CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

JULY 25, 2014 DECLARATION OF RICHARD R. WIEBE IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

(Fourth Amendment Violation)

Date: October 31, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action. Except as otherwise stated below, I could and would testify competently to the following.

2. Each exhibit attached hereto is a true and correct copy of the document located at the indicated source.

3. **Exhibit A:** Attached hereto as Exhibit A is a true and correct copy of pages 7, 24-25, 27, 35-37, 111, 121-22, and 137-38 of the 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) ("PCLOB 702 Report"), *available at* http://www.pclob.gov/All Documents/Report on the Section 702 Program/PCLOB-Section-702-Report.pdf.

4. **Exhibit B:** Attached hereto as Exhibit B is a true and correct copy of NSA PRISM slides, published by the Guardian on November 1, 2013, *available at* http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document and also *available at* http://s3.documentcloud.org/documents/813847/prism.pdf.

5. **Exhibit C:** Attached hereto as Exhibit C is an excerpt from the NSA's Special Source Operations Weekly, March 14, 2013 edition, published by the Washington Post on October 30, 2013 *available at* http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/ and also *available at* http://s3.documentcloud.org/documents/813020/sso-weekly-excerpt-for-posting-redacted.pdf.

6. **Exhibit D:** Attached hereto as Exhibit D is a true and correct copy of pages 6-8 of the December 8, 2011 Joint Statement of Assistant Attorney General Lisa Monaco, National Security Agency Deputy Director John Inglis, and General Counsel, Office of the Director of National Intelligence, Robert Litt, *available at* http://www.dni.gov/files/documents/Joint Statement FAA Reauthorization Hearing - December 2011.pdf.

7. **Exhibit E:** Attached hereto as Exhibit E is a true and correct copy of figure 9, page 29 of Federal Communications Commission, Common Carrier Bureau, 1999 International

Telecommunications Data (Dec. 2000), *available at*: http://transition.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/Intl/4361-f99.pdf.

8. **Exhibit F:** Attached hereto as Exhibit F is a true and correct copy of page 183 of the President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Dec. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

9. **Exhibit G:** Attached hereto as Exhibit G is a true and correct copy of pages 35-37 of the Testimony of the Hon. James Robertson (U.S. District Judge, ret.), "Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act" (July 9, 2013), *available at* http://www.pclob.gov/All Documents/July 9, 2013 Workshop Transcript.pdf.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed at San Francisco, California on July 25, 2014.

s/ *Richard R. Wiebe*
Richard R. Wiebe

EXHIBIT A

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

targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program.

Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government identifies or "tasks" certain "selectors," such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection.

In PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider ("ISP"), and the provider is compelled to give the communications sent to or from that selector to the government. PRISM collection does not include the acquisition of telephone calls. The National Security Agency ("NSA") receives all data collected through PRISM. In addition, the Central Intelligence Agency ("CIA") and the Federal Bureau of Investigation ("FBI") each receive a select portion of PRISM collection.

Upstream collection differs from PRISM collection in several respects. First, the acquisition occurs with the compelled assistance of providers that control the telecommunications "backbone" over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies. Upstream collection also includes telephone calls in addition to Internet communications. Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data. Finally, the upstream collection of Internet communications includes two features that are not present in PRISM collection: the acquisition of so-called "about" communications and the acquisition of so-called "multiple communications transactions" ("MCTs"). An "about" communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being "to" or "from" the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be "about" the selector. An MCT is an Internet "transaction" that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or "about" a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.

Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency's use,

of the acquisition to be located in the United States."[63] Finally, Section 702 contains a limitation (and a reminder) that any acquisition must always be conducted consistent with the requirements of the Fourth Amendment to the Constitution.[64]

B. Section 702 Certifications

The Attorney General and the Director of National Intelligence authorize Section 702 targeting in a manner substantially different than traditional electronic surveillance under FISA. To authorize traditional FISA electronic surveillance, an application approved by the Attorney General must be made to the FISC.[65] This individualized application must include, among other things, the identity (if known) of the specific target of the electronic surveillance; facts justifying a probable cause finding that this target is a foreign power or agent of a foreign power and uses (or is about to use) the communication facilities or places at which electronic surveillance is being directed;[66] minimization procedures governing the acquisition, retention, and dissemination of non-publicly available U.S. person information acquired through the electronic surveillance; and a certification regarding the foreign intelligence information sought.[67] If the FISC judge who reviews the government's application determines that it meets the required elements — including that there is probable cause that the specified target is a foreign power or agent of a foreign power and that the minimization procedures meet the statutory requirements — the judge will issue an order authorizing the requested electronic surveillance.[68]

Section 702 differs from this traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualized determinations by the FISC. Under the statute, the Attorney General and Director of National Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted.[69] Instead of identifying particular individuals to be targeted under Section 702, the certifications identify categories of foreign intelligence information regarding which the Attorney

---

63 50 U.S.C. § 1881a(b)(4).

64 50 U.S.C. § 1881a(b)(5).

65 50 U.S.C. § 1804(a). FISA also grants additional authority to conduct emergency electronic surveillance without first making an application to the FISC. 50 U.S.C. § 1805(e).

66 *But see* 50 U.S.C. § 1805(c)(3) (permitting electronic surveillance orders "in circumstances where the nature and location of each of the facilities or places at which surveillance will be directed is unknown")

67 50 U.S.C. §§ 1804(a), 1805(a).

68 50 U.S.C. § 1805(a), (c), (d).

69 50 U.S.C. § 1881a(a); NSA DCLPO REPORT, *supra*, at 2 (noting that Section 702 certifications do not require "individualized determination" by the FISC).

General and Director of National Intelligence authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad.[70] There also is no requirement that the government demonstrate probable cause to believe that a Section 702 target is a foreign power or agent of a foreign power, as is required under traditional FISA. Rather, the categories of information being sought must meet the definition of foreign intelligence information described above. The government has not declassified the full scope of the certifications that have been authorized, but officials have stated that these certifications have authorized the acquisition of information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.[71]

While individual targets are not specified, Section 702 certifications must instead contain "targeting procedures" approved by the Attorney General that must be "reasonably designed" to ensure that any Section 702 acquisition is "limited to targeting persons reasonably believed to be located outside the United States" and prevents the "intentional acquisition" of wholly domestic communications.[72] The targeting procedures specify the manner in which the Intelligence Community must determine whether a person is a non-U.S. person reasonably believed to be located outside the United States who possesses (or is likely to possess or receive) the types of foreign intelligence information authorized by a certification. The process by which individuals are permitted to be targeted pursuant to the targeting procedures is discussed in detail below. In addition, the Attorney General and Director of National Intelligence must also attest in the certification that the Attorney General has adopted additional guidelines to ensure compliance with both these and the other statutory limitations on the Section 702 program.[73] Most critically, these Attorney General Guidelines explain how the government implements the statutory prohibition against reverse targeting.

While only non-U.S. persons may be intentionally targeted, the information of or concerning U.S. persons may be acquired through Section 702 targeting in a variety of ways, such as when a U.S. person is in communication with a non-U.S. person Section 702

---

70 *See* 50 U.S.C. § 1881a(g)(2)(A)(v) (requiring Attorney General and Director of National Intelligence to attest that a significant purpose of the acquisition authorized by the certification is to acquire foreign intelligence information); PCLOB March 2014 Hearing Transcript, *supra*, at 8-9 (statement of Robert Litt, General Counsel, ODNI) (stating that certifications "identify categories of information that may be acquired"); NSA DCLPO REPORT, *supra*, at 2 (noting the "annual topical certifications" authorized by Section 702).

71 PCLOB March 2014 Hearing Transcript at 13 (statement of Robert Litt, General Counsel, ODNI) (stating that the Section 702 program has been an important source of information "not only about terrorism, but about a wide variety of other threats to our nation"); *id.* at 59 (statement of Rajesh De, General Counsel, NSA) (stating that there are certifications on "counterterrorism" and "weapons of mass destruction"); *id.* at 68 (statement of James A. Baker, General Counsel, FBI) ("[T]his program is not limited just to counterterrorism.").

72 50 U.S.C. § 1881a(d)(1), (g)(2)(A)(i), (g)(2)(B).

73 50 U.S.C. § 1881a(f), (g)(2)(A)(iii).

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).

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.

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.

While we believe that the measures taken by the NSA to exclude wholly domestic "about" communications may be reasonable in light of current technological limits, they are not perfect.[506] Even where both parties to a communication are located in the United States, in a number of situations the communication might be routed internationally, in which case it could be acquired by the NSA's upstream collection devices.[507] There are reasons to suppose that this occurs rarely, but presently no one knows how many wholly domestic communications the NSA may be acquiring each year as a result of "about" collection.[508]

The more fundamental concern raised by "about" collection is that it 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.[509] This practice fundamentally differs from "incidental" collection, discussed above. While incidental collection also permits the government to acquire communications of people about whom it may have had no prior knowledge, that is an inevitable result of the fact that conversations generally involve at least two people: acquiring a target's communications by definition involves acquiring his communications with other people. But no effort is made to acquire those other peoples' communications — the government simply is acquiring the target's communications. In "about" collection, by contrast, the NSA's

---

506 December 2011 Joint Statement, *supra*, at 7 (acknowledging that the NSA's efforts "are not perfect").

507 *See generally* Bates October 2011 Opinion, *supra*, at 34, 2011 WL 10945618, at *11.

508 Although the NSA conducted a study in 2011, at the behest of the FISA court, to estimate how many wholly domestic communications it was annually acquiring as a result of collecting "MCTs" (discussed below), the study did not focus on how many domestic communications the NSA may be acquiring due to "about" collection where the communication acquired was not an MCT but rather a single, discrete communication. Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11, n.32. At the urging of the FISA court, the NSA subsequently spent some time examining this question, but ultimately did not provide an estimate, instead explaining to the court the logistical reasons that the chance of acquiring domestic communications in "about" collection "should be smaller — and certainly no greater — than potentially encountering wholly domestic communications within MCTs." *Id.* This statement prompted the FISA court to adopt the assumption that the percentage of wholly domestic communications within the agency's "about" collection might equal the percentage of wholly domestic communications within its collection of "MCTs," leading to an estimate of as many as 46,000 wholly domestic "about" communications acquired each year. *Id.* We do not view this as a particularly valid estimate, because there is no reason to suppose that the number of wholly domestic "about" communications matches the number of wholly domestic MCTs, but the fact remains that the NSA cannot say how many domestic "about" communications it may be obtaining each year.

509 *See* December 2011 Joint Statement, *supra*, at 7 ("[U]pstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant."); The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4 ("Upstream collection . . . lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties.").

collection devices can acquire communications to which the target is not a participant, based at times on their contents.[510]

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, under the Fourth Amendment the government may not, without a warrant, open and read letters sent through the mail in order to acquire those that contain particular information.[511] Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.[512] And without the ability to engage in inspection of this sort, nothing akin to "about" collection could feasibly occur with respect to such traditional forms of communication. Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them.

The government values "about" communications for the unique intelligence benefits that they can provide. Although we cannot discuss the details in an unclassified public report, the moniker "about" collection describes a number of distinct scenarios, which the government has in the past characterized as different "categories" of "about" collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the different forms of communications that are neither to nor from a tasked selector but nevertheless are collected because they contain the selector somewhere within them.[513] In some instances, the targeted person actually is a participant to the communication (using a different communications selector than the one that was "tasked" for collection), and so the term "about" collection may be misleading.[514] In other instances, a communication may not involve the targeted person, but for various logistical and technological reasons it will almost never involve a person located in the United States.

---

510 *See* December 2011 Joint Statement, *supra*, at 7.

511 *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Ex parte Jackson*, 96 U.S. 727, 733 (1877).

512 *See Katz v. United States*, 389 U.S. 347 (1967).

513 Such communications include "any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the . . . previously identified categories of 'about communications[.]'" Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *11.

514 The term *"about" communications* was originally devised to describe communications that were "about" the selectors of targeted persons — meaning communications that contained such a selector within the communication. But the term has been used more loosely by officials in a way that suggests these communications are "about" the targeted persons. References to targeted *persons* do not themselves lead to "about" collection; only references to the communications *selectors* of targeted persons lead to "about" collection.

internal agency reviews to ensure that the new targeting procedures have been adopted by its analysts. The executive branch compliance audits should also be modified to reflect the new targeting procedures and to include more rigorous scrutiny of whether valid foreign intelligence purpose determinations are being properly articulated.

II. U.S. Person Queries

Recommendation 2: The FBI's minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters.

When an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime, it is routine practice, pursuant to the Attorney General Guidelines for Domestic FBI Operations, to conduct a query of FBI databases in order to determine whether they contain information on the subject of the assessment or investigation. The databases queried may include information collected under various FISA authorities, including data collected under Section 702. The FBI's rules relating to queries do not distinguish between U.S. persons and non-U.S. persons; as a domestic law enforcement agency, most of the FBI's work concerns U.S. persons. If a query leads to a "hit" in the FISA data (i.e., if a communication is found within a repository of Section 702 data that is responsive to the query), then the agent or analyst is alerted to the existence of the hit. If the agent or analyst has received training on how to handle FISA-acquired materials, he or she is able to view the Section 702 data that was responsive to the query; however, if the agent or analyst has not received FISA training he or she is merely alerted to the existence of the information but cannot access it. The agent or analyst would have to contact a FISA-trained agent or analyst and ask him or her to review the information.

Even though FBI analysts and agents who solely work on non-foreign intelligence crimes are not *required* to conduct queries of databases containing Section 702 data, they are *permitted* to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI's minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices. Among other benefits, this improved clarity will better enable the FISA court to assess statutory and constitutional compliance when

the minimization procedures are presented to the court for approval with the government's next recertification application.

In light of the privacy and civil liberties implications of using Section 702 information, collected under lower thresholds and for a foreign intelligence purpose, in the FBI's pursuit of non-foreign intelligence crimes, the Board believes it is appropriate to place some additional limits on what can be done with Section 702 information. Members of the Board differ on the nature of the limitations that should be placed on the use of that information. Board Members' proposals and a brief explanation of the reasoning supporting each are stated below, with elaboration in the two separate statements.

Additional Comment of Chairman David Medine and Board Member Patricia Wald

For acquisitions authorized under Section 702, FISA permits the FBI for law enforcement purposes, to retain and disseminate evidence of a crime. However, there is a difference between obtaining a U.S. person's communications when they are in plain view as an analyst reviews the target's communications, and the retrieval of a U.S. person's communications by querying the FBI's Section 702 holdings collected over the course of years.[545] Therefore, consistent with our separate statement regarding Recommendation 3, we believe that U.S. persons' privacy interests regarding 702 data should be protected by requiring that each identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, other than in exigent circumstances. The court should determine, based on documentation submitted by the government, whether 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. As discussed in more detail in our separate statement, this judicial review would not be necessary for U.S. persons who are already suspected terrorists and subject to surveillance under other government programs.

Additional Comment of Board Members Rachel Brand and Elisebeth Collins Cook

As explained in our separate statement, we would support a requirement that an analyst conducting a query in a non-foreign intelligence criminal matter obtain supervisory approval before accessing any Section 702 information that was responsive to the query. We would also support a requirement of higher-level Justice Department approval, to the extent not already required, before Section 702 information could be used

---

545 On June 25, 2014, the United States Supreme Court ruled unanimously that a search of a cell phone seized by the police from an individual who has been arrested required a warrant. *Riley v. California*, No. 13-132, 2014 WL 2864483 (U.S. June 25, 2014). The Court distinguished between reviewing one record versus conducting an extensive records search over a long period: "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." *Id.* at *18. Likewise, observing evidence of a crime in one email does not justify conducting a search of an American's emails over the prior five years to or from everyone targeted under the Section 702 program.

EXHIBIT B

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

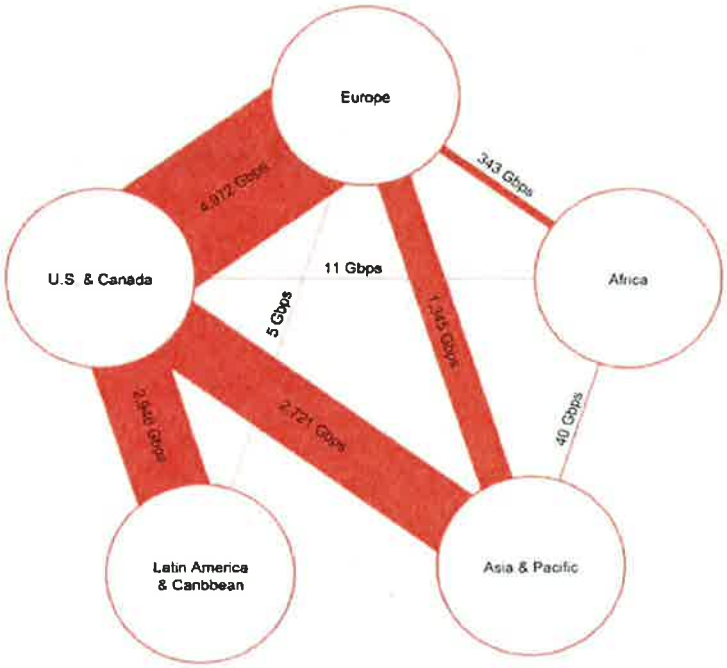
[redacted] PRISM Collection Manager, S35333

April 2013

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

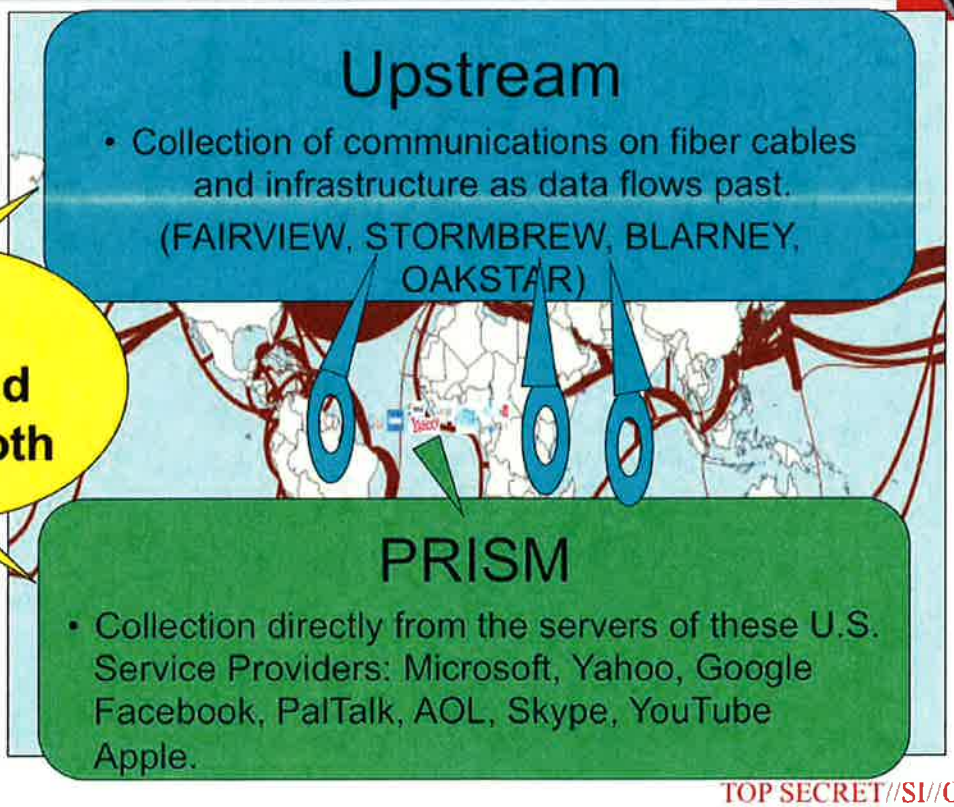
(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)



You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

(TS//SI//NF) FAA702 Operations

Why Use Both: PRISM vs. Upstream

	PRISM	Upstream
DNI Selectors	✓ 9 U.S. based service providers	✓ Worldwide sources
DNR Selectors	⊘ Coming soon	✓ Worldwide sources
Access to Stored Communications (Search)	✓	⊘
Real-Time Collection (Surveillance)	✓	✓
"Abouts" Collection	⊘	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	⊘ Only through FBI	✓

(TS//SI//NF) PRISM Collection Details

Current Providers

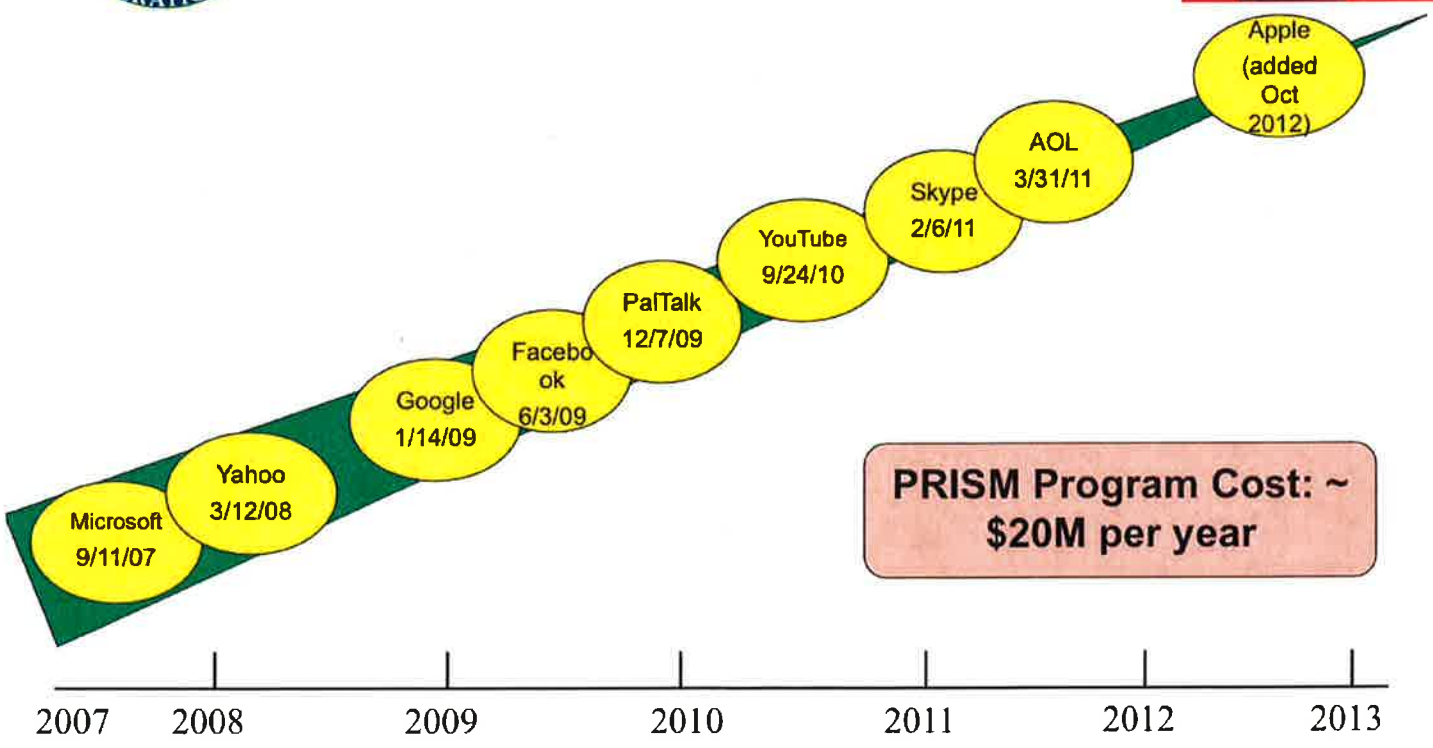
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



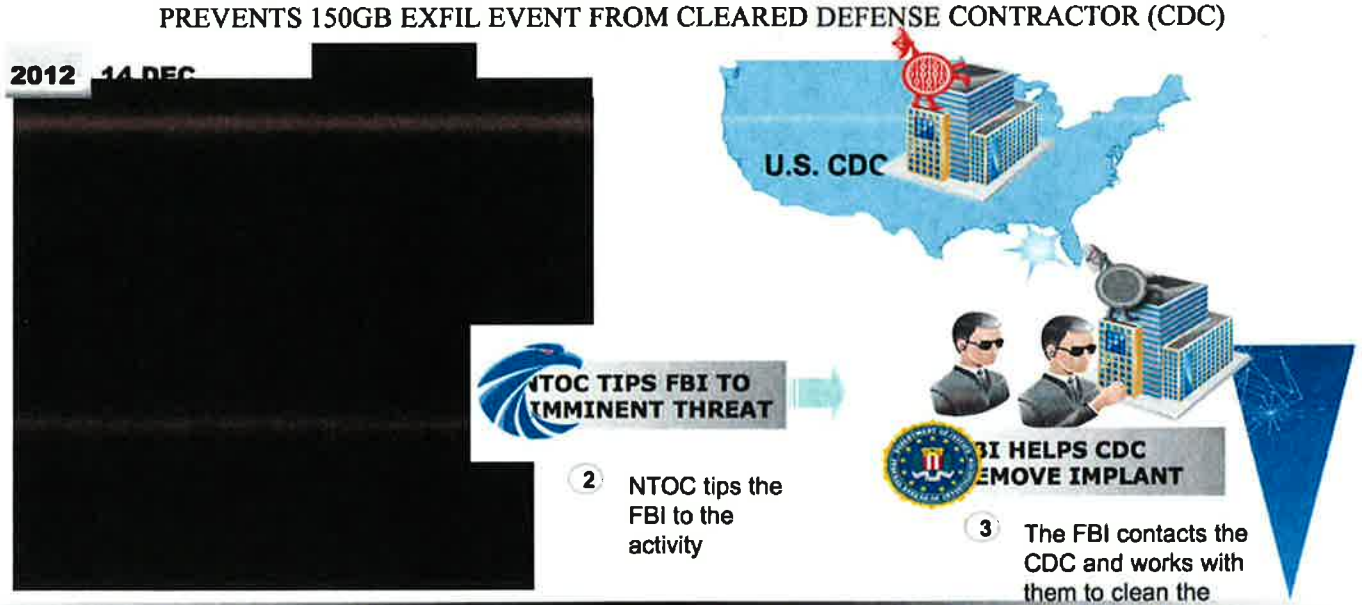
(TS//SI//NF) FAA702 Reporting Highlight

PRISM and STORMBREW Combine

To Thwart [redacted]

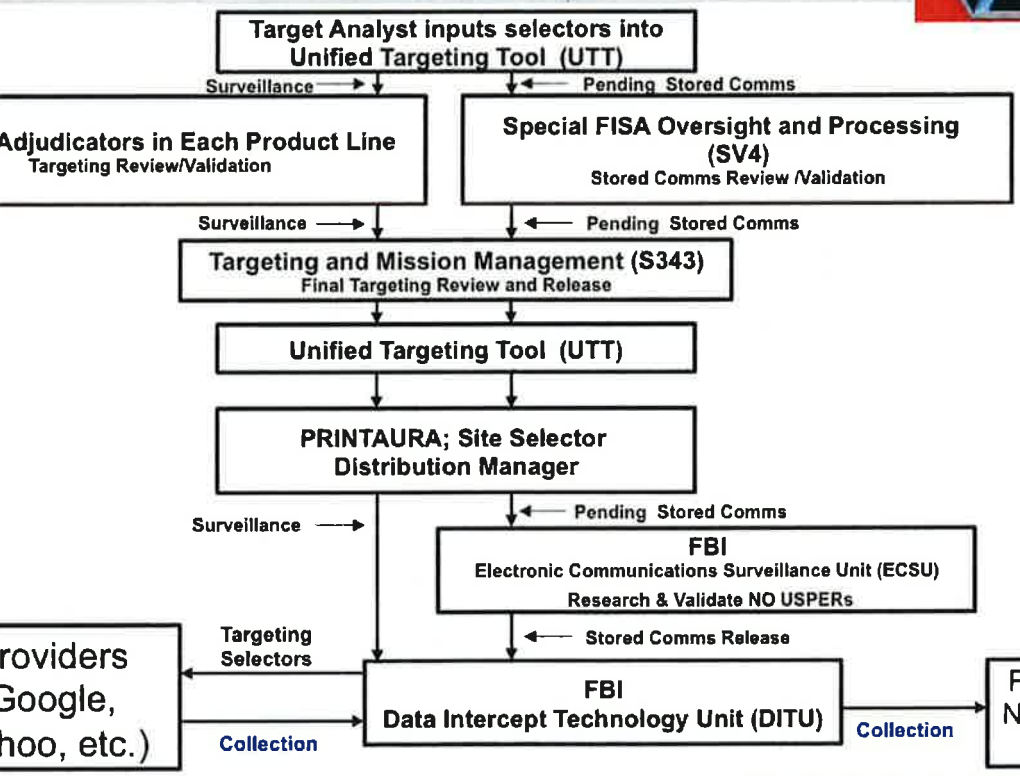
SAME-DAY NTOC/FBI COLLABORATION

PREVENTS 150GB EXFIL EVENT FROM CLEARED DEFENSE CONTRACTOR (CDC)

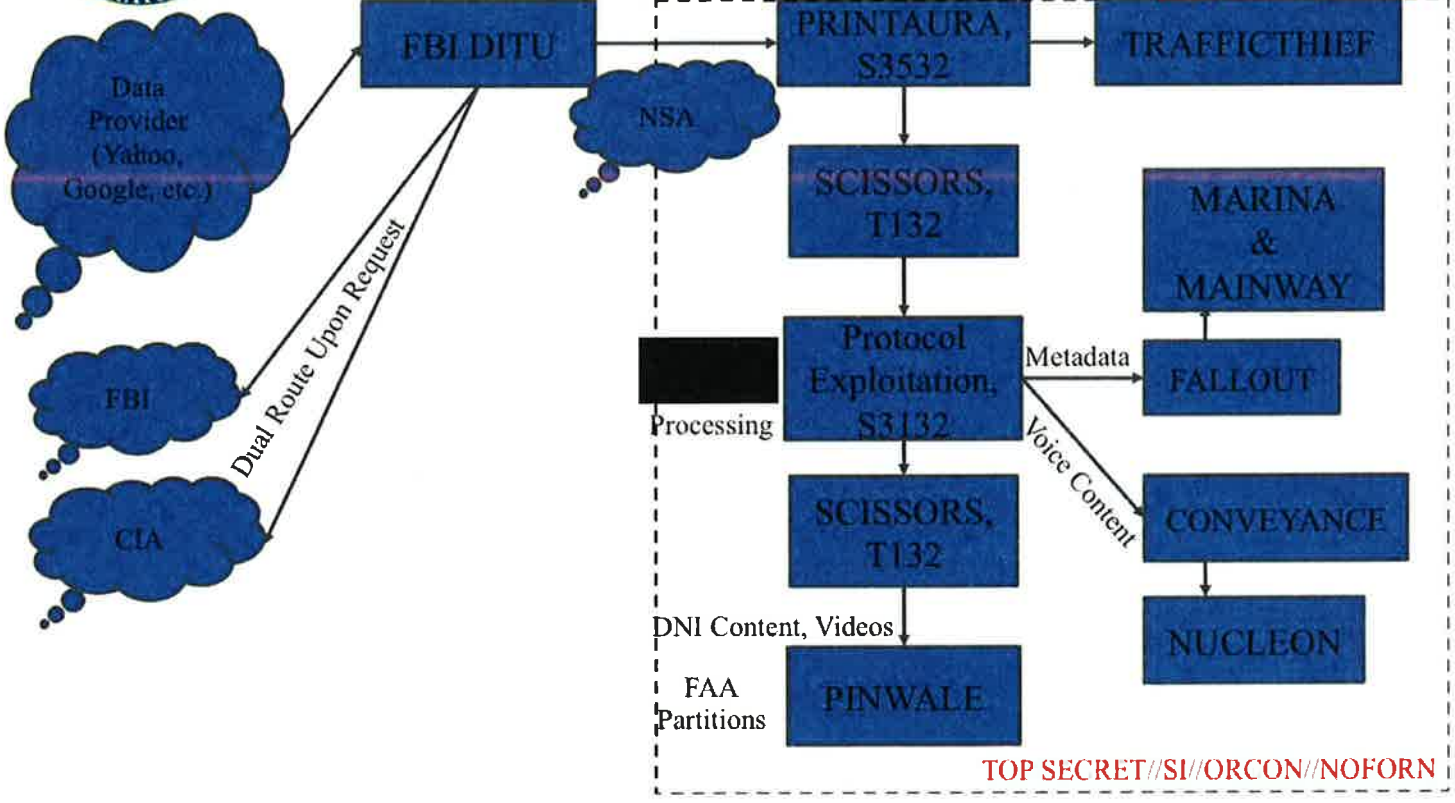


The victim performed comprehensive actions on the infected network, thus **PREVENTING EXFILTRATION** on the **SAME DAY NTOC DISCOVERED ADVERSARY INTENT**

(TS//SI//NF) PRISM Tasking Process



(TS//SI//NF) PRISM Collection Dataflow



(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
- P1: Microsoft
- P2: Yahoo
- P3: Google
- P4: Facebook
- P5: PalTalk
- P6: YouTube
- P7: Skype
- P8: AOL
- PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
- A: Stored Comms (Search)
- B: IM (chat)
- C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
- D: RTN-IM (real-time notification of a chat login or logout event)
- E: E-Mail
- F: VoIP
- G: Full (WebForum)
- H: OSN Messaging (photos, wallposts, activity, etc.)
- I: OSN Basic Subscriber Info
- J: Videos
- . (dot): Indicates multiple types

(TS//SI//NF) REPRISMFISA TIPS

[redacted]

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET/[redacted]/SI/TK//ORCON/NOFORN

REPRISMFISA

COUNTERTERRORISM

[redacted] 2013-Apr-05 13:10:28Z

Click on the PRISM icon first (from the initial webpage)

PRISM ENTRIES

Last Load on Apr 05, 2013 at 12:22 PM GMT

Check the total record status, click on this link

QUICK LINKS

- See Entire List (Current)
- See Entire List (Current and Expired)
- See NSA List
- See New Records
- Ownership Count

If the total count is much less than this, REPRISMFISA is having issues, E-MAIL the REPRISMFISA HELP DESK AT [redacted] AND INFORM THEM

SEARCH

The search form below can be used as a filter to see a partial list of records.

Search For:

AND OR

Expiration days

(+ - from now)

Filter

Prism Current Entries

Records 1 - 50 out of 117675 Page 1 of 2354 > >> Records per page: 50

Clear Sort Order Click on column headers to sort. * = column is not sortable.

[redacted]

EXHIBIT C

SECRET//SI//REL USA, GBR

(U//FOUO) WINDSTOP/2P System Highlights

MUSCULAR

- Minor circuit move, not collection suite move (so-2013-00762)
- XKS FP updates across TU systems / NArchive throttle update

INCENSER

- INCS4 config issue (uo-2013-00471)

SECRET//SI//REL USA, GBR

Speaker's Notes

From Feb 28 2013: Proposed/imminent latest DO/Volume reduction: Narchive

BLUF: Requested S2 concurrence at S2 TLC on 25 Feb with partial throttling of content from Yahoo, Narchive email traffic which contains data older than 6 months from MUSCULAR. Numerous S2 analysts have complained of its existence, and the relatively small intelligence value it contains does not justify the sheer volume of collection at MUSCULAR (1/4th of the total daily collect).

Background: Since July of 2012, Yahoo has been transferring entire email accounts using the Narchive data format (a proprietary format for which NSA had to develop custom demultiplexers). To date, we are unsure why these accounts are being transferred – movement of individuals, backup of data from overseas servers to US servers, or some other reason. There is no way currently to predict if an account will be transferred via Yahoo Narchive.

Currently, Narchive traffic is collected and forwarded to NSA for memorialization in any quantity only from DS-200B. On any given day, Narchive traffic represents 25% (15GB) of DS-200B's daily PINWALE content allocation (60GB currently). DS-200B is scheduled to be upgraded in the summer of 2013; it is likely that memorialized Narchive traffic, if still present in the environment, will grow proportionally (i.e. double now, to 30 GB/day).

Narchive traffic is mailbox formatted email, meaning unlike Yahoo webmail, any attachments present would be collected as part of the message. This is a distinct advantage. However, it has not been determined what causes an Narchive transfer of an account, so these messages are rarely collected "live".

Based on analysis of Narchive email data by [redacted] and [redacted], we were able to indentify statistics for the original communications date for Narchive email messages collected:

< 30 days	1118	11%
> 30 days, < 90 days	1758	17%
> 90 days < 180 days	1302	13%
> 180 days, < 1 year	2592	26%
> 1years, < 5 years	3084	31%
> 5years	154	>1%

Numerous target offices have complained about this collection "diluting" their workflow. One argument for keeping it is that it provides a retrospective look at target activity – this argument is hampered by a) the unreliable and non-understood nature of when the transfer occurs for an account, and b) that FISA restrospective collection would retrieve the exact same data "on demand".

SSO Optimization believes that while this is "valid" collection of content, the sheer volume and the age – coupled with the unpredictable nature of Narchive activity – makes collecting older data a less desirable use of valuable resources. 59% of Narchive email collected was originally sent and received more than 180 days after collection. This represents about 8.9 GB a day of "less desirable" collection – long term allocation that could be easily filled with more timely, useful FI from this lucrative SSO site. As always with our optimization, the data would still be available at the site store for SIGDEV. This would not impact metadata extraction.

Past DO volume reduction efforts:
Webmail OAB- Leap day 2012: the original defeat only targeted gmail, yahoo, and hotmail webmail protocol
FB buddylist sampling since last year

Today: FB OAB defeat/atxks/facebook/ownerless_addressbook : this is a JSON addressbook

EXHIBIT D

~~TOP SECRET//COMINT//ORCON/NOFORN~~

JOINT STATEMENT OF

LISA O. MONACO
ASSISTANT ATTORNEY GENERAL
FOR NATIONAL SECURITY
U.S. DEPARTMENT OF JUSTICE

JOHN C. (CHRIS) INGLIS
DEPUTY DIRECTOR
NATIONAL SECURITY AGENCY

ROBERT S. LITT
GENERAL COUNSEL
OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING
"FISA AMENDMENTS ACT REAUTHORIZATION"

PRESENTED ON
DECEMBER 8, 2011

[redacted]

Joint Statement of

Lisa O. Monaco
Assistant Attorney General
for National Security
U.S. Department of Justice

John C. (Chris) Inglis
Deputy Director
National Security Agency

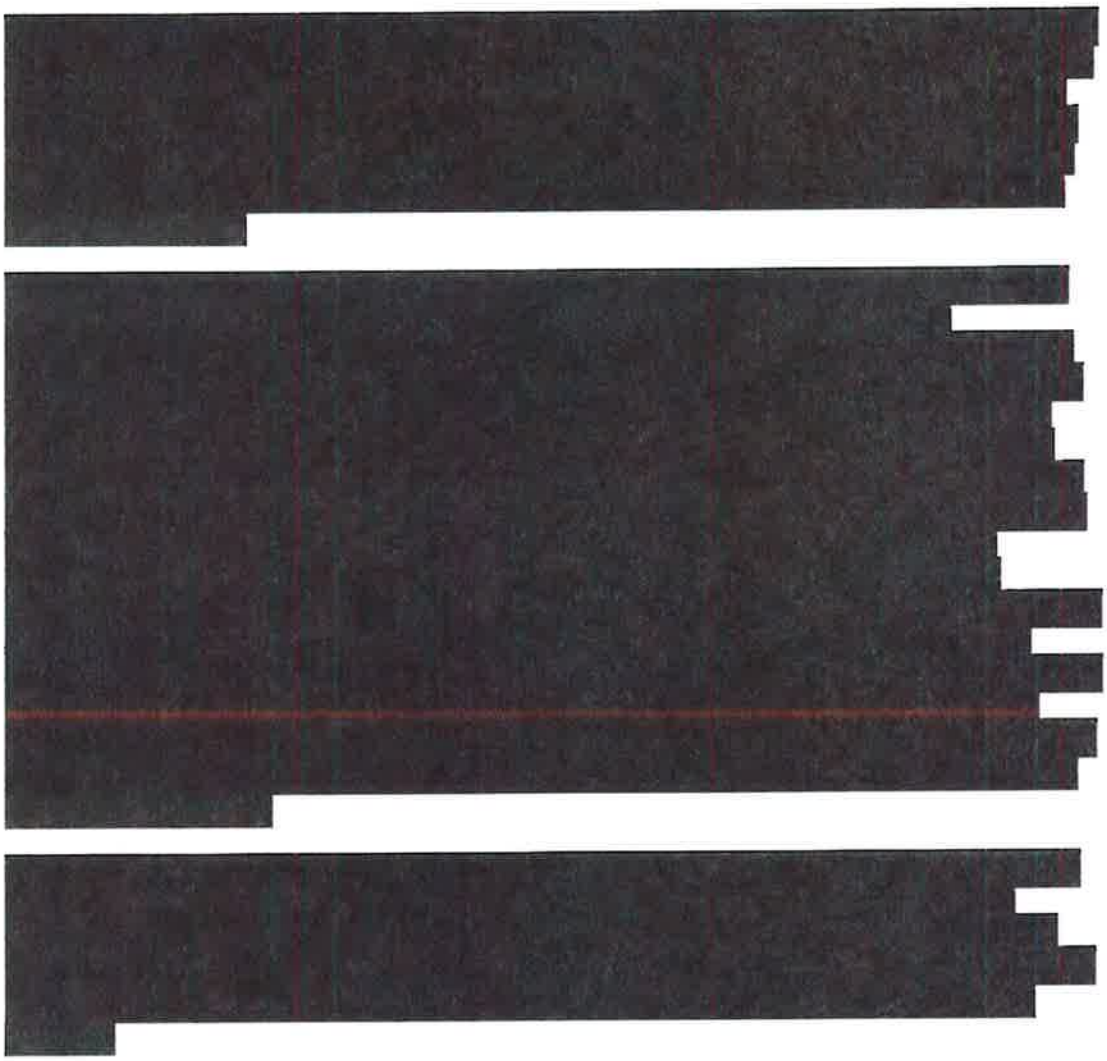
Robert S. Litt
General Counsel
Office of Director of National Intelligence

Before the
Permanent Select Committee on Intelligence
United States House of Representatives

At a Hearing Concerning
"FISA Amendments Act Reauthorization"

Presented on
December 8, 2011

[redacted]



(U) **Recent FISC Opinion**

~~(TS//SI//NF)~~ On October 3, 2011, the FISC issued an opinion addressing the Government's submission of replacement certifications under section 702. *In re DNI/AG Certification 2009-C, et. al.*, [redacted], Mem. Op. The FISC approved most of the Government's submission. It upheld NSA's and FBI's targeting procedures, CIA's and FBI's minimization procedures, and most of NSA's minimization procedures. Nevertheless, the FISC denied in part the Government's requests because of its concerns about the rules governing the retention of certain non-targeted Internet communications acquired through NSA's upstream collection. The FISC's exhaustive analysis of the Government's submission, like its other decisions, refutes any argument that the court is a "rubber stamp," and demonstrates the rigorous nature of the oversight it conducts.

~~(TS//SI//NF)~~ As described above, upstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant. In doing so, NSA uses [redacted] that are reasonably designed to screen out communications that are wholly domestic in nature, in accordance with section 702's requirements. Although reasonably designed to accomplish this result, [redacted] are not perfect. In addition, upstream collection devices acquire Internet "transactions" that include tasked selectors. Such a transaction may consist of a single communication (a "single-communication transaction," or SCT) or multiple communications sent in a single transaction (a "multi-communication transaction," or MCT) [redacted] In such instances, upstream collection acquires the entire MCT, which in all cases will include a communication to, from, or about a tasked selector but in some cases may also include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship, to the targeted selector. Thus although upstream collection only targets Internet communications that are not between individuals located in the United States and are to, from, or about a tasked account, there is some inevitable incidental collection of wholly domestic communications or communications not to, from, or about a tasked account that could contain U.S. person information. Based on a sample reviewed by NSA, the percentage of such communications is very small (about .02%), but given the volume of the upstream collection, the FISC concluded that the actual number of such communications may be in the tens of thousands annually.

~~(TS//SI//NF)~~ The FISC upheld NSA's continued upstream acquisition of Internet communications under section 702 even though it includes the unintentional acquisition of wholly domestic communications and the incidental acquisition of MCTs that may contain one or more individual communications that are not to, from, or about the tasked selector. *See id.* at 74, 78-79. The FISC also reaffirmed that the acquisition of foreign intelligence information under section 702 falls within the foreign intelligence exception to the warrant requirement of the Fourth Amendment, and confirmed that nothing had disturbed its "prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures." *Id.* at 69.

~~(TS//SI//NF)~~ The FISC determined, however, that the minimization procedures governing *retention* of MCTs were inconsistent with the requirements of section 702. The FISC found that the Government had not fully explored options regarding data retention that would be more protective of U.S. persons, and that the FISC thus could not determine that the Government's minimization procedures satisfied FISA's requirement that such procedures be "reasonably designed" to minimize the retention of protected U.S. person information. The FISC further held that, although the Fourth Amendment's warrant requirement was not implicated, in light of NSA's proposed procedures for handling MCTs, NSA's proposed acquisition and minimization procedures did not satisfy the Fourth Amendment's reasonableness requirement. The FISC recognized, however, that the Government may be able to "tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment," and suggested a number of possibilities as to how this might be done. *Id.* at 61-63, 78-80.

~~(TS//SI//NF)~~ On October 31, 2011, after extensive consultations among the Department, ODNI, and NSA, the Attorney General submitted amended minimization procedures to the FISC addressing the deficiencies noted by the court. These amended procedures continue to allow for the upstream collection of MCTs; however, they also create more rigorous rules governing the retention of MCTs as well as NSA analysts' exposure to, and use of, non-targeted communications. On balance, NSA believes that the impact of these procedures on operations is acceptable as a necessary requirement in order to continue upstream collection, and that these procedures will allow for continued useful intelligence collection and analysis. On November 30, the FISC granted the Government's request for approval of the amended procedures, stating that, with regard to information acquired pursuant to 2011 certifications, "the government has adequately corrected the deficiencies identified in the October 3 Opinion," and that the amended procedures, when "viewed as a whole, meet the applicable statutory and constitutional requirements."

(U) The Government has provided copies of the opinions and the filings by the Government to this Committee, and the Government will continue to inform the Committee about developments in this matter.

[redacted]

EXHIBIT E

1999
International Telecommunications Data

(Filed as of October 31, 2000)

December 2000

Linda Blake
Jim Lande

Industry Analysis Division
Common Carrier Bureau
Federal Communications Commission
Washington, DC 20554

This report is available for reference in the FCC's Reference Information Center at 445 12th Street, S.W., Courtyard Level. Copies may be purchased by calling International Transcription Services, Inc., (ITS) at (202) 857-3800. The report can be downloaded [file names: 4361-F99.ZIP or 4361-F99.PDF] from the **FCC-State Link** internet site at http://www.fcc.gov/ccb/stats on the World Wide Web.

Figure 9
International Message Telephone Traffic and Revenues
for the Three Largest International Carriers

	U.S. Billed Traffic			All Traffic that Originates or Terminates in the U.S.		
	Number of Minutes (000,000)	U.S. Carrier Revenue ($000,000)	Billed Revenue per Minute	Number of Minutes (000,000)	U.S. Carrier Retained Revenue ($000,000)	Net of Settlements Revenue per Minute
AT&T						
1991	6,596	$6,962	$1.06	10,020	$4,279	$0.43
1992	7,039	$7,314	$1.04	10,741	$4,814	$0.45
1993	7,201	$7,482	$1.04	10,938	$4,979	$0.46
1994	8,040	$7,984	$0.99	11,807	$5,229	$0.44
1995	8,831	$8,425	$0.95	12,778	$5,634	$0.44
1996	9,546	$8,559	$0.90	13,563	$5,705	$0.42
1997	10,331	$8,351	$0.81	14,529	$5,786	$0.40
1998	10,452	$7,533	$0.72	15,113	$5,332	$0.35
1999	10,900	$6,755	$0.62	15,944	$4,921	$0.31
MCI *						
1991	1,600	$1,487	$0.93	2,450	$958	$0.39
1992	2,101	$2,065	$0.98	3,163	$1,360	$0.43
1993	2,857	$2,779	$0.97	4,175	$1,789	$0.43
1994	3,529	$2,952	$0.84	5,206	$1,790	$0.34
1995	4,486	$3,968	$0.88	6,350	$2,402	$0.38
1996	5,372	$3,550	$0.66	7,496	$1,772	$0.24
1997	5,913	$4,243	$0.72	8,216	$2,634	$0.32
1998	7,195	$4,298	$0.60	10,257	$2,745	$0.27
1999	8,306	$5,056	$0.61	11,396	$3,489	$0.31
Sprint						
1991	728	$604	$0.83	1,139	$407	$0.36
1992	946	$786	$0.83	1,424	$520	$0.37
1993	1,181	$1,048	$0.89	1,730	$706	$0.41
1994	1,490	$1,229	$0.82	2,140	$742	$0.35
1995	1,772	$1,289	$0.73	2,480	$741	$0.30
1996	2,745	$1,493	$0.54	4,060	$672	$0.17
1997	2,794	$1,478	$0.53	4,505	$822	$0.18
1998	2,916	$1,421	$0.49	4,795	$922	$0.19
1999	3,640	$1,379	$0.38	5,507	$825	$0.15
WorldCom, Inc.						
1991	3	$2	$0.52	4	$1	$0.26
1992	12	$10	$0.82	21	$6	$0.29
1993	92	$64	$0.70	132	$27	$0.21
1994	278	$124	$0.45	362	$38	$0.10
1995	544	$291	$0.53	798	$144	$0.18
1996	846	$364	$0.43	1,137	$100	$0.09
1997	1,400	$500	$0.36	1,842	$114	$0.06
1998	-	-	-	-	-	-
1999	-	-	-	-	-	-

* MCI for years 1991-1997, MCI WorldCom, Inc. thereafter.

EXHIBIT F

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies

During the Cold War, ordinary Americans used the telephone for many local calls, but they were cautious about expensive "long-distance" calls to other area codes and were even more cautious about the especially expensive "international" phone calls. Many people today, by contrast, treat the idea of "long-distance" or "international" calls as a relic of the past. We make international calls through purchases of inexpensive phone cards or free global video services. International e-mails are cost-free for users.

The pervasively international nature of communications today was the principal rationale for creating Section 702 and other parts of the FISA Amendments Act of 2008. In addition, any communication on the Internet might be routed through a location outside of the United States, in which case FISA does not apply and collection is governed under broader authorities such as Executive Order 12333. Today, and unbeknownst to US users, websites and cloud servers may be located outside the United States. Even for a person in the US who never knowingly sends communications abroad, there may be collection by US intelligence agencies outside of the US. [160] The cross-border nature of today's communications suggests that when decisions are made about foreign surveillance, there is a need for greater consideration of policy goals involving the protection of civilian commerce and individual privacy.

---

[160] *See* Jonathan Mayer, "The Web is Flat" Oct. 30, 2013 (study showing "pervasive" flow of web browsing data outside of the US for US individuals using US-based websites), available at http://webpolicy.org/2013/10/30/the-web-is-flat/.

EXHIBIT G

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act

July 9, 2013

The workshop was held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue NW, Washington, D.C. 20036 commencing at 9:30 a.m.

Reported by: Lynne Livingston

BOARD MEMBERS

David Medine, Chairman
Rachel Brand
Patricia Wald
James Dempsey
Elizabeth Collins Cook

PANEL I

Legal/Constitutional Perspective

Steven Bradbury, formerly DOJ Office of Legal Counsel
Jameel Jaffer, ACLU
Kate Martin, Center for National Security Studies
Hon. James Robertson, Ret., formerly District Court and Foreign Intelligence Surveillance Court
Kenneth Wainstein, formerly DOJ National Security Division/White House Homeland Security Advisor

Judging is choosing between adversaries. I read the other day that one of my former FISA Court colleagues resisted the suggestion that the FISA approval process accommodated the executive, or maybe the word was cooperated. Not so, the judge replied. The judge said the process was adjudicating.

I very respectfully take issue with that use of the word adjudicating. The ex parte FISA process hears only one side and what the FISA process does is not adjudication, it is approval.

Which brings me to my second and I think closely related point. The FISA approval process works just fine when it deals with individual applications for surveillance warrants because approving search warrants and wiretap orders and trap and trace orders and foreign intelligence surveillance warrants one at a time is familiar ground for judges.

And not only that, but at some point a search warrant or wiretap order, if it leads on to a prosecution or some other consequence is usually

reviewable by another court.

But what happened about the revelations in late 2005 about NSA circumventing the FISA process was that Congress passed the FISA Amendments Act of 2008 and introduced a new role for the FISC, which was to approve surveillance programs.

That change, in my view, turned the FISA Court into something like an administrative agency which makes and approves rules for others to follow.

Again, that's not the bailiwick of judges. Judges don't make policy. They review policy determinations for compliance with statutory law but they do so in the context once again of adversary process.

Now the great paradox of this intelligence surveillance process of course is the undeniable need for security. Secrecy, especially to protect what the national security community calls sources and methods.

That is why the Supreme Court had to

refuse to hear Clapper versus Amnesty International. The plaintiffs could not prove that their communications were likely to be monitored so they had no standing. That is a classic catch-22 of Supreme Court jurisprudence.

But I submit that this process needs an adversary, if it's not the ACLU or Amnesty International, perhaps the PCLOB itself could have some role as kind of an institutional adversary to challenge and take the other side of anything that is presented to the FISA Court.

Thank you.

MS. BRAND: Thank you, Judge. Ken.

MR. WAINSTEIN: Okay, good morning, everybody. I'd like to thank the board for inviting me here to speak on these very important issues.

I'd like to focus my remarks today on the FISA Amendments Act and the authority in Section 702.

MS. BRAND: Ken, can you pull the mic over to you.