PREPARED STATEMENT

For the

SENATE COMMITTEE ON THE JUDICIARY

on

OVERSIGHT AND REAUTHORIZATION OF THE FISA AMENDMENTS ACT: THE BALANCE BETWEEN NATIONAL SECURITY, PRIVACY AND CIVIL LIBERTIES

David Medine

Chairman, Privacy and Civil Liberties Oversight Board

May 10, 2016

Chairman Grassley, Ranking Member Leahy, members of the Committee, thank you for the opportunity to testify today.[1] Since May 2013, I have served as Chairman of the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board").

The focus of this hearing, the Section 702 surveillance program, collects the contents of communications by non-U.S. persons ("non-USPs") outside of the U.S. and has proven to be a valuable intelligence tool for the U.S. government. However, the program also raises significant privacy and civil liberties issues through its incidental collection of the contents of U.S. persons' communications. It has been nearly two years since the Privacy and Civil Liberties Oversight Board issued its report on the Section 702 program. The Board's report made a number of non-legislative recommendations, many of which have been implemented. The Judiciary Committee's consideration of reauthorization of Section 702, which is set to expire at the end of 2017, provides an opportunity to consider legislative changes to strengthen this important program. I urge the Committee to adopt three legislative reforms: (1) require judicial approval when searching for United States persons'[2] communications; (2) mandate stricter controls over Upstream "about" collections; and (3) insist that diligent efforts be made to quantify the government's USP collections under Section 702.

My testimony today will first provide some background about the Section 702 program, which is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. This will be followed by a discussion of the PCLOB's recommendations and the status of their acceptance and implementation. Finally, I propose the adoption of three legislative reforms building upon recommendations I made in the PCLOB's Section 702 report.

I. Background on the Section 702 Program

Before speaking to the future of the Section 702 program, I would like to briefly discuss its past. The Section 702 program has its roots in the Terrorist Surveillance Program in which the President, in the wake of the September 11th terrorist attacks, authorized the interception of the contents of international communications from within the United States. Congress provided a statutory framework for the activity, first in the Protect America Act of 2007, and later in the FISA Amendments Act of 2008 ("FAA"). But these changes were not permanent. Section 702, added by the FAA, was originally written to sunset on December 31, 2012. This expiration was extended when Congress subsequently passed the FISA Amendments Act Reauthorization Act of 2012, which established the current sunset date of December 31, 2017.

[1] The views expressed in this written testimony and the oral testimony provided on May 10, 2016, represent my views and do not necessarily reflect the views of the Privacy and Civil Liberties Oversight Board or any of its other members.

[2] Under FISA and the FISA Amendments Act, the term "United States person" includes U.S. citizens, legal permanent residents, unincorporated associations with a substantial number of U.S. citizens or legal permanent residents as members, and corporations incorporated in the United States. It does not include associations or corporations that qualify as a "foreign power." *See* 50 U.S.C. § 1801(i). For convenience, this testimony will refer to USPs and "Americans" interchangeably.

Section 702 permits the Attorney General ("AG") and the Director of National Intelligence ("DNI") to jointly authorize surveillance targeting non-U.S. persons who are reasonably believed to be located outside the United States. Collection of information about a target is conducted with the compelled assistance of electronic communication service providers, and is limited to foreign intelligence information. Although the FISA Court does not approve targeting decisions under the Section 702 program, the AG and DNI must provide certifications to the court on an annual basis. The 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 topics, such as the acquisition of weapons of mass destruction. Additionally, the FISA Court must approve targeting and minimization procedures that govern the program.

Taking a closer look at how surveillance is conducted under Section 702, the program can be divided into seven distinct stages: Certification, Targeting, Tasking, Minimization, Analysis, Dissemination, and Retention/Destruction. I will briefly discuss each of these stages. Before proceeding, I would like to emphasize that this is a tremendously complex program, and it would take hours to explain every detail. For additional information, I refer the Committee to the PCLOB's unclassified Section 702 report, which is nearly 200 pages long. However, even this report does not touch on the many details of the program that remain classified.

Certification: Once a year, the AG and DNI must certify to the FISA Court a list of foreign intelligence topics for which they intend to collect information under Section 702. The certification must state that "a significant purpose of the acquisition is to obtain foreign intelligence information," and include detailed procedures that ensure U.S. persons are not targeted. The FISA Court is responsible for reviewing and approving the list of topics and can request changes to the certifications. Surveillance under the terrorism certification was the subject of the Board's Section 702 inquiry.

Targeting: According to DNI's latest Transparency Report,[3] there were 94,368 targets in the Section 702 program in 2015. The FISA Court did not approve these individual targets. Instead, an NSA analyst can identify non-U.S. persons outside of the United States as potential surveillance targets. In addition to identifying a valid foreign intelligence purpose derived from the list certified by the FISA Court, an analyst must follow a detailed set of targeting procedures. These procedures require a careful examination of the target and the email address, phone number, or other selector associated with the target, to verify that they are sufficiently foreign. Once an analyst has documented a valid foreign intelligence purpose and the steps taken to ensure the target is foreign, she must obtain the approval of two senior NSA analysts. If approval is obtained, an electronic communications service provider can be compelled to gather communications about the target through tasking.

The Department of Justice ("DOJ") conducts a post-tasking review of every tasking sheet provided by the NSA and the Office of the Director of National Intelligence ("ODNI") staff reviews a sample of these sheets. In addition to evaluating whether the tasking complied with the

[3] https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

targeting procedures, DOJ and ODNI staff reviews the targeting for overall compliance with the statutory limitations, such as the prohibition against reverse targeting.[4] The DOJ and ODNI also conduct approximately monthly reviews of the FBI's application of its own targeting procedures. Subsequently, the results of the NSA and FBI reviews are provided to Congressional Committees.

Tasking: After a selector is tasked, the NSA receives information from service providers in one of two ways: PRISM and Upstream collection.

In PRISM collection, the government sends a selector, such as an email address, to a U.S.-based electronic communications service provider, and the provider is compelled to give the communications sent to or from that selector to the government. The NSA receives all data collected through PRISM, while the CIA and FBI each receive a select portion of PRISM collection.

Upstream collection, which accounts for approximately 10 percent of all information collection under Section 702, differs from PRISM in several significant ways. First, the acquisition occurs with the compelled assistance of providers that control the telecommunications "backbone" over which some telephone and Internet communications transit and can be collected. Additionally, information from Upstream collection is only received by the NSA, and contains "about" communications and "multiple communications transactions," known as MCTs.[5]

An "about communication" is a subset of Upstream collections in which the selector of a targeted person (such as an email address) may be contained within the communication but the targeted person is not necessarily a participant in the communication. In addition to collecting communications that are "to" or "from" the selector that has been tasked, communications may be collected if they contain the selector in the body of the communication, and thus are "about" the selector.

Minimization: In this testimony, it is not possible to list all or even most of the policies that fall under the umbrella of minimization. However, the agency minimization procedures are particular procedures that are central to the program and worth special mention. Every agency that accesses Section 702 information must have its own set of minimization procedures that are approved by the FISA Court. Minimization procedures are best understood as a set of controls designed to balance privacy and national security interests, minimize the acquisition and retention of U.S. person information, and control the dissemination of nonpublic information about United States persons.

An agency's minimization procedures significantly impact how analysts at that agency can access and analyze Section 702 information. All minimization procedures reviewed by the

[4] "Reverse targeting" would occur if the government were to intentionally target persons reasonably believed to be located outside the United States "if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States."

[5] An MCT is an Internet "transaction" that contains more than one discrete communication within it, which could contain purely domestic communications if one of the communications contains a selector.

Board dictate that an analyst can only access unminimized Section 702 information as a result of a query if that analyst or agent has the appropriate training and authorization. Different agencies accomplish this in different ways. The NSA procedures further require that queries of unminimized Section 702 information be designed such that they are "reasonably likely to return foreign intelligence information." This prohibition against overbroad queries or queries conducted for purposes other than to identify foreign intelligence information applies to all of the NSA queries of unminimized Section 702 information, not just queries containing U.S. person identifiers.

Analysis: Once an analyst has tasked selectors and obtained information from communications providers, the information can be analyzed and queried. A query is similar to a search term that is used in an Internet search engine. The term could be, for example, an email address, a telephone number, a key word or phrase, or a specific identifier that an agency has assigned to an acquired communication.

In addition to the general requirements that queries be reasonably scoped and related to a foreign intelligence purpose, I want to mention two additional NSA policies that illustrate the complex rules that govern querying

First, special rules apply when an NSA analyst wants to use a U.S. person identifier to query unminimized Section 702 information. Analysts are flatly prohibited from using U.S. person identifiers to query the NSA's Section 702 Upstream collection of Internet transactions. In contrast to this prohibition, the NSA's Upstream telephony collection and PRISM data may be queried using U.S. person identifiers if those U.S. person identifiers have been approved pursuant to internal NSA procedures.

Second, content queries using U.S. person identifiers are not permitted under NSA procedures unless the U.S. person identifiers have been pre-approved through one of several processes, a number of which incorporate other FISA procedures.

Dissemination: Agencies that receive Section 702 communications may disseminate to another U.S. intelligence agency foreign intelligence information of or concerning a U.S. person, or evidence of a crime concerning a U.S. person, acquired from such communications. This is done most frequently by the NSA, which typically masks the information about that U.S. person by redacting details that could be used to identify him or her. Agencies receiving this information may request the NSA unmask it if they are deemed to legitimately require the information for their mission.

Retention/Destruction: Retention and destruction of information gathered under the Section 702 program is also governed by agency-specific policies. Under NSA procedures, if a communication is purely domestic, the communication must be promptly destroyed upon recognition unless the Director of the NSA determines that the sender or recipient has been lawfully targeted and that the communication is reasonably believed to contain significant foreign intelligence information, evidence of a crime, or technical information for signal exploitation. The agency also may retain communications that contain information indicating an imminent threat of serious harm to life or property.

As a general matter, NSA procedures mandate that all telephone and Internet transactions obtained from service providers under Section 702 be destroyed within five years of the FISC's certification. A transaction may be retained for longer than five years if the NSA determines that the information is necessary for the maintenance of technical databases, evidence of a crime, or satisfies the dissemination standards.

Although these exceptions seem limited, they can allow the government to retain a substantial amount of information beyond the time when it would automatically be purged. Information can satisfy the dissemination standard, for example, if it is "necessary to understand foreign intelligence information or assess its importance," indicates that U.S. person "may be the target of intelligence activities" by a foreign government, or "the communication indicates that the United States person may be engaging international terrorist activities." The NSA may also retain a communication containing U.S. person information if the communication is reasonably believed to contain evidence of a crime and the NSA has or will disseminate that evidence to a federal law enforcement entity. Additionally, the NSA may retain communications beyond the normal age-off period if encrypted or if they are being used to decrypt other communications.

The NSA's minimization procedures further require the destruction of irrelevant U.S. person communications, but analysts are required to make such determinations only "at the earliest practicable point in the processing cycle," and 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. In practice, this destruction rarely happens.

Upstream Internet transactions are subject to different rules. These transactions must be destroyed within two years of the expiration of the FISC's certification, unless at least one communication within the transaction meets the NSA's retention standards.

II. PCLOB's Recommended Changes to the Section 702 Program

In addition to understanding the authorities and mechanisms underlying the Section 702 program, it is important to recognize how the program has changed in the past several years. One of the primary catalysts of this change was the 2014 PCLOB report, which closely examined the program. The report was drafted after months of working with the Intelligence Community to understand surveillance under Section 702, holding public meetings, conferring with Congressional staff, and meeting with advocacy groups. It embodied the Board's statutory mission of ensuring that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

After describing and analyzing surveillance under Section 702, the PCLOB report concluded that "the program was authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool." Although the report noted that "the applicable rules potentially allow a great deal of private information about U.S. persons to be acquired by the government," the Board did not conclude that the program was illegal or unconstitutional. During the course of its investigation, the Board found that the program has proven valuable in a number of ways to the government's efforts to combat terrorism. It has helped the United States learn more about the membership, leadership structure, priorities, strategies, 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. The Board was informed that over a quarter of the NSA's 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.

As part of its review of the Section 702 program, the Board provided a set of ten unanimous recommendations to "ensure that the program remains tied to its constitutionally legitimate core." The Board's recommendations touched on all stages of the program and implicated every agency that had access to information derived from it. Recommendations ranged from making the CIA, FBI, and NSA minimization procedures public, to requiring analysts to document their justification for conducting queries with U.S. person identifiers, to examining the possibility of limiting certain types of "about collection."

The Executive Branch, including the Intelligence Community, has been receptive to the PCLOB recommendations. Changes made by the government have been compiled and published in two Recommendations Assessment Reports released by the PCLOB in early 2015 and 2016. According to the most recent report, five Board recommendations were implemented, one was substantially implemented, one was implemented in part, and three are in the process of being implemented.

It is encouraging that every one of the Board's recommendations has either been implemented to some degree or is being implemented. Looking at the changes to the Section 702 program, there is no question that the government has made substantial efforts to address the Board's concerns. Notably, as part of the annual process of reauthorizing the Section 702 program, the government submitted revised targeting and minimization procedures for approval by the FISA Court. These revised procedures, all of which were approved, include changes designed to address several recommendations in the Board's report. In seeking annual recertification of the Section 702 program, the government also submitted all the supplemental materials recommended by the PCLOB. These included a sample of tasking sheets, a sample of U.S. person query terms, and a single consolidated document describing all significant rules governing the program. In doing so, the government has helped facilitate the FISA Court's ability to take a greater role in assessing the Section 702 program.

In light of these reforms, there is no question that the Section 702 program is more protective of privacy and civil liberties than it was in 2014. However, there is still room for important improvements.

III. Recommended Legislative Changes

In the coming months, the Committee will consider whether to reauthorize the Section 702 program and, if the program is to continue, how it can be improved. On the question of reauthorization, I remain convinced that the program provides important tools that the Intelligence Community effectively leverages to further its mission. But if the program is to continue, it should be more protective of privacy and civil liberties, particularly when U.S. persons are implicated. Against this backdrop, there are three areas of particular concern that I

would like to address: (1) the standards for querying Section 702 information using U.S. person identifiers; (2) the Upstream collection of "about" communications; and (3) quantifying the number of USPs communications that are collected under Section 702.

A. U.S. Person Queries

The first area of concern that I want to focus on is queries using U.S. person identifiers. U.S. person queries inherently raise privacy and civil liberties concerns because they are the means through which government analysts can access and compile vast amounts of sensitive information about U.S. persons. Section 702 allows the government to collect a massive number of communications, and as a default, store them for five years or more. Although U.S. persons cannot be targeted for Section 702 collection, the government incidentally acquires information about a U.S. person when a target communicates with that person. As a result, government databases inevitably contain deeply personal communications by, from, and concerning U.S. persons. Many of these communications have nothing to do with terrorism or crime. Rather, they can include family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges. U.S. person queries are, therefore, capable of revealing a significant slice of an American's personal life. This is particularly the case for Americans who correspond frequently with foreigners, including relatives, friends, and business associates.

It is important to remember that Section 702 targets need not be suspected terrorists or wrongdoers – they must only have relevant foreign intelligence information. As a result, the target could be completely innocent of any actual or even suspected transgression, making it even less likely that the U.S. person's communications with the target will have foreign intelligence value. In theory, such innocent communications will be deleted by the intelligence agencies. But in practice, as the Board's Section 702 report notes, they rarely are deleted.[6]

Once an agency receives Section 702 information, it can query it using one or more terms or identifiers. Section 702 queries do not cause the government to collect any new communications, but do permit the government to more efficiently search through and discover information in the data the government has already acquired. While the U.S. person cannot be targeted, this means that the person's communications with any or all of the tens of thousands of Section 702 targets over a period of five years or more could be compiled and reviewed many times over.

[6] I would also urge the Committee to consider imposing additional requirements regarding the purging of the results of U.S. person queries. The current internal agency procedures for reviewing communications and purging those portions that are of no foreign intelligence value are wholly inadequate to protect Americans' acknowledged constitutional rights to protection of their private information. Minimization guidelines approved by the FISA court were intended to afford these protections, but in their present form, they do not. As a practical matter, most collected communications are not reviewed for purging of non-foreign intelligence matters upon collection, or at any set time thereafter prior to use. Congress can remedy this situation by requiring that, no later than when the results of a U.S. person query of Section 702 data are generated, Americans' communications be purged of information that does not meet the statutory definition of foreign intelligence information.

Agency-specific minimization procedures govern queries, and generally require that queries not be overbroad and only be conducted if an analyst has a foreign intelligence purpose. Additional rules apply to U.S. person queries. If it is a content query, special approval is required. For example, the NSA allows U.S. person queries if the subject is already subject to a FISA Court-approved electronic surveillance, or with approval from the NSA's Office of General Counsel after a showing is made regarding why the proposed use of the U.S. person identifier would be "reasonably likely to return foreign intelligence information." In 2015, ODNI estimates that 23,800 U.S. person metadata queries and 4,672 U.S. person content queries were conducted.

U.S. person queries can clearly have value in determining whether U.S. persons present a danger to the United States or if such persons have valuable information that could be used to protect the country. The question is how to balance these national security benefits with the impact of queries on Americans' privacy and civil liberties. In my view, to adequately address the intrusive potential of U.S. person queries and protect the privacy of innocent Americans, Congress should change the way such queries are approved.

By analogy, in a typical criminal case, it is not unusual to collect Americans' incidental communications after a judge has issued a search warrant. In contrast, under Section 702 a federal judge has never issued a warrant to approve the collection. Since Section 702 collections lack the important Constitutional protections associated with prior approval by a federal judge, it is critical that the same protections be provided later in the process when the focus shifts from a non-U.S. person's to a U.S. person's communications. The Executive Branch has consistently informed the PCLOB that collection of such communications falls under the protections of the Fourth Amendment.

Intelligence agencies should be required to submit each U.S. person identifier to the FISA Court for approval before the identifier may be used to query information collected under Section 702 for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law. In Board Member Patricia Wald's and my separate statement in the Section 702 report, we proposed that the court should determine whether the use of the U.S. person identifier for Section 702 queries is reasonably likely to return foreign intelligence information as defined under FISA. This proposal represented a middle course: it did not ban queries or require a warrant, but instead required judicial approval of queries with a focus on the evidence expected to be obtained. While I still support this legislative recommendation, I would not oppose requiring the government to meet a more exacting probable cause standard as others have suggested. Most important is that an impartial, life-tenured federal judge has the final say over access to Americans' personal communications collected incidentally under Section 702.

The discussion above has focused primarily on the NSA's activities in conducting queries for national security purposes. But, the FBI is also permitted to query Section 702 communications for law enforcement purposes. The FBI's minimization procedures permit the agency to conduct reasonably designed queries "to find and extract" both "foreign intelligence information" and "evidence of a crime." Although pursuant to a PCLOB recommendation, the FBI has recently updated its procedures to be more transparent about how often such queries are

conducted, it should be noted that the FBI does not just conduct U.S. person queries in the context of law enforcement investigations when there is some suspicion of wrongdoing. It also queries its Section 702 holdings when it opens "assessments," which do not require a belief that there has been any wrongdoing.

As a matter of law, the reasonableness of surveillance depends upon whether there are sufficient safeguards to adequately protect the Fourth Amendment interests of persons whose communications may be collected, used, and disseminated. Against this backdrop, I find it perplexing that the FBI can search through years of a U.S. person's communications for information that may lead to criminal charges without a warrant or any kind of external oversight. As the Supreme Court recently explained in *Riley v. California*, "the fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years."[7] Likewise, the FBI should not be able to review vast amounts of personal information based on an unfounded or even no suspicion.

To remedy this situation, I recommend that in a reauthorized Section 702, the Committee require that the FBI submit each U.S. person identifier to the FISA Court for approval before the identifier may be used to query Section 702 data, other than in exigent circumstances. The court should determine at a minimum that, based on documentation submitted by the government, the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime, or a higher probable cause standard should Congress choose to impose it.

B. Upstream Collection/About Communications

Upstream collection and "about" communications are linked in the context of the Section 702 program. As noted above, Upstream collection occurs with the compelled assistance of providers that control the telecommunications "backbone" over which telephone and Internet communications transit. Internet transactions obtained in this manner are first filtered to eliminate potential domestic transactions, and then screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. Once ingested, information from Upstream collection can be stored for two years.

An "about" communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication. For example, assume the NSA tasked the email address "JohnTarget@example.com" to Section 702 Upstream collection. The NSA could potentially acquire communications routed through the Internet backbone that were sent *from* email address JohnTarget@example.com, that were sent *to* JohnTarget@example.com, and communications that *mentioned* JohnTarget@example.com in the body of the message.

The Upstream collection of "about" communications raises a number of distinct concerns. One issue raised in the PCLOB report is that "about" collection may be more likely

[7] 134 S. Ct. 2473, 2493 (2014).

than other forms of collection to acquire wholly domestic communications. This is because filters are imperfect, and "about" communications are not necessarily to or from the email address that was tasked for acquisition, which is used by a non-U.S. person reasonably believed to be located outside the United States. Under these circumstances, there is no guarantee that any of the participants to the communication are located outside the United States.

More significantly, "about" collection permits the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications. Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, without a warrant the Fourth Amendment prohibits the government from opening and reading letters sent through the mail in order to acquire those that contain particular information. The government likewise cannot listen to and record telephone conversations without probable cause about one of the callers. Admittedly, in these more traditional contexts, it is not feasible to inspect communications so that only communications "about" someone or something are accessible. But this fact does not make "about" communications less intrusive, or entitle them to less scrutiny.

Reiterating and building on the recommendations put forward in the PCLOB Section 702 report, I urge the Committee to impose additional limits on "about" collection and push for more safeguards on how such information is analyzed. Section 702 should not allow the NSA to access potentially sensitive communications between innocent people unless the need is great and the alternatives are limited. An important preliminary reform is for the NSA to build on its efforts to filter Upstream communications to avoid collection of purely domestic communications. Even if domestic communications were to constitute a very small percentage of Upstream collection, this could still result in a large overall number of purely domestic communications being collected. It is thus important that, as technology evolves, the government be required to evaluate the effectiveness of existing filters and investigate ways to improve them. The government should make every effort to utilize the best technology consistent with program needs to prevent the inadvertent collection of domestic communications. To facilitate this, the government must continue to engage in a dialogue with telecommunications providers and independent experts, and provide regular updates to the Committee and oversight agencies to ensure that the best filtering technology is being used.

Another recommendation is that the NSA be required to periodically review whether it is technically feasible to limit, as appropriate, the types of "about" collection or to separate the results of such collections into different categories. Some forms of "about" communications are actually the communications of targeted persons. Other types of "about" collection can result in the acquisition of communications between two non-targets, thereby implicating greater privacy concerns. Requiring such segregation can allow for legal and policies decisions to be made about the propriety of each type of collection. The NSA has indicated that current technological limits make it largely infeasible to restrict "about" collection without also limiting the other Upstream collections that are important to the government's counterterrorism efforts. The NSA should be

required to investigate and develop technology that will allow it to automatically segregate all "about" communications after collection (and, if possible, to individually segregate different types of "about" communications from one another after collection) and report regularly to Congress on its efforts. It may be that this technology is never feasible, but given the stakes, the NSA should bear the burden of continually and proactively pursuing it if the agency is to continue to utilize collection of "about" communications.

C. Quantifying USP Collections

From a privacy and civil liberties perspective, the collection and querying of U.S. person information are among the most concerning aspects of the Section 702 program. Section 702 only authorizes the collection of information about foreign targets, but large numbers of U.S. persons' incidental communications are also collected. In order to have an informed democratic debate about the scope of this program, it is important for citizens and members of Congress to know how many U.S. persons are implicated. In recognition of this fact, the PCLOB recommended that the NSA annually provide certain statistics that would provide insight into the number of U.S. person records it incidentally collects. The government had asserted that it could not provide the actual number because it is often difficult to determine from a communication the nationality of its participants. Additionally, the government noted that the large volume of collection under Section 702 would make it impossible to conduct such determinations for every communication that is acquired. In the nearly two years since the PCLOB report, the government has made efforts to implement the particular metrics recommended by the PCLOB, but has reiterated that gathering certain statistics continues to pose a variety of challenges.

I have no reason to doubt that the government has encountered difficulties in quantifying the number of U.S. person records that it incidentally collects. Nevertheless, going beyond the recommendations in the Board's report, I urge the Congress to require all agencies collecting information under Section 702 to develop a manageable way to gather these statistics and provide them to ODNI on an annual basis. ODNI, in turn, should issue yearly reports to Congress and relevant oversight agencies. The reports should include a variety of statistics that can facilitate an impact analysis of the Section 702 program, including the number of U.S. person records incidentally collected, and clearly describe the methodology used to gather the statistics. If this information is not available, it will be difficult for Congress to determine if the program is operating as it should be and ensure there is sufficient accountability.

Two arguments are likely to be put forward against this recommendation. First, the government may claim it is too burdensome to count the number of U.S. persons' communications given the huge volume of Section 702 collections. The government should be permitted to use appropriate sampling methodology to address this concern. Second, the government may assert that any attempt to document the nationality of participants to communications acquired under Section 702 would actually be invasive of privacy, because it would require government personnel to spend time scrutinizing the contents of private messages that they otherwise might never access or closely review. Again, this need not be done for every communication. There may also be indications that a communications involves a U.S. person

without reviewing it. The methodology used by the government can and should be designed to minimize the privacy impact of this effort.

IV. Conclusion

I hope Congress will use the reauthorization process as an opportunity to enhance privacy and civil protections in Section 702 while maintaining a program that has provided enormously valuable information to protect our country from terrorism. I appreciate the opportunity to present my views to the Committee.