EXHIBIT C

Privacy and Civil Liberties Oversight Board

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Part 1:

INTRODUCTION

I. Background

Shortly after the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") began operation as a new independent agency, Board Members identified a series of programs and issues to prioritize for review. As announced at the Board's public meeting in March 2013, one of these issues was the implementation of the Foreign Intelligence Surveillance Act Amendments Act of 2008.[1]

Several months later, in June 2013, two classified National Security Agency ("NSA") collection programs were first reported about by the press based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA. Under one program, implemented under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata (i.e., call records) in bulk. Under the other program, implemented under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person[2] located outside the United States.

A bipartisan group of U.S. Senators asked the Board to investigate the two NSA programs and provide an unclassified report.[3] House Minority Leader Nancy Pelosi subsequently asked the Board to consider the operations of the Foreign Intelligence Surveillance Court ("FISA court").[4] Additionally, the Board met with President Obama, who asked the Board to "review where our counterterrorism efforts and our values come into

---

1 *See* Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, *available at* http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf.

2 Under the statute, the term "U.S. persons" includes United States citizens, United States permanent residents, and virtually all United States corporations.

3 Letter from Tom Udall *et al*. to the Privacy and Civil Liberties Oversight Board (June 12, 2013), *available at* http://www.pclob.gov/SiteAssets/newsroom/6.12.13%20Senate%20letter%20to%20PCLOB.pdf. Response *available at* http://www.pclob.gov/SiteAssets/newsroom/PCLOB_TUdall.pdf.

4 Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), *available at* http://www.pclob.gov/SiteAssets/newsroom/Pelosi%20Letter%20to%20PCLOB.pdf. Response *available at* http://www.pclob.gov/SiteAssets/newsroom/PCLOB%20Pelosi%20Response%20Final.pdf.

tension."[5] In response to the requests from Congress and the President, the Board began a comprehensive study of the two NSA programs. The Board held public hearings and met with the Intelligence Community and the Department of Justice, White House, and congressional committee staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies.

During the course of this study, it became clear to the Board that each program required a level of review that was best undertaken and presented to the public in a separate report. As such, the Board released a report on the Section 215 telephone records program and the operation of the FISA court on January 23, 2014.[6] Subsequently, the Board held an additional public hearing and continued its study of the second program. Now, the Board is issuing the current report, which examines the collection of electronic communications under Section 702, and provides analysis and recommendations regarding the program's implementation.

The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

The Board has found that certain aspects of the program's implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons' communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

II. Study Methodology

In order to gain a full understanding of the program's operations, the Board and its staff received multiple briefings on the operation of the program, including the technical

---

[5] Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

[6] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

target, because two non-U.S. persons are discussing a U.S. person, or because a U.S. person was mistakenly targeted. Section 702 therefore requires that certifications also include "minimization procedures" that control the acquisition, retention, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program.[74] As discussed below, the minimization procedures include different procedures for handling U.S. person information depending on the circumstances of how it was acquired. Along with the targeting procedures, the minimization procedures contain the government's core privacy and civil liberties protections and are more fully discussed throughout this Report.

C. FISC Review

The government's Section 702 certifications, targeting procedures, and minimization procedures (but not the Attorney General Guidelines) are all subject to review by the FISC.[75] In addition to the required procedures and guidelines, the Section 702 certifications are accompanied by affidavits of national security officials[76] that further describe to the FISC the government's basis for assessing that the proposed Section 702 acquisition will be consistent with the applicable statutory authorization and limits.[77] Through court filings or the testimony of witnesses at hearings before the FISC, the government also submits additional information explaining how the targeting and minimization procedures will be applied and describing the operation of the program in a way that defines its scope.[78]

The FISC's review of the Section 702 certifications has been called "limited" by scholars,[79] privacy advocates,[80] and in one instance, shortly after the FISA Amendments Act

---

74 50 U.S.C. § 1881a(e)(1), (g)(2)(A)(ii), (g)(2)(B).

75 50 U.S.C. § 1881a(d)(2), (e)(2), (i). The Attorney General Guidelines must, however, be submitted to the FISA court. 50 U.S.C. § 1881a(f)(2)(C). Section 702 does have a provision permitting the Attorney General and the Director of National Intelligence to authorize acquisition prior to judicial review of a certification under certain exigent circumstances. 50 U.S.C. § 1881a(c)(2). To date, the Attorney General and the Director of National Intelligence have never exercised this authority.

76 50 U.S.C. § 1881a(g)(2)(C); *see, e.g.*, Memorandum Opinion at 3, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011) ("Bates October 2011 Opinion") (noting submitted affidavits by the Director or Acting Director of NSA and the Director of FBI), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

77 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-1 to A-2.

78 *See, e.g.,* Bates October 2011 Opinion, *supra*, at 5-9, 2011 WL 10945618, at *2-4 (describing 2011 government filings with, and testimony before, the FISA court); *id*. at 15-16, 2011 WL 10945618, at *5 (describing representations made to the FISA court in prior Section 702 certifications).

79 *See, e.g.*, Laura K. Donohue, Section 702 and the Collection of International Telephone and Internet Content, at 15, 18, 30-34, *available at* http://justsecurity.org/wp-content/uploads/2014/05/donahue.702.pdf.

was passed, by the FISC itself.[81] In certain respects, this characterization is accurate. Unlike traditional FISA applications, the FISC does not review the targeting of particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding which information is to be acquired, the FISC does not see or approve the specific persons targeted or the specific communication facilities that are actually tasked for acquisition. As such the government does not present evidence to the FISC, nor does the FISC determine — under probable cause or any other standard — that the particular individuals being targeted are non-U.S. persons reasonably believed to be located outside the United States who are being properly targeted to acquire foreign intelligence information.[82] Instead of requiring judicial review of these elements, Section 702 calls upon the FISA court only to decide whether the targeting procedures are reasonably designed to ensure compliance with certain limitations and that the minimization procedures satisfy certain criteria (described below). The FISC is not required to independently determine that a significant purpose of the proposed acquisition is to obtain foreign intelligence information,[83] although the foreign intelligence purpose of the collection does play a role in the court's Fourth Amendment analysis.[84]

In other respects, however, the FISC's role in the Section 702 program is more extensive. The FISC reviews both the targeting procedures and the minimization procedures, the core set of documents that implement Section 702's statutory requirements and limitations.[85] With respect to the targeting procedures, the FISC must

---

80 *See, e.g.*, Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation, Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, at 9 (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf.

81 Memorandum Opinion, *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, Docket Misc. No. 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug. 27, 2008).

82 *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 2 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. *See* Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Honorable Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

83 50 U.S.C. § 1881a(i)(2).

84 Additionally, if the FISC determines that a Section 702 certification and related documents are insufficient on Constitutional or statutory grounds, the FISC cannot itself modify the certification and related documents governing the Section 702 program, but instead must issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification. 50 U.S.C. § 1881a(i)(3)(B).

85 50 U.S.C. § 1881a(d)(2), (e)(2), (i)(1)(A).

determine that they "are reasonably designed" to "ensure" that targeting is "limited to targeting persons reasonably believed to be located outside the United States."[86] The FISC also must determine that the targeting procedures are reasonably designed to prevent the intentional acquisition of wholly domestic communications.[87] In addition, the FISC must also review the proposed minimization procedures under the same standard of review that is required in traditional FISA electronic surveillance and physical search applications.[88] The FISC must find that such minimization procedures are "specific procedures" that are "reasonably designed" to control the acquisition, retention, and dissemination of non–publicly available U.S. person information.[89] Each time the FISC reviews a Section 702 certification, the FISC must also determine whether the proposed Section 702 acquisition as provided for, and restricted by, the targeting and minimization procedures complies with the Fourth Amendment.[90] After conducting its analysis, the FISC must issue a written opinion explaining the reasons why the court has held that the proposed targeting and minimization procedures do, or do not, comply with statutory and Fourth Amendment requirements.[91]

The FISC has held that it cannot make determinations in a vacuum regarding whether targeting and minimization procedures are "reasonably designed" to meet the statutory requirements and comply with the Fourth Amendment. To the contrary, the FISC "has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired," and that "[s]ubstantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the communications of non-U.S. persons outside the United States.'"[92] Therefore, although the FISC reviews the targeting procedures, minimization procedures, and related affidavits that

---

86 50 U.S.C. § 1881a(i)(2)(B)(i).

87 50 U.S.C. § 1881a(i)(2)(B)(ii).

88 *Compare* 50 U.S.C. § 1881a(i)(2)(C) (requirement to evaluate Section 702 minimization procedures) *with* 50 U.S.C. § 1805(a)(3) (requirement to evaluate FISA electronic surveillance minimization procedures) *and* 50 U.S.C. § 1824(a)(3) (requirement to evaluate FISA physical search minimization procedures).

89 50 U.S.C. § 1801(h).

90 50 U.S.C. § 1881a(i)(3)(A), (i)(3)(B).

91 50 U.S.C. § 1881a(i)(3)(C). While FISC judges may write opinions explaining their orders with regard to other aspects of FISA, the statutory requirement for an opinion explaining the rationale of all orders approving Section 702 certifications is unique within FISA. Though not required by FISA, FISC Rule of Procedure 18(b)(1) also requires FISC judges to provide a written statement of reasons for any denials of the government's other FISA applications. *See* United States Foreign Intelligence Surveillance Court Rules of Procedure ("FISC Rule of Procedure"), Rule 18(b)(1), *available at* http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

92 Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9 (quoting FISC opinion with redacted docket number).

are submitted with a Section 702 certification, the court's review is not limited to the four corners of those documents. The FISC also takes into consideration additional filings by the government to supplement or clarify the record, responses to FISC orders to supplement the record,[93] and the sworn testimony of witnesses at hearings.[94]

Commitments regarding how the targeting and minimization procedures will be implemented that are made to the FISC in these representations have been found to be binding on the government. For example, during the consideration of the first Section 702 certification in 2008, the government stated that that the targeting procedures impose a requirement that analysts conduct "due diligence" in determining the U.S. person status of any Section 702 target, even though the phrase "due diligence" is not explicitly found in the text of the NSA targeting procedures. The FISC incorporated the government's representation regarding due diligence into its opinion, and the government has subsequently reported to Congress and the FISC — as incidents of noncompliance — instances in which the Intelligence Community conducted insufficient due diligence that resulted in the targeting of a U.S. person.[95]

In evaluating the Section 702 certifications, the court also considers additional filings required by the FISC's Rules of Procedure. One such rule requires the government to notify the FISA court whenever the government discovers a material misstatement or omissions in a prior filing with the court.[96] Another rule mandates that the government report to the FISA court incidents of noncompliance with targeting or minimization procedures previously approved by the court.[97] In a still-classified 2009 opinion, the FISC held that the judicial review requirements regarding the targeting and minimization procedures required that the FISC be fully informed of every incident of noncompliance

---

93 *See* FISC Rule of Procedure 5(c) (stating that the FISC Judges have the authority to order any party to a proceeding to supplement the record by "furnish[ing] any information that the Judge deems necessary").

94 FISC Rule of Procedure 17.

95 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29 (describing incidents and stating "In each of these incidents, all Section 702–acquired data was purged. Together, these [redacted] instances represent isolated instances of insufficient due diligence that do not reflect the [redacted] of taskings that occur during the reporting period.").

96 *See* FISC Rule of Procedure 13(a).

97 *See* FISC Rule of Procedure 13(b); SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, MAY 2010, at 22 ("MAY 2010 SEMIANNUAL ASSESSMENT") (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure), *available at* http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf. The government also provides the FISC the Semiannual Section 702 Joint Assessment, portions of the Section 707 Semiannual report, and a separate quarterly report to the FISC, all of which describe scope, nature, and actions taken in response to compliance incidents. *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 5; 50 U.S.C. § 1881a(l)(1).

with those procedures. In the 2009 opinion, the court analyzed whether several errors in applying the targeting and minimization procedures that had been reported to the court undermined either the court's statutory or constitutional analysis. (The court concluded that they did not.)

In addition to identifying errors that could impact the sufficiency of the targeting and minimization procedures, these compliance notices play an additional role in informing the FISC regarding how the government is in fact applying the targeting and minimization procedures. Specifically, the compliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident.[98] In doing so, representations to the FISA court have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court's conclusions regarding whether those procedures — as actually applied by the Intelligence Community to particular, real-life factual scenarios — comply with Section 702's statutory requirements and the Fourth Amendment. For example, while the 2008 FISC opinion incorporated the government's commitment to apply due diligence in determining the U.S. person status of potential targets, notices of non-compliance filed by the government reflect that the government interprets the targeting procedures to also require due diligence in determining the *location* of potential targets. Similarly, the government has filed letters clarifying aspects of its "post-tasking" process, which are discussed further below, and it has reported — as compliance incidents — instances when its performance of the post-tasking process has not complied with those representations. The government's interpretations of the targeting and minimization procedures reflected in these compliance filings, however, are not necessarily formally endorsed or incorporated into the FISC's subsequent opinions. In the Board's opinion Intelligence Community personnel applying these procedures months or years later may not be aware of the interpretive gloss arising from prior interactions between the government and the FISC on these procedures.

Former FISC Presiding Judge John Bates' October 3, 2011 opinion provides both an example of the scope of the FISA court's review of Section 702 certifications in practice and an illustration of what actions the court can take if it determines that the government has not satisfied the court's expectations to be kept fully, accurately, and timely informed. In April 2011, the government filed multiple Section 702 certifications with the FISC.[99] In early May 2011, however, the government filed a letter with the court (under a FISC procedural rule regarding material misstatements or omissions) acknowledging that the scope of the NSA's "upstream" collection (described below) was more expansive than

---

98 FISC Rule of Procedure 13(b).

99 Bates October 2011 Opinion, *supra*, at 3, 2011 WL 10945618, at *1.

previously represented to the court.[100] As a result of the filing, the FISC expressed serious concern that the upstream collection, as described by the government, may have exceeded the scope of collection previously approved by the FISC and what could be authorized under Section 702. The FISC therefore ordered the government to respond to a number of questions regarding the upstream collection program.[101] Throughout the summer of 2011, the government continued to supplement the record in response to the FISA court's concerns with a number of filings, including by conducting and reporting to the court the results of a statistical sample of the NSA's acquisition of upstream collection.[102] The government's supplemental filings discussed both factual matters, such as how many domestic communications were being acquired as a result of the manner in which the government was conducting upstream collection, as well as the government's legal interpretations regarding how the NSA's minimization procedures should be applied to such acquisition.[103] The FISA court also met with the government and held a hearing to ask additional questions of NSA and Department of Justice personnel.[104]

Based on this record, Judge Bates ultimately held that in light of the new information, portions of the NSA minimization procedures met neither the requirements of FISA nor the Fourth Amendment and ordered the government to correct the deficient procedures or cease Section 702 upstream collection.[105] The government subsequently modified the NSA minimization procedures to remedy the deficiencies identified by the FISA court.[106] The FISC continued to have questions, however, regarding upstream collection that had been acquired prior to the implementation of these modified NSA minimization procedures.[107] The government took several actions with regard to this past upstream collection, and ultimately decided to purge it all.[108]

---

100 Bates October 2011 Opinion, *supra*, at 5, 2011 WL 10945618, at *2.

101 Bates October 2011 Opinion, *supra*, at 7, 2011 WL 10945618, at *2.

102 Bates October 2011 Opinion, *supra*, at 10, 2011 WL 10945618, at *3-4.

103 Bates October 2011 Opinion, *supra*, at 33-35, 50, 54-56, 2011 WL 10945618, at *11, *17, *18-19.

104 Bates October 2011 Opinion, *supra*, at 7-9, 2011 WL 10945618, at *4.

105 Bates October 2011 Opinion, *supra*, at 59-63, 67-80, 2011 WL 10945618, at *20-28.

106 *See generally* Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011) ("Bates November 2011 Opinion"), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

107 *See* Memorandum Opinion at 26-30, [*Caption Redacted*], [Docket No. Redacted], 2012 WL 9189263, at *1-4 (FISA Ct. Sept. 25, 2012) ("Bates September 2012 Opinion"), *available at* http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

108 Bates September 2012 Opinion, *supra*, at 30-32, 2012 WL 9189263, at *3-4.

D. Directives

As noted above, Section 702 targeting may occur only with the assistance of electronic communication service providers. Once Section 702 acquisition has been authorized, the Attorney General and the Director of National Intelligence send written directives to electronic communication service providers compelling the providers' assistance in the acquisition.[109] Providers that receive a Section 702 directive may challenge the legality of the directive in the FISC.[110] The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government's acquisition of foreign intelligence information.[111] The FISC's decisions regarding challenges and enforcement actions regarding directives are appealable to the Foreign Intelligence Surveillance Court of Review ("FISCR"), and either the government or a provider may request that the United States Supreme Court review a decision of the FISCR.[112]

III. Acquisition Process: How Does Section 702 Surveillance Actually Work?

Once a Section 702 certification has been approved, non-U.S. persons reasonably believed to be located outside the United States may be targeted to acquire foreign intelligence information within the scope of that certification. The process by which non-U.S. persons are targeted is detailed in the next section. This section describes how Section 702 acquisition takes place once an individual has been targeted.

A. Targeting Persons by Tasking Selectors

The Section 702 certifications permit non-U.S. persons to be targeted only through the "tasking" of what are called "selectors." A selector must be a specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number.[113] Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are *targeted*; selectors (e.g., email addresses, telephone numbers) are *tasked*. The users of any tasked selector are

---

109 50 U.S.C. § 1881a(h).

110 50 U.S.C. § 1881a(h)(4).

111 50 U.S.C. § 1881a(h)(5).

112 50 U.S.C. § 1881a(h)(6). However, as noted in the Board's Section 215 report, to date, only two cases have been appealed to the FISCR. One, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004 (FISA Ct. Rev. 2008), involved a directive under the Protect America Act, the predecessor to Section 702, but none have involved Section 702. Nor has the U.S. Supreme Court ever considered the merits of a FISA order or ruled on the merits of any challenge to FISA.

113 *See* AUGUST 2013 JOINT ASSESSMENT, *supra*, at A-2; NSA DCLPO REPORT, *supra*, at 4; The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

considered targets — and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process.

Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden").[114] Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.[115]

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.[116]

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection. PRISM collection is the easier of the two acquisition methods to understand.

B. PRISM Collection

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or "ISP") that has been served a directive.[117] Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only "about" the selector, as described below).[118] As of mid-2011, 91 percent of the

---

114 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

115 NSA DCLPO REPORT, *supra*, at 6.

116 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), a*vailable at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

117 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. *See also* PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company "would have received legal process").

118 PCLOB March 2014 Hearing Transcript at 70; *see also* NSA DCLPO REPORT, *supra*, at 5.

Internet communications that the NSA acquired each year were obtained through PRISM collection.[119]

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company ("USA-ISP Company") may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address "johntarget@usa-ISP.com" to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and "tasks" johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government "detasks" johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.[120] The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.[121]

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.

---

119 Bates October 2011 Opinion, *supra*, at 29-30 and n.24, 2011 WL 10945618, at *25 & n.24.

120 Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 6(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures"), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

121 NSA 2011 Minimization Procedures, *supra*, § 6(c).

C. Upstream Collection

The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit.[122] The collection therefore does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs "upstream" in the flow of communications between communication service providers.[123]

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA's minimization procedures. [124] CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems.

The upstream acquisition of telephone and Internet communications differ from each other, and these differences affect privacy and civil liberty interests in varied ways.[125] Each type of Section 702 upstream collection is discussed below. In conducting both types of upstream acquisition, NSA employs certain collection monitoring programs to identify anomalies that could indicate that technical issues in the collection platform are causing data to be overcollected.[126]

---

122 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.").

123 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.").

124 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4.

125 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 27 (statement of Rajesh De, General Counsel, NSA).

126 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29.

1. Upstream Collection of Telephone Communications

Like PRISM collection, the upstream collection of telephone communications begins with the NSA's tasking of a selector.[127] The same targeting procedures that govern the tasking of an email address in PRISM collection also apply to the tasking of a telephone number in upstream collection.[128] Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-U.S. person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorized under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition.[129] The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are merely "about" the tasked telephone number.[130]

2. Upstream Collection of Internet "Transactions"

The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection.[131] And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.[132]

Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet

---

127 PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *id*. at 51-53 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

128 NSA DCLPO REPORT, *supra*, at 6.

129 PCLOB March 2014 Hearing Transcript, *supra*, at 53-54 (statements of Rajesh De, General Counsel, NSA, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

130 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5.

131 NSA DCLPO REPORT, *supra*, at 5-6.

132 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

communications, what is referred to as the "Internet backbone."[133] The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection.[134]

Upstream collection acquires Internet transactions that are "to," "from," or "about" a tasked selector.[135] With respect to "to" and "from" communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an "about" communication. 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.[136] If the NSA therefore applied its targeting procedures to task email address "JohnTarget@example.com," to Section 702 upstream collection, the NSA would 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 NSA would not, however, acquire communications simply because they contained the name "John Target." In a still-classified September 2008 opinion, the FISC agreed with the government's conclusion that the government's target when it acquires an "about" communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC's reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the

---

133 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4.

134 Bates October 2011 Opinion, *supra*, at 73, 2011 WL 10945618, at *26.

135 *See, e.g.*, October 2011 Opinion, *supra*, at 15-16, 2011 WL 10945618, at *5-6 (describing the government's representations regarding upstream collection in the first Section 702 certification the FISC reviewed).

136 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5; Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) ("December 2011 Joint Statement") (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf; PCLOB March 2014 Hearing Transcript, *supra*, at 55.

privacy intrusion even in the absence of abuse, and a number of the Board's recommendations are motivated by a desire to provide more clarity and transparency regarding the government's activities in the Section 702 program.

II. Value of the Section 702 Program

A. Advantages and Unique Capabilities

The Section 702 program makes a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition. 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, our focus in this section is limited to the counterterrorism value of the Section 702 program, although the program serves a broader range of foreign intelligence purposes.[457]

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 and Executive Order 12333, Section 702 offers advantages over these other authorities.

In order to conduct electronic surveillance under "traditional" FISA (i.e., Title I of the Foreign Intelligence Surveillance Act of 1978), the government must persuade the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"), 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.[458] 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.[459] To meet these requirements and satisfy the probable cause standard, facts must be gathered by the Intelligence Community, a detailed FISA court application must be drafted by the DOJ, the facts in the application must be vetted for accuracy, the senior

457 See page 25 of this Report.

458 50 U.S.C. § 1805(a)(2).

459 50 U.S.C. § 1804(a)(6).

government official's certification must be prepared, the Attorney General must approve the application, and the application must be submitted to the FISA court, which must review it, determine if the pertinent standards are met, and, if so, grant it.[460] These steps consume significant time and resources.[461] In practice, FISA applications are lengthy and the process not infrequently takes weeks from beginning to final approval.[462]

This system is deliberately rigorous, for it was designed to provide a check on the government's surveillance of U.S. persons and other people located in the United States. Its goal was to prevent the abusive and politically motivated surveillance of U.S. persons and domestic activists that had occurred under the guise of foreign intelligence surveillance in the mid-twentieth century. Under FISA, electronic surveillance may be directed only at individuals who are acting at the behest of a foreign power (such as a foreign government or international terrorist organization), only for legitimate foreign intelligence purposes, and only where the aims of the surveillance cannot be achieved by other means.[463] The statute's procedural hurdles help to ensure that surveillance takes place only after detailed analysis, a strong factual showing, measured judgment by high-level executive branch officials, and approval by a neutral judge.

Although the FISA process was designed for surveillance directed at people located in the United States, the government later sought and obtained approval from the FISA court to use this process to target foreign persons located outside the United States as well. Developments in communications technology and the Internet services industry meant that such surveillance could feasibly be conducted from within the United States in some instances.[464] Utilizing the process of traditional FISA to target significant numbers of individuals overseas, however, required considerable time and resources, and government officials have argued that it slowed and sometimes prevented the acquisition of important intelligence.[465]

---

460 *See* 50 U.S.C. §§ 1804, 1805.

461 These steps also must be repeated each time the government wishes to continue the surveillance beyond the time limit specified in the original order. *See* 50 U.S.C. § 1805(d).

462 FISA permits surveillance to begin prior to court approval in emergency situations, but in order to exercise this option the Attorney General must make a determination that an emergency exists and that the factual basis required for the surveillance exists, and an application must be submitted to the FISA court for the normal probable cause determination within seven days. *See* 50 U.S.C. § 1805(e).

463 Moreover, when the target of surveillance is a U.S. person, that person must be "knowingly" acting on behalf of a foreign power. *See* 50 U.S.C. § 1801(b)(1), (2). An exception to the requirement that the target be acting on behalf of a foreign power permits a so-called "lone wolf" with no apparent connection to a foreign power to be targeted, if there is probable cause that the person is engaged in international terrorism or proliferation of weapons of mass destruction. *See* 50 U.S.C. §§ 1801(b)(1)(C), (D), 1805(a)(2)(A).

464 See pages 16-18 of this Report.

465 See pages 18-19 of this Report.

Section 702 imposes significantly fewer limits on the government when it targets non–U.S. persons located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted.[466] Rather than approving or denying individual targeting requests, the FISA court 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.[467] 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.[468] 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. Targeting decisions are made by NSA analysts and reviewed only within the executive branch.[469] Once monitoring of a particular person begins, it may continue until new information indicates that the person no longer is an appropriate target. Whether a person remains a valid target must be reviewed annually.[470]

These differences allow the government to target a much wider range of foreigners 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, Section 702 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 FISA court for each targeting decision.

As a result of these two factors, the number of people who can feasibly be targeted is significantly greater under Section 702 than under the traditional FISA process. And

---

466 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).

467 50 U.S.C. § 1881a(a), (i).

468 NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 4 (April 16, 2014) ("NSA DCLPO REPORT"), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

469 NSA DCLPO REPORT, *supra*, at 4-5.

470 Analysts are required to review the communications acquired from a target at least annually, to ensure that the targeting is still expected to provide the foreign intelligence sought and that the person otherwise remains an appropriate target under Section 702. *See* NSA DCLPO REPORT, *supra*, at 6.

indeed, the number of targets under the program has been steadily increasing since the statute was enacted in 2008.

The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above.[471] Nevertheless, Section 702 offers advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In addition, acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.

B. Contributions to Counterterrorism

The Section 702 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, 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 the Section 702 program is indeed a *program*, operating to some degree as a cohesive whole and approved by the FISA court accordingly, its implementation consists entirely of targeting specific individuals about whom the government already knows something. Because surveillance is conducted on an individualized basis where there is reason to target a particular person, it is perhaps unsurprising that the program yields a great deal of useful information.

The value of the Section 702 program is to some extent reflected in the breadth of NSA intelligence reporting based on information derived from the program. Since 2008, the number of signals intelligence reports based in whole or in part on Section 702 has

---

471 FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes. *See* 50 U.S.C. §§ 1801(f), 1881c.

increased exponentially. A significant portion of those reports relate to counterterrorism, and the NSA disseminates hundreds of reports per month concerning terrorism that include information derived from Section 702. Presently, 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. 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.

More concretely, information acquired from Section 702 has helped the Intelligence Community to understand the structure and hierarchy of international terrorist networks, as well as their intentions and tactics. In even the most well-known terrorist organizations, only a small number of individuals have a public presence. Terrorist groups use a number of practices to obscure their membership and activities. Section 702 has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve.

Monitoring these networks under Section 702 has led the government to identify previously unknown individuals who are involved in international terrorism. Identifying such persons allows the government to pursue new efforts focusing on those individuals and the disruption of their activities, such as taking action to prevent them from entering the United States. Finally, the flexibility of Section 702 surveillance enables the government to effectively maintain coverage on particular individuals as they add or switch their modes of communications.

As important as discovering the identities of individuals engaged in international terrorism is determining where those individuals are located. Modern communications permit the members of a terrorist group, and even a small number of people involved in a specific plot, to be spread out all over the world. Information acquired from Section 702 has been used to monitor individuals believed to be engaged in terrorism.

In one case, for example, the NSA was conducting surveillance under Section 702 of an email address used 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.

Finally, pursuit of the foregoing information under Section 702 has led to the discovery of previously unknown terrorist plots and has enabled the government to

disrupt them. By providing the sites of specific targets of attacks, the means being contemplated to carry out the attacks, and the identities and locations of the participants, the Section 702 program has directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries.

For instance, in September 2009, the NSA monitored under Section 702 the email address of an Al Qaeda courier based in Pakistan. Through that collection, the agency intercepted emails sent to that address from an unknown individual located in the United States. Despite using language designed to mask their true intent, the messages indicated that the sender was urgently seeking advice on the correct mixture of ingredients to use for making explosives. The NSA passed this information to the FBI, which used a national security letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado. The FBI then began intense monitoring of Zazi, including physical surveillance and obtaining legal authority to monitor his Internet activity. The Bureau was able to track Zazi as he left Colorado a few days later to drive to New York City, where he and a group of confederates were planning to detonate explosives on subway lines in Manhattan within the week. Once Zazi became aware that law enforcement was tracking him, he returned to Colorado, where he was arrested soon after. Further investigative work identified Zazi's co-conspirators and located bomb-making components related to the planned attack. Zazi and one of his confederates later pled guilty and cooperated with the government, while another confederate was convicted and sentenced to life imprisonment. Without the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded.

In cases like the Zazi and Ouazzani investigations, one might ask whether the government could have monitored the communications of the overseas extremists without Section 702, using the traditional FISA process. In some instances, that might be the case. But the process of obtaining court approval for the surveillance under the standards of traditional FISA may, for the reasons explained above, limit the number of people the government can feasibly target and increase the delay before surveillance on a target begins, such that significant communications could be missed.

The Board has received information about other instances in which the Section 702 program has played a role in counterterrorism efforts. Most of these instances are included in a compilation of 54 "success stories" involving the Section 215 and 702 programs that was prepared by the Intelligence Community last year in the wake of Edward Snowden's unauthorized disclosures. Other examples have been shared with the Board more recently. Information about these cases has not been declassified, but some general information about them can be shared. In approximately twenty cases that we have reviewed, surveillance conducted under Section 702 was used in support of an already existing counterterrorism investigation, while in approximately thirty cases, Section 702

information was the initial catalyst that identified previously unknown terrorist operatives and/or plots. In the vast majority of these cases, efforts undertaken with the support of Section 702 appear to have begun with narrowly focused surveillance of a specific individual whom the government had a reasonable basis to believe was involved with terrorist activities, leading to the discovery of a specific plot, after which a short, intensive period of further investigation ensued, leading to the identification of confederates and arrests of the plotters. A rough count of these cases identifies well over one hundred arrests on terrorism-related offenses. In other cases that did not lead to disruption of a plot or apprehension of conspirators, Section 702 appears to have been used to provide warnings about a continuing threat or to assist in investigations that remain ongoing. Approximately fifteen of the cases we reviewed involved some connection to the United States, such as the site of a planned attack or the location of operatives, while approximately forty cases exclusively involved operatives and plots in foreign countries.[472]

C. Contributions to Other Foreign Intelligence Efforts

As noted above, the oversight mandate of our Board extends only to those measures taken by the government to protect the nation from terrorism. Some governmental activities, including the Section 702 program, are not aimed exclusively at preventing terrorism but also serve other foreign intelligence and foreign policy goals. The Section 702 program, for instance, is also used for surveillance aimed at countering the efforts of proliferators of weapons of mass destruction.[473] Given that these other foreign intelligence purposes of the program are not strictly within the Board's mandate, we have not scrutinized the effectiveness of Section 702 in contributing to those other purposes with the same rigor that we have applied in assessing the program's contribution to counterterrorism. Nevertheless, we have come to learn how the program is used for these other purposes, including, for example, specific ways in which it has been used to combat weapons proliferation and the degree to which the program supports the government's efforts to gather foreign intelligence for the benefit of policymakers. Our assessment is that the program is highly valuable for these other purposes, in addition to its usefulness in supporting efforts to prevent terrorism.

---

472 The examples described in this paragraph do not represent an exhaustive list of all instances in which the Section 702 program has proven useful, even in counterterrorism efforts.

473 *See* S. Rep. No. 112-229, at 32 (2012) (appendix reproducing Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director or National Intelligence) ("Section 702 . . . lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.").

III. Privacy and Civil Liberties Implications of the Section 702 Program

A. Nature of the Collection under Section 702

1. Programmatic Surveillance

Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information — and that this person uses a particular communications "selector," such as an email address or telephone number — the government acquires only those communications involving that particular selector.[474]

Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ and the ODNI ("the DOJ/ODNI oversight team") in an effort to ensure that the person targeted is reasonably believed to be a non-U.S. person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA court does not approve individual targeting decisions or review them after they are made.

Although the "persons" who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,[475] the government is not exploiting any legal ambiguity by "targeting" an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence. Rather, the government first identifies a communications identifier, like an email address, that it reasonably believes is used by the target, whether that target is an individual or an entity. It then acquires only those communications that are related to this identifier.[476] In other words, selectors are always

---

474 See pages 20-23 and 32-33 of this Report.

475 *See* 50 U.S.C. §§ 1801(m), 1881a(a).

476 The NSA's "upstream collection" (described elsewhere in this Report) may require access to a larger body of international communications than those that contain a tasked selector. Nevertheless, the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector. Only those communications (or more precisely, "transactions") that contain a tasked selector go into government databases. See pages 36-41 of this Report.

For now, therefore, "about" collection is an inextricable part of the NSA's upstream collection, which we agree has unique value overall that militates against eliminating it entirely. As a result, any policy debate about whether "about" collection should be eliminated in whole or in part may be, to some degree, a fruitless exercise under present conditions. From our perspective, given a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable. As explained later, however, because of the serious and novel questions raised by "about" collection as a constitutional and policy matter, we recommend that the NSA develop technology that would allow it to selectively limit or segregate certain forms of "about" communications — so that a debate can be had in which the national security benefits of the different forms of "about" collection are weighed against their respective privacy implications.

We emphasize, however, that our acceptance of "about" collection rests on the considerations described above — the inextricability of the practice from a broader form of collection that has unique value, and the limited nature of what "about" collection presently consists of: the acquisition of Internet communications that include the communications identifier of a targeted person. Although those identifiers may sometimes be found in the body of a communication, the government is not making any effort to obtain communications based on the ideas expressed therein. We are not condoning expanding "about" collection to encompass names or key words, nor to its use in PRISM collection, where it is not similarly inevitable. Finally, our unwillingness to call for the end of "about" collection is also influenced by the constraints that presently govern the use of such communications after acquisition. As with all upstream collection, "about" communications have a default retention period of two years instead of five, are not routed to the CIA or FBI, and may not be queried using U.S. person identifiers.

4. Multi-Communication Transactions ("MCTs")

The technical means used to conduct the NSA's upstream collection result in another issue with privacy implications. Because of the manner in which the agency intercepts communications directly from the Internet "backbone," the NSA sometimes acquires communications that are not themselves authorized for collection (because they are not to, from, or "about" a tasked selector) in the process of acquiring a communication that *is* authorized for collection (because it is to, from, or "about" a tasked selector). In 2011, the FISA court held that the NSA's procedures for addressing this problem were inadequate, and that without adequate procedures this aspect of the NSA's collection practices violated the Fourth Amendment. The government subsequently altered its procedures to the satisfaction of the FISA court. Based on the Board's assessment of how those procedures are being implemented today, the Board agrees that existing practices strike a reasonable balance between national security and privacy.