid today as they were when we issued them in 2014.

I personally view the Section 702 program as an extraordinarily valuable tool in the fight against terrorism and believe the current framework for the Program provides the necessary protections to ensure that our American values are not compromised.

Congress designed the statutory framework to ensure that multiple layers of oversight governed activities conducted pursuant to Section 702 and the judiciary maintains an important role in ensuring the Program's compliance with the framework.

I appreciate the opportunity to provide this testimony.